

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»

ЦИФРОВИЗАЦИЯ ДЕЯТЕЛЬНОСТИ СЛЕДСТВЕННЫХ ПОДРАЗДЕЛЕНИЙ
ОРГАНОВ ВНУТРЕННИХ ДЕЛ

ФГАОУ ВО «ЮУрГУ» (НИУ) – 40.05.02. 2016. 518. ВКР

Руководитель работы,
д-р. юрид. наук, доцент
заведующий кафедрой
_____ Сергей Васильевич Зуев
_____ 2021 г.

Автор работы,
студент группы Ю-518
__ Анастасия Владимировна Суркова
_____ 2021 г.

Нормоконтролер,
канд. юрид. наук
__ Оксана Витальевна Овчинникова
_____ 2021 г.

Челябинск
2021

АННОТАЦИЯ

Суркова А.В. Выпускная квалификационная работа «Цифровизация деятельности следственных подразделений органов внутренних дел»: ФГАОУ ВО «ЮУрГУ (НИУ)», Ю-518, 95 с., библиогр. список – 86 наим., прил. 3.

Объектом исследования в выпускной квалификационной работе являются общественные отношения, связанные с процессами внедрения и применения информационных технологий в деятельности следственных подразделений органов внутренних дел.

Предметом исследования являются нормы отечественного и международного законодательства, определяющие порядок внедрения и применения информационных технологий в деятельности следственных подразделений органов внутренних дел.

Цель исследования заключается в изучении и анализе действующего законодательства, регламентирующего порядок внедрения и применения информационных технологий в деятельности следственных подразделений органов внутренних дел, а также разработке предложений, направленных на усовершенствование практической деятельности в сфере применения информационных технологий сотрудниками указанных подразделений.

В работе изучены правовые акты как международного, так и отечественного законодательства, в том числе уголовно-процессуальное законодательство по вопросам применения информационных технологий в деятельности следственных подразделений ОВД; исследована организация процесса расследования преступлений и специфика применения информационных технологий при проведении следственных действий, а также отражена актуальность такого исследования и выявлены перспективы развития информационных технологий в деятельности указанного подразделения.

Результаты исследования имеют практическую значимость, содержат выводы и предложения автора по проблемам, связанным с внедрением и применением информационных технологий в деятельности следственных подразделений органов внутренних дел и анализа практики такого применения. Результаты исследования могут быть полезны при разработке программ обучения юристов, а также в преподавании предметов «Правоохранительные органы», «Уголовно-процессуальное право», «Тактико-специальная подготовка».

ОГЛАВЛЕНИЕ

	ВВЕДЕНИЕ.....	6
1	ПРАВОВАЯ ОСНОВА ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТИ СЛЕДСТВЕННЫХ ПОДРАЗДЕЛЕНИЙ ОРГАНОВ ВНУТРЕННИХ ДЕЛ	
1.1	Международные правовые акты и правовые акты Российской Федерации по вопросам использования информационных технологий в расследовании преступлений	10
1.2	Анализ уголовно-процессуального законодательства по применению информационных технологий в деятельности следственных подразделений органов внутренних дел.....	23
2	ОСОБЕННОСТИ ПРИМЕНЕНИЯ СЛЕДСТВЕННЫМИ ПОДРАЗДЕЛЕНИЯМИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ЦИФРОВЫХ ТЕХНОЛОГИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ	
2.1	Организация процесса расследования преступлений следственными подразделениями органов внутренних дел с использованием информационных технологий.....	35
2.2	Применение информационных технологий при проведении следственных действий	46
2.3	Перспективы развития информационных технологий в деятельности следственных подразделений органов внутренних дел Российской Федерации.....	60
	ЗАКЛЮЧЕНИЕ.....	72
	БИБЛИОГРАФИЧЕСКИЙ СПИСОК.....	76
	ПРИЛОЖЕНИЯ.....	87

ВВЕДЕНИЕ

В настоящее время информационные технологии активно внедряются в деятельность правоохранительных органов по всему миру. Так, в соответствии со «Стратегией развития информационного общества в Российской Федерации на 2017–2030 годы» главной целью на ближайшее десятилетие является построение информационного общества в Российской Федерации. Федеральный закон «О полиции» от 7 февраля 2011 г. №3-ФЗ также провозгласил основным принципом деятельности полиции использование достижений науки и техники, современных технологий и информационных систем, тем самым положив основу создания единой системы информационно-аналитического обеспечения деятельности МВД России. Легальное определение «информационной технологии» содержится в Федеральном законе «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 №149-ФЗ, где данная категория определяется как «процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов».

Информационные технологии используются в деятельности всей системы органов внутренних дел, как на всех уровнях, так и всеми службами и подразделениями. Особый интерес заключается в интеграции информационных технологий в работу следственных подразделений органов внутренних дел, поскольку важная роль в обеспечении общественного порядка и общественной безопасности возложена на данное подразделение.

Актуальность темы выпускной квалификационной работы обусловлена тем, что внедрение информационных технологий в деятельность следственных подразделений ОВД, например, таких как искусственный интеллект, роботизация, виртуализация способствуют повышению эффективности деятельности полиции, однако достаточно масштабный характер настоящих и будущих преобразований затрудняет осознание

потенциальных и реальных опасностей, которые скрывается за грядущими новациями. На сегодняшний день вопросы правового регулирования внедрения, применения и использования информационных технологий деятельности следственных подразделений ОВД в Российской Федерации требуют большого внимания со стороны законодателя. Так, к примеру, ни уголовно-процессуальное законодательство, ни федеральные законы не содержат четких предписаний по применению информационно-технических средств в доказывании по уголовным делам. Отметим также, что из-за избытия информации существует проблема с быстрым обменом информацией между следственными подразделениями органов внутренних дел, что говорит об отсутствии единого информационного пространства в Российской Федерации.

Цель исследования заключается в изучении и анализе действующего законодательства, регламентирующего порядок внедрения и применения информационных технологий в деятельности следственных подразделений органов внутренних дел, а также разработке предложений, направленных на усовершенствование практической деятельности в сфере применения информационных технологий сотрудниками указанных подразделений.

Достижение поставленной цели возможно при условии успешного решения следующих задач:

- изучение международных правовых актов и правовых актов отечественного законодательства по вопросам использования информационных технологий в расследовании преступлений;
- анализ уголовно-процессуального законодательства по применению информационных технологий в деятельности следственных подразделений ОВД;
- исследование организации процесса расследования преступлений следственными подразделениями ОВД с использованием информационных технологий;

- анализ специфики применения информационных технологий при проведении следственных действий;
- выявление перспектив развития информационных технологий в деятельности следственных подразделений ОВД Российской Федерации;
- разработка рекомендаций по совершенствованию дальнейшего развития законодательства и практики применения в указанной сфере.

Объектом выпускной квалификационной работы являются общественные отношения, связанные с процессами внедрения и применения информационных технологий в деятельности следственных подразделений органов внутренних дел.

Предметом выпускной квалификационной работы выступают нормы отечественного и международного законодательства, определяющие порядок внедрения и применения информационных технологий в деятельности следственных подразделений органов внутренних дел.

Методологической основой выпускной квалификационной работы является диалектический метод, а также общенаучные методы познания: анализа, синтеза, индукции, кроме того использованы специальные методы, такие, как сравнительно-правовой, системно-аналитический, метод сравнительного правоведения, формально-логический, контент-анализ периодической печати и др. В процессе исследования мы неоднократно обращались к учебным изданиям и научным публикациям в периодической печати по исследуемой теме.

Теоретической основой выпускной квалификационной работы выступают исследования в области цифрового права, как нового научного направления, преследующего своей целью повышение эффективности развития уголовного, уголовно-процессуального законодательства и уголовного судопроизводства в области использования информационных технологий. В специальной юридической литературе процессы цифровизации рассматривались в исследованиях: В.С. Балакшина, В.Б. Вехова, В.Н. Григорьева, А.И. Зазулина, О.А. Зайцева, Н.А. Зигура, С.В. Зуева, М.О.

Медведевой, П.М.Морхат, Н.Г. Муратовой, П.С. Пастухова, В.А.Родивилиной, М.С. Сергеева, И.В.Смольковой, В.Ю. Стельмах, О.В. Овчинниковой и других авторов.

Нормативную и эмпирическую основу выпускной квалификационной работы составляют Конституция РФ, международные нормативно-правовые акты, Уголовный кодекс РФ, Уголовно-процессуальный кодекс РФ, федеральные законы, а также материалы судебной практики судов общей юрисдикции.

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

1 ПРАВОВАЯ ОСНОВА ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТИ СЛЕДСТВЕННЫХ ПОДРАЗДЕЛЕНИЙ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

1.1 Международные правовые акты и правовые акты Российской Федерации по вопросам использования информационных технологий в расследовании преступлений

В настоящее время деятельность следственных подразделений органов внутренних дел, как в Российской Федерации, так и во всем мире характеризуется стремительным использованием информационных технологий. Процесс интеграции информационных технологий в деятельность следственных подразделений органов внутренних дел в Российской Федерации регламентируют как международные нормативно-правовые акты, так и нормативно-правовые акты отечественного законодательства.

Прежде чем перейдем к характеристике массива нормативно-правовых актов необходимо дать определение ключевого термина данной работы: «информационные технологии». Так, в соответствии с п.2 ст.2 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 №149-ФЗ данная категория определяется как «процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов»¹. К информационным технологиям относятся: устройства, позволяющие осуществлять запись и воспроизведение звука и изображения; устройства телеобработки данных; устройства, предназначенные для автоматической обработки текстов и изображений; программы, способные осуществлять автоматический перевод с одного языка на другой, а также производить поиск информации в базах данных;

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

программное обеспечение для технической диагностики и контроля; экспертные системы; видеотекст и телетекст; полиграфы¹.

Итак, для начала рассмотрим международные правовые акты, регламентирующие особенности внедрения, применения и использования информационных технологий в деятельности следственных подразделений ОВД РФ.

Идея создания глобального информационного общества впервые была озвучена на совещаниях, организованных Советом Европы, Европейским сообществом, ЮНЕСКО. Так, в 1998 г. Международный Телекоммуникационный союз (ITU) в Миннеаполисе принял решение (Резолюция №73) выступить с предложением Организационному комитету ООН о проведении Всемирного саммита по информационному обществу (WSIS) и впервые в истории вопросы создания информационного общества обсуждались на уровне глав государств-членов ООН. По итогам Всемирного саммита были подготовлены следующие основные документы: Декларации принципов и План действий. Декларация принципов «Построение информационного общества—глобальная задача в новом тысячелетии» провозглашает приоритетную задачу для современного общества – создание и развитие глобального информационного сообщества в целях получения, обмена и накопления информационных данных в различных сферах деятельности, в том числе в правоохранительной². «План действий» ООН носит более конкретный характер и устанавливает ориентировочные показатели применения информационно-коммуникационных технологий в странах-участниках Саммита³. Отметим, что в ходе международных конференций была сформирована нормативно-правовая база для широкого

¹Медведева М.О. Уголовно-процессуальная форма информационных технологий: современное состояние и основные направления развития: дис. ... канд.юрид.наук.М.,2018. С.34.

² Декларация принципов «Построение информационного общества – глобальная задача в новом тысячелетии» от 12 декабря 2003 г. // Законодательство и практика масс-медиа. 2004. № 1.

³ Миланский план действий от 29 ноября 1985 г. // Советская юстиция. 1992. № 13–14; № 15–16.

использования информационных технологий в целом, при этом, внедрение информационных технологий в уголовное судопроизводство способствует повышению не только эффективности уголовного процесса, но и сокращению процессуальных сроков, а также обеспечивает гарантии безопасности участников уголовного судопроизводства¹.

Указанные нормативно-правовые акты имеют важное практическое значение в деятельности следственных подразделений ОВД РФ, поскольку устанавливают национальные процессуальные аспекты в области сбора, легализации, передачи доказательств по преступлениям в сфере информационных технологий, которые имеют особенности, связанные с обеспечением сохранности и неизменности доказательств на таких носителях. Также, указанные правовые акты регламентируют особенности проведения оперативно-розыскных мероприятий по изъятию данных из автоматизированных информационных систем, что имеет принципиальное значение для последующей оценки таких доказательств правоохранительными органами.

Одним из основополагающих нормативно-правовых актов, регламентирующим особенности внедрения и применения информационных технологий в деятельности следственных подразделений ОВД РФ является Конвенция против транснациональной организованной преступности (принята 15 ноября 2000 г. Резолюцией 55/25 на 62-м пленарном заседании 55-й сессии Генеральной Ассамблеи ООН в Нью-Йорке; с изм. от 15.11 2000 г.). Данная Конвенция, а именно п.14 в ст.18 определяет допустимые формы сотрудничества, при этом указывая, что передача запроса и ответа допускается с помощью «любых средств», также отмечается, что информация, запрашиваемая по средствам электронной связи может запрашиваться в целях получения свидетельских показаний, проведения обыска и производства выемки или ареста, осмотра объектов и участков

¹Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт. М.: Норма, 2004. С. 215.

местности, предоставления вещественных доказательств и оценок экспертов, а также выявления или отслеживания средств совершения преступлений или других предметов для целей, доказывания и т. д. В статье 20 документа среди специальных методов расследования указан такой метод, как «электронное наблюдение», под которым понимается совокупность использования таких методов оперативно-розыскных мероприятий как вторжение и использование аппаратуры внутри домов или частных строений, запись и перехват телефонных разговоров, долгосрочное наблюдение. Также, в соответствии со ст.24 Конвенции странами-участниками определена возможность использования видеосвязи для дачи свидетельских показаний и использование видеоконференц-связи при исполнении запросов о правовой помощи по уголовным делам¹.

Декларативным нормативно-правовым актом, определяющим международные принципы создания информационного общества, и регламентирующим порядок применения информационных технологий в рамках уголовного судопроизводства на международном уровне является Окинавская хартия глобального информационного общества (подписана представителями государств «Большой восьмёрки» 22 июля 2000г.)². Во исполнение положений Хартии первым стратегическим документом, определившим направления развития информационного общества в России, стала «Стратегия развития информационного общества в Российской Федерации, утвержденная Президентом РФ»³.

Положения Конвенции о защите физических лиц при автоматизированной обработке персональных данных (заключена в г. Страсбурге 28 января 1981г.) имеют также важное значение в сфере регламентации особенностей внедрения, применения и использования

¹ «Конвенция против транснациональной организованной преступности» от 15 ноября 2000 г. // СЗ РФ. 2004. № 40. Ст. 3882.

²Окинавская хартия глобального информационного общества от 22 июля 2000 г. // Дипломатический вестник. 2000 г. № 8.

³ Указ Президента РФ «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» от 9 мая 2017г. № 203 // СЗ РФ.2017. № 20. Ст. 2901.

информационных технологий в деятельности следственных подразделений ОВД РФ, поскольку устанавливают принципы и порядок защиты физических лиц при автоматизированной обработке персональных данных, а также регулируют использование при помощи информационных технологий странами участниками Конвенции персональных данных физических лиц¹.

По-нашему мнению, представленные международные правовые акты выступают правовой базой для национального законодательства государства в области внедрения и применения информационно-цифровых технологий в деятельности правоохранительных органов Российской Федерации.

Прежде чем перейдём к характеристике нормативно-правовых актов Российской Федерации, призванных регламентировать особенности внедрения, применения и использования информационных технологий в деятельности указанного подразделения необходимо отметить, что отечественное законодательство в данной области обладает достаточно обширной нормативно-правовой базой. Так, в настоящее время на территории РФ действуют более 40 федеральных законов в области информации, более 80 актов президента, около 200 актов Правительства в России, обеспечивающие правовые основы информационного общества.

Приведём характеристику основных нормативно-правовых актов, регламентирующих процессы цифровизации деятельности следственных подразделений ОВД РФ:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» является одним из нормативно-правовых актов, регулирующих отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации при применении информационных технологий, а также при обеспечении защиты информации, в частности при проведении оперативно-розыскных мероприятий и производстве

¹ «Конвенция о защите физических лиц при автоматизированной обработке персональных данных» от 28 января 1981 г. //СЗ РФ. 2014. № 5.Ст.419.

следственных действий. Данный федеральный закон также содержит легальное определение «информационной технологии», под которой следует понимать «процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов»¹;

2. Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» примечателен тем, что впервые провозгласил основным принципом деятельности полиции принцип использования достижений науки и техники, современных технологий и информационных систем, тем самым положив основу создания единой системы информационно-аналитического обеспечения деятельности МВД России и законодательно закрепил возможность использование инновационных процессов в правоохранительной деятельности. Также, федеральный закон закрепил положение, в соответствии с которым полиция Российской Федерации имеет право на использование технических средств, включая средства аудио-, фото- и видеофиксации в рамках осуществления документирования обстоятельств совершения преступлений, административных правонарушений, обстоятельств происшествий, в том числе в общественных местах, а также для фиксирования действий сотрудников полиции, выполняющих возложенные на них обязанности²;

3. Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» имеет важное значение, поскольку регламентирует особенности внедрения, применения и использования информационных технологий непосредственно следственными подразделениями ОВД в процессе производства оперативно-розыскных мероприятий в целях расследования и раскрытия преступлений, а также обеспечения общественной безопасности. Так, в соответствии со ст.6

¹ Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 № 149-ФЗ // СЗ РФ. 2006. № 31. Ст. 3448.

² Федеральный закон «О полиции» от 7 февраля 2011 г. № 3-ФЗ // СЗ РФ. 2011. № 25. Ст. 900.

указанного федерального закона в ходе проведения оперативно-розыскных мероприятий используются информационные системы, видео- и аудиозапись, кино- и фотосъемка, а также другие технические и иные средства, не наносящие ущерба жизни и здоровью людей и не причиняющие вреда окружающей среде. Указанный законодательный акт определяет условия и порядок и ограничения применения цифровых технологий непосредственно в рамках осуществления оперативно-розыскной деятельности¹;

4. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи». Указанный правовой акт регламентирует правовые основы деятельности в области связи, как на территории Российской Федерации, так и на находящихся под юрисдикцией Российской Федерации территориях. Также, определяет полномочия органов государственной власти в области связи, в том числе правоохранительных органов в лице следственных подразделений ОВД РФ, а также определяет права и обязанности лиц, участвующих в указанной деятельности или пользующихся услугами связи²;

5. Указ Президента РФ от 1 сентября 1995 г. № 891 «Об упорядочении организации и проведения оперативно-розыскных мероприятий с использованием технических средств» устанавливает положения, в соответствии с которыми оперативно-розыскные мероприятия, связанные с подключением к стационарной аппаратуре предприятий, учреждений и организаций независимо от форм собственности, физических и юридических лиц, предоставляющих услуги связи осуществляются непосредственно в интересах следственных подразделений ОВД РФ при отсутствии необходимых оперативно-технических средств органов ФСБ России³;

6. Постановление Правительства РФ от 10 марта 2000 г. № 214 «Об утверждении Положения о ввозе в Российскую Федерацию и вывозе из

¹ Федеральный закон «Об оперативно-розыскной деятельности» от 12 августа 1995 г. № 144-ФЗ // СЗ РФ. 1995. № 33. Ст. 3349.

² Федеральный закон «О связи» от 7 июля 2003 г. № 126-ФЗ // СЗ РФ. 2003. № 28. Ст. 2895.

³ Указ Президента РФ «Об упорядочении организации и проведения оперативно-розыскных мероприятий с использованием технических средств» от 1 сентября 1995 г. № 891 // СЗ РФ. 1999 г. № 24. Ст. 2954.

Российской Федерации специальных технических средств, предназначенных для негласного получения информации, и списка видов специальных технических средств, предназначенных для негласного получения информации, ввоз и вывоз которых подлежат лицензированию». Согласно данному Положению решение о возможности ввоза в Российскую Федерацию или же вывоза из Российской Федерации специальных технических средств принимается Центром по результатам экспертизы предоставляемой заявителем документации, а также данным Положением регламентированы особенности и порядок осуществлений такой процедуры¹.

Отметим также, что влияние процесса цифровизации нашло отражение в директивных документах стратегического планирования социально-экономического развития страны, в которых сформулированы национальные цели и задачи, предусматривающие грядущие масштабные преобразования во всех сферах деятельности. Среди таких документов можно выделить «Стратегию развития информационного общества на 2017–2030 годы» (утв. Указом Президента РФ от 9 мая 2017 г. № 203), «Национальную стратегию развития искусственного интеллекта на период до 2030 года» (утв. Указом Президента РФ от 10 октября 2019 г. № 490)².

«Стратегия развития информационного общества на 2017–2030 годы» определяет цели, задачи и меры по реализации внутренней и внешней политики Российской Федерации в сфере применения информационных и коммуникационных технологий. По мнению законодателя внедрение новейших информационных и коммуникационных технологий способствует развитию информационного общества, формированию национальной

¹Постановление Правительства РФ «Об утверждении Положения о ввозе в Российскую Федерацию и вывозе из Российской Федерации специальных технических средств, предназначенных для негласного получения информации, и списка видов специальных технических средств, предназначенных для негласного получения информации, ввоз и вывоз которых подлежат лицензированию» от 10 марта 2000 г. № 214 // СЗ РФ. 2000 г. № 12. Ст.1292.

²Указ Президента РФ «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») от 10 октября 2019 г. № 490 // СЗ РФ.2019. № 27. Ст. 2987.

цифровой экономики, а также обеспечивает национальные интересы и реализацию стратегических национальных приоритетов. Особый интерес в документе представляют положения о «критической информационной инфраструктуре» России. К ней, в частности, относятся информационные системы, телекоммуникационные сети и автоматизированные системы управления технологическими процессами, которые используются государственными органами, а также в сферах обороны, здравоохранения, транспорта, связи, финансов, энергетики и в различных отраслях промышленности. Эту инфраструктуру, как отмечается в Стратегии, необходимо защищать «с использованием государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы»¹. «Национальная стратегия развития искусственного интеллекта на период до 2030 года» (утв. Указом Президента РФ от 10 октября 2019 г. №490) представляет собой документ, призванный обеспечить, прежде всего, ускоренное развитие искусственного интеллекта, проведение научных исследований в этой области, повышение доступности информации и вычислительных ресурсов для пользователей, а также совершенствование системы подготовки кадров в данной сфере². Так, одной из приоритетных задач в настоящее время является разработка и утверждение федерального проекта «Искусственный интеллект», что по нашему мнению является достаточно актуальной задачей, поскольку деятельность ОВД РФ в настоящее время сопряжена с большим объёмом как получаемой, так и хранящейся в различных базах данных информацией. Развитие компьютерных технологий привело к появлению широкого спектра преступлений, связанных с незаконным доступом к информации и её использованием. Например, создание и распространение вредоносных компьютерных программ, организация DDOS-атак; хищения денежных

¹Зуев С.В. Цифровизация судопроизводства. Научно-практический (постатейный) комментарий правовых актов. М.: Юрлитинформ, 2020. С.61.

²Там же. С.62.

средств кредитных и иных организаций, а также их клиентов; мошенничество¹. В связи с этим становится актуальным вопрос о внедрении в деятельность следственных подразделений ОВД систем искусственного интеллекта, которые смогли бы систематизировать всю имеющуюся информацию, адаптироваться к задаваемым параметрам и самостоятельно выполнять те задачи, которые раньше были под силу только человеку.

Указанные выше нормативно-правовые акты отечественного законодательства имеют принципиальное значение в деятельности следственных подразделений ОВД РФ, поскольку устанавливают основополагающие правовые положения, касающиеся применения следователем информационных технологий в процессе работы: устанавливают критерии работы, порядок, права и ограничения по внедрению и применению информационно-цифровых технологий.

Говоря о нормативно-правовой регламентации внедрения и применения информационных технологий в деятельности следственных подразделений ОВД РФ интересен также опыт зарубежных стран, касательно правовой регламентации информационно-цифровых технологий в деятельности органов правопорядка.

Наибольшей базой нормативных правовых актов, регламентирующих особенности внедрения, применения и использования информационных технологий в деятельности органов правопорядка обладают США². Основным источником американского права в указанной области выступает прецедентное право, статуты, руководства, правила судопроизводства. Так, первый федеральный закон США, предназначенный для перехвата электронных сообщений (Electronic Communications Privacy Act – ECPA) был принят ещё в 1986 г., который позднее был усовершенствован принятием нового законопроекта под названием «О сплочении и укреплении Америки

¹ Давыдов В.А., Качалова О.В. Современные тенденции развития российского уголовного судопроизводства // Вестник Томского государственного университета. 2018. № 29. С.78.

² Смарин В.И., Луцик В.В. Уголовный процесс европейских государств: монография. М.: Проспект, 2018. С.178.

путем обеспечения надлежащими средствами, требуемыми для пресечения и воспрепятствования терроризму» принятый после теракта в 2001 г., который внёс значительные изменения в регламентацию внедрения, применения и использования информационных технологий¹. Закон «О внешней разведке США», принятый в 1978 г. со значительными изменениями 2008 г. значительно расширил права правоохранительных органов США в рамках использования информационных технологий в части контрразведывательной деятельности и других целей².

В Великобритании же основополагающим нормативным правовым актом, регулирующим вопросы интеграции информационных технологий в деятельность правоохранительных органов является Статут «Об использовании компьютера в противоправных целях», в котором закреплены уголовно-правовые нормы, устанавливающие элементы различных компьютерных преступлений в сфере компьютерной информации³. В ст.10 указанного документа закреплены уголовно-процессуальные положения, регламентирующие обыск, изъятие цифровой доказательственной информации, полномочия органов расследования. Ассоциация руководителей полиции Англии, Уэльса и Северной Ирландии имеют в своём распоряжении «Руководство для работы с цифровыми доказательствами»⁴.

В Германии главным нормативным документом, который регламентирует вопросы обеспечения информационной безопасности государства, является «Основной закон Федеративной Республики Германия» или Конституция Германии, принятый 8 мая 1949 г. и закрепляющий основы правовой и политической системы страны. В июле 2015 г. в Германии был принят «Акт об информационной безопасности»

¹ Зуев С.В. Развитие информационных технологий в уголовном судопроизводстве. М.: Юрлитинформ, 2018. С.46.

² Дремлюга Р.И. Компьютерная информация как предмет посягательства при неправомерном доступе: сравнительный анализ законодательства США и России // Журнал зарубежного и сравнительного правоведения. 2018. № 6 (73). С. 87.

³ Зуев С.В. Развитие информационных технологий в уголовном судопроизводстве. С.54.

⁴ Трефилов А.А. Уголовный процесс зарубежных стран. М.: НИПКЦ Восход-А, 2019. С.345.

(IT SecurityAct), целью которого является предотвращение ущерба важнейшим ИТ-системам, таким, например, как системы Министерства внутренних дел (BSI), провайдеров телекоммуникационных услуг, операторов критически важных элементов инфраструктуры и др. В настоящее время, BSI занимается реализацией положений этого Акта, который включает в себя минимальные стандарты кибербезопасности для более 2000 критически важных инфраструктурных компаний¹.

Анализируя нормативно-правовые акты зарубежного законодательства в области цифровизации можно прийти к выводу о том, что темпы развития информационных технологий в каждой стране имеют свои особенности, что связано уровнем научно-технического и экономического прогресса, а также состоянием правовой системы в государстве.

Таким образом, рассмотренный в параграфе перечень нормативных правовых актов, безусловно, не является исчерпывающим, нами были озвучены наиболее значимые международные и отечественные нормативно-правовые акты, касающиеся применения цифровых технологий в деятельности следственных подразделений ОВД РФ. Отметим, что цифровизация становится ключевым фактором прогрессивного развития любого государства. На сегодняшний день в Российской Федерации происходит переход от внедрения цифровых технологий к комплексному построению цифровой системы в масштабах всей страны, поэтому немаловажное значение приобретает нормативно-правовая регламентация данного процесса в целях оптимизации деятельности сотрудников правоохранительных органов, а также защиты законных прав и свобод граждан. Представленный в работе перечень основных международных нормативно-правовых актов по нашему мнению является правовой базой для национального законодательства государства, в области внедрения

¹Муратова Н.Г., Сергеев М.С. Правовое регулирование применения электронной информации и электронных носителей информации в уголовном судопроизводстве: отечественный и зарубежный опыт: монография. М., Юрлитинформ, 2019. С.168.

и применения информационных технологий в деятельности правоохранительных органов, в том числе следственных подразделений ОВД.

Непосредственно практическое значение нормативно-правовых актов, например Конвенции против транснациональной организованной преступности, Окинавской хартии глобального информационного общества, Декларации принципов «Построение информационного общества и др. для деятельности следователей заключается в том, что они представляют собой стандарты применения механизмов и процедур, связанных с процессами цифровизации в правоохранительной деятельности.

Важное значение, безусловно, имеют и нормативно-правовые акты отечественного законодательства, поскольку следователь в процессе применения информационных технологий непосредственно руководствуется положениями, закрепленными в федеральных законах, постановлениях Правительства РФ, Указах Президента РФ, кодексах, а также в ведомственных инструкциях и регламентах.

Говоря о процессах цифровизации очевидным является тот факт, что зарубежные страны обладают большей, более развитой правовой базой в этой сфере. В связи с чем полагаем, что для отечественного правоприменителя, безусловно, интерес вызывает законодательство зарубежных стран, в частности США, Великобритании, Германии, как с точки зрения правового анализа, так и возможного правопреемства.

По-нашему мнению, внедрение в деятельность следственных подразделений ОВД системы, работающей по принципу искусственного интеллекта, позволило бы оптимизировать данный вид деятельности, в частности, облегчить работу с массивом нормативно-правовых актов.

1.2 Анализ уголовно-процессуального законодательства по применению информационных технологий в деятельности следственных подразделений органов внутренних дел

Современное общество трудно представить безпередовых информационных технологий, которые находят свое применение во всех сферах общественной жизни, в том числе правоохранительной. На сегодняшний день становится очевидным, что эффективность борьбы с преступностью находится в прямой зависимости от информационно-технологического обеспечения органов правопорядка. При этом именно уголовно-процессуальное законодательство имеет наиболее важное, принципиальное значение в регламентации порядка использования информационных технологий в деятельности следственных подразделений ОВД РФ.

Говоря об особенностях регулирования уголовно-процессуальным законодательством порядка использования информационных технологий в деятельности ОВД РФ необходимо отметить, что под информационными технологиями в уголовном процессе следует понимать, прежде всего, «определенную совокупность средств, приемов и методов собирания (поиска, обнаружения, фиксации, изъятия), обработки и передачи первичной информации о расследуемом событии для получения доказательств, позволяющих в ходе производства по уголовному делу устанавливать наличие или отсутствие обстоятельств, подлежащих доказыванию, а также иных обстоятельств, имеющих значение для расследования конкретного преступления»¹.

УПК РФ от 18 декабря 2001 г. № 174-ФЗ представляет собой правовой акт, который содержит нормативные предписания в части применения информационно-технических средств в процессе осуществления предварительного расследования по делу и в ходе уголовного судопроизводства². Отметим, что на сегодняшний день происходит

¹ Медведева М.О. Уголовно-процессуальная форма информационных технологий: современное состояние и основные направления развития: дис. ... канд.юрид.наук. С.76.

² Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 177-ФЗ // СЗ РФ. 2001. № 51. Ст. 4921; Зуев С.В. Цифровизация судопроизводства. Научно-практический (постатейный) комментарий правовых актов. С.66.

совершенствование правового регулирования информационного обеспечения уголовного процесса, поскольку содержащиеся в УПК РФ положения о применении информационных и технических средств не соответствуют современным реалиям, к примеру, многие моменты не учтены и остаются без практического применения. В подтверждение представленной точки зрения перейдём к детальной характеристике норм УПК РФ, регламентирующих особенности порядка применения информационных технологий и технических средств.

Анализируя действующий УПК РФ можно выделить несколько видов правовых норм, характеризующих применение информационных технологий и технических средств. Во-первых, это уголовно-процессуальные нормы, регламентирующие порядок использования информационных технологий и технических средств в ходе производства следственных действий.

Во-вторых, уголовно-процессуальные нормы, касающиеся обеспечения участников уголовного судопроизводства возможностью использования технических средств в целях ознакомления с материалами уголовного дела. В-третьих, процессуальные нормы, определяющие возможность использования технических средств следователями для изготовления процессуальных документов по делу. И, наконец, нормы, содержащие правовую регламентацию порядка использования технических средств в судах первой, апелляционной и кассационной инстанции.

Перейдём к детальному анализу уголовно-процессуальных норм, регламентирующих порядок использования информационных технологий и технических средств в процессе производства следственных действий. В соответствии с ч.6 ст.164 УПК РФ при производстве следственных действий могут применяться технические средства и способы обнаружения, фиксации и изъятия следов преступлений и вещественных доказательств. Также, в соответствии с ч.2 ст.166 УПК РФ допускается применение при производстве следственного действия дополнительных способов фиксации получаемой

информации, например стенографирование, аудио- и видеозапись. При этом, согласно ч.1.1 ст. 170 УПК РФ, применение технических средств фиксации может стать альтернативой приглашению понятых при проведении следственных действий, например, при производстве осмотра (ст. 177 УПК РФ), эксгумации (ст. 178 УПК РФ), следственного эксперимента (ст.181 УПК РФ), допроса (ст.189 УПК РФ) и др. Остановимся на детальной характеристике возможностей использования информационно-технических средств в рамках осуществления следственных действий, предусмотренных УПК РФ.

Так, при производстве такого следственного действия, как допрос (ст. 187–191 УПК РФ), в соответствии с ч.4 ст. 189 УПК РФ по инициативе следователя или по ходатайству допрашиваемого лица в ходе допроса могут быть проведены фотографирование, аудио- и (или) видеозапись, киносъемка, материалы которых хранятся при уголовном деле и по окончании предварительного следствия опечатываются. Указанная норма определяет возможность применения следователем технических средств в рамках проведения следственного действия¹. Частью 4 статьи 190 УПК РФ названа одна из форм использования в процессе допроса среди всех прочих доказательств «воспроизведение материалов аудио- и (или) видеозаписи, киносъемки следственных действий». При производстве данных источников доказательств обязательно применение технических средств, соответственно при этом должны выполняться все предписания УПК РФ, касающиеся применения технических средств². В соответствии с ч.6 ст.192 УПК РФ при производстве очной ставки соблюдаются общие правила, установленные для допроса участвующих в ней лиц. Так, ч.4 ст.192 УПК РФ указывает на возможность оглашения показаний допрашиваемых лиц посредством их воспроизведения через аудио-и (или) видеозаписи, киносъемки этих

¹ Зуев С.В. Цифровизация судопроизводства. Научно-практический (постатейный) комментарий правовых актов. С.69.

²Зазулина А.И. Правовые и методологические основы использования цифровой информации в доказывании по уголовным делам: дис. .. канд. юрид. наук. Екатеринбург, 2018. С.178.

показаний. Предъявление для опознания также, по мнению законодателя, может осуществляться с использованием специальных технических средств. Так, ч.5 ст. 193 УПК РФ указывает, что при невозможности предъявления лица опознание может быть произведено по его фотографии, предъявляемой одновременно с фотографиями других лиц, внешне сходных с опознаваемым лицом.

В подтверждение представленной нами точки зрения, относительно отсутствия в действующей редакции УПК РФ норм, регламентирующих особенности порядка применения информационных технологий и технических средств приведем следующий пример.

Одним из распространенных следственных действий является осмотр места происшествия, который, как правило, носит неотложный характер и «состоит в непосредственном изучении следователем и другими участниками осмотра обстановки места происшествия, в обнаружении, фиксации и изъятии следов и других вещественных доказательств в целях выяснения обстоятельств, имеющих значение для дела» (ст.176–177 УПК РФ). Однако, анализируя нормы УПК РФ, регламентирующие порядок осуществления осмотра, в том числе осмотра места происшествия, указание на возможность использования информационных и технических средств, например, таких как аудио, видео и фотосредства, а также технологии глобального позиционирования (ГЛОНАСС, GPS), позволяющие наиболее точно определить местоположение объектов вовсе отсутствует. По мнению А.И. Леонова и П.Г. Смагина «применение технологий трехмерной фото-и видеофиксации обстановки места производства следственного действия, связанного с осмотром, несомненно, сможет вывести на новый уровень процесс доказывания по уголовным делам»¹. Тем самым, можно говорить о том, что нормы действующего УПК РФ настоятельно требуют

¹ Ленов А.И., Смагин П.Г. Использование информационных технологий при производстве следственных действий, в том числе связанных с ограничением конституционных прав граждан // Вестник Тамбовского университета. 2011. № 9 (101). С.349.

совершенствования с учётом развития правоприменительной практики, в том числе, необходимо также учитывать технический прогресс, который подразумевает внедрение и применение информационных средств повсеместно, в частности, и в процессе осуществления предварительного расследования по делу.

Говоря о характеристике уголовно-процессуальных норм в области обеспечения участников уголовного судопроизводства возможностью применять технические средства для ознакомления с материалами уголовного дела, укажем, что данную группу норм регламентируют положения статей УПК РФ, касающиеся обеспечения осуществления права потерпевшего (ст.42 УПК РФ), обвиняемого (ст.47 УПК РФ), специалиста (ст.58 УПК РФ), защитника (ст.53 УПК РФ), а также иных участников уголовного судопроизводства знакомиться в рамках представленных полномочий с материалами уголовного дела при помощи технических средств. Под техническими средствами в данном случае следует понимать средства фиксации и копирования информации, такие как фото, видеосъемка, печать, копирование, сканирование материалов. Указанные нормы регламентируют лишь общий порядок, только указывают на право использовать те или иные технические средства. Тем самым мы видим, что в УПК РФ прослеживается тенденция отсутствия детальной регламентации применения информационных и технических средств.

К нормам УПК РФ, определяющим возможность использования технических средств следователем в целях изготовления процессуальных документов по делу можно отнести положение ч.2 ст.166 УПК РФ, в соответствии с которой протоколы следственных действий могут быть написаны либо от руки, либо могут быть изготовлены с помощью технических средств. Применяться такие средства могут также в рамках выполнения организационной работы. В УПК РФ под информационными и технологиями и техническими средствами понимается, прежде всего, средства организационной техники, такие как компьютеры, пишущие

машинки и иные печатающие устройства, позволяющие изготавливать письменный текст на материальном носителе¹.

Наряду с нормативным регулированием применения информационно-технических средств в ходе предварительного расследования по делу, в УПК РФ содержатся также нормативные предписания относительно их применения в судебных стадиях уголовного судопроизводства². Так, в ч. 1 ст.259 УПК РФ содержится указание о том, что в ходе судебного заседания судов первой и апелляционной инстанций составляется протокол в письменной форме и ведется протоколирование с использованием средств аудиозаписи (аудиопротоколирование). Также, ч.2 ст.259 УПК РФ указывает на возможность изготовления протокола судебного заседания на пишущей машинке или компьютере, при этом для обеспечения полноты протокола при его ведении могут быть использованы стенографирование, а также иные технические средства. Об использовании технических средств в процессе фиксирования хода судебного заседания в протоколе делается отметка, а соответствующие носители информации приобщаются к материалам уголовного дела. Указанное правило предусмотрено ч.5 ст.259 УПК РФ среди прочих обязательных требований к протоколу судебного заседания, а также изложено в Инструкции по делопроизводству в районном суде. В соответствии с ч.2 ст. 303 УПК РФ приговор также может быть изготовлен с помощью технических средств. Иные процессуальные документы, на основании ч.2 ст.474 УПК РФ также могут быть выполнены типографическим, электронным или иным способом, а согласно ч. 5 ст. 241 УПК РФ все лица, присутствующие на открытом судебном заседании, вправе с разрешения председательствующего судьи осуществлять фото, киносъемку и (или) видеозапись. Статья 474.1. УПК РФ устанавливает, что ходатайства, заявления, жалобы и представления могут

¹ Тарасов М.А. О некоторых проблемах правового регулирования применения технических средств в уголовном судопроизводстве // Вестник Южно-Уральского государственного университета. 2009. № 40 (173). С.71.

² Там же. С.72

быть поданы в суд в форме электронного документа, подписанного лицом, направившим такой документ электронной подписью в соответствии с законодательством Российской Федерации. К ходатайству (заявлению, жалобе или представлению) могут прилагаться материалы в форме электронных документов.

Анализируя представленные нормативные положения, регулирующие применение информационных и технических средств в ходе судебного заседания необходимо отметить что, их применение на различных стадиях уголовного судопроизводства носит не урегулированный характер. УПК РФ предусматривает лишь наиболее общие положения по их применению в рамках уголовного судопроизводства, однако, как и было отмечено нами ранее детальная регламентация отсутствует. Примером может служить аудиопотоколирование в зале судебного заседания. В данном случае неясность вносит положение ч. 5 ст. 259 УПК РФ, указывающая, что если в ходе судебного разбирательства проводились «фотографирование, аудио-и (или) видеозапись, киносъемка допросов», то об этом делается отметка в протоколе судебного заседания, а полученные результаты применения технических средств прилагаются к материалам уголовного дела». Положение данной статьи представляется не вполне понятным, поскольку не ясно, почему положение касается только допросов и имеется ли отношение к аудиозаписи, полученной лицами, присутствующими на судебном заседании¹.

В действующем УПК РФ предусмотрен и процессуальный порядок использования электронных доказательств в уголовном судопроизводстве. В соответствии со ст.82 УПК РФ ввиду особой специфики таких доказательств, как электронные носители информации уголовно-процессуальное законодательство регламентирует порядок их

¹ Зуев С.В. Развитие информационных технологий в уголовном судопроизводстве. С.146.

хранения в рамках производства по уголовному делу¹. Под электронным носителем информации следует понимать внутренний накопитель на жестком магнитном диске, оптические диски различных видов, магнитно-оптические диски, карты памяти различных форматов, USB, флеш-накопители, гибкие магнитные диски, интегральная микросхема памяти, оперативное запоминающее устройство ЭВМ, постоянное программируемое запоминающее устройство ЭВМ, оперативное запоминающее устройство периферийных устройств и иные носители². По мнению ряда исследователей, электронные доказательства (флеш-накопители, электронные письма на почте, телефоны и др.) следует регулировать специальными нормами УПК РФ³.

Из вышесказанного можно сделать вывод о том, что действующее уголовно-процессуальное законодательство требует совершенствования по вопросам регулирования порядка применения информационных технологий и технических средств в деятельности следственных подразделений ОВД РФ. Несмотря на то, что в контексте закона неоднократно встречаются формулировки, касающиеся технических средств, а также в УПК РФ содержатся и другие упоминания об использовании технических, информационных, коммуникационных и иных средств без установления их понятийного значения, тем не менее, в ст.5 УПК РФ отсутствует понятие информационных технологий и технических средств. Отсутствует и прямое упоминание о компьютере. Предполагаем, что отсутствие необходимых формулировок приводит к затруднительной оценке порядка применения указанных средств в правоохранительной деятельности⁴. Так, по мнению А.Е. Федюнина «Отсутствие единого понимания сущности технических

¹ Зуев С.В., Черкасов В.С. Новые правила изъятия электронных носителей и копирования информации // Законность. 2019. № 5 (1015). С. 42.

² Медведева М.О. Уголовно-процессуальная форма информационных технологий: современное состояние и основные направления развития: дис. ... канд.юрид.наук. С.76

³ Олиндер Н.В. К вопросу о доказательствах, содержащих цифровую информацию // Юридический вестник Самарского университета. 2017. № 3. С. 108.

⁴ Зуев С.В. Основы теории электронных доказательств. М.: Юрлитинформ, 2019, С. 34.

средств, применяемых в сфере уголовного судопроизводства, неопределенность их правового статуса и порядка использования в уголовно-процессуальной деятельности влекут за собой не только неясность нормативно-правовых формулировок, но и негативно сказываются на качестве дознания, предварительного следствия и судебного разбирательства уголовных дел»¹. Считаем также, что уголовно-процессуальное законодательство в области регулирования информационных технологий и технических средств носит пока лишь фрагментарный и непоследовательный характер, а содержащиеся в УПК РФ положения применении информационных технологий и технических средств не соответствуют современному уровню развития информационных технологий. Согласимся с мнением А.А. Сарапулова, который считает, что «в действующем УПК РФ многие моменты не учтены и остаются без практического применения, отсутствуют общие положения об использовании информационных технологий, само понятие технических средств, критерии допустимости использования технических средств за редкими исключениями также не находят своего отражения в процессуальном законодательстве»². Так, УПК РФ содержит лишь общее указание на возможность их использования в рамках проведения следственных действий. Это же касается как порядка использования информационных технологий на разных стадиях уголовного судопроизводства, так и порядка использования электронных доказательств в уголовном судопроизводстве.

Предполагаем, что необходимо дополнить УПК РФ рядом норм, конкретизирующих порядок использования правоохранительными органами информационных технологий и технических средств в рамках осуществления досудебного производства по делу и на стадии судебного рассмотрения дела.

¹ Федюнин А.Е. Правовое регулирование технических средств в уголовном процессе: автореф. дис. ... докт.юрид.наук.Саратов,2008. С.31.

² Сарапулов А.А. Информационные технологии в уголовном процессе: история, современное состояние, перспективы //Вестник Южно-Уральского государственного университета. 2013. № 2.С.107.

Порядок применения электронного документооборота должен быть урегулирован законом. Важность должного правового регулирования уголовно-процессуальных отношений, возникающих в процессе доказывания с применением цифровых технологий, заключается в том, что ненадлежащий характер такого регулирования влечет за собой определенные правовые последствия, в том числе признание доказательств недопустимыми, а в конечном итоге – возможность освобождения виновного лица от уголовного преследования.

По-нашему мнению, развитие уголовно-процессуального законодательства в данной области можно реализовать в следующем направлении: совершенствование УПК РФ, путём внесения нормативных положений, касающихся детальной регламентации порядка применения информационных технологий и технических средств, как в процессе осуществления предварительного расследования по делу, так и в ходе судебного заседания. Представленную нами точку зрения разделяют и действующие сотрудники следственных подразделений ОВД РФ. Так, по итогам проведённого нами социологического опроса среди сотрудников Отдела по расследованию преступлений на территории, обслуживаемой отделом полиции «Центральный» СУ УМВД России по г. Челябинску 81,25% респондентов поддержали нашу точку зрения и всего лишь 6,25% высказались против (анкета и результаты проведённого социологического опроса представлены в Приложении № 1 и Приложении № 2 к выпускной квалификационной работе).

Выводы по первой главе. В настоящее время цифровизация становится ключевым фактором прогрессивного развития любого государства. Процессы цифровизации затрагивают различные сферы жизнедеятельности человека: здравоохранение, экономику, социальную сферу, политику и многие другие. Влияние процессов цифровизации на правоохранительную деятельность имеет принципиальное значение, поскольку преследует своей целью повышение эффективности раскрываемости и предотвращения совершения

преступлений и правонарушений, а также оптимизацию деятельности сотрудников правоохранительных органов, защиты законных прав и свобод граждан, что в конечном итоге способствует уменьшению уровня преступности в государстве.

Говоря о цифровизации деятельности следственных подразделений ОВД РФ немаловажное значение приобретает в первую очередь, правовая основа использования информационных технологий, поскольку она представляет собой определенные стандарты и принципиальные положения, влияющие на процесс цифровизации в целом. На сегодняшний день правовую основу использования информационных технологий и технических средств в деятельности следственных подразделений ОВД РФ составляют как нормативно-правовые акты отечественного, так и международного законодательства.

Указанный нами в работе перечень нормативно-правовых актов в области международного законодательства представляют собой стандарты применения механизмов и процедур, связанных с процессами цифровизации в правоохранительной деятельности, а также являются правовой базой для национального законодательства государств области внедрения и применения информационных технологий и технических средств (Декларация принципов «Построение информационного общества – глобальная задача в новом тысячелетии», «План действий», Конвенция против транснациональной организованной преступности и др).

Акты отечественного законодательства, представленные федеральными законами, указами Президента РФ, кодексами, ведомственными инструкциями и регламентами, постановлениями Правительства РФ выполняют также важную роль в процессе правового регулирования информационных технологий, поскольку сотрудник следственного отдела в процессе применения информационных технологий и технических средств непосредственно руководствуется положениями, закрепленными в актах отечественного законодательства.

Немаловажная роль в нормативном регулировании порядка использования информационных технологий и технических средств отводится нормам уголовно-процессуального законодательства, регламентирующего применение информационно-технических средств как в процессе досудебного производства по делу, так и в судебном порядке.

Уголовно-процессуальное регулирование порядка применения информационных и технических средств на сегодняшний день носит фрагментарный и непоследовательный характер, отсутствуют общие положения об использовании информационных технологий, само понятие технических средств, критерии допустимости использования технических средств, конкретные информационные технологии также не находят своего отражения в УПК РФ. Отсутствие необходимых формулировок приводит к затруднительной оценке порядка использования информационно-технических средств следственными подразделениями ОВД РФ. В связи с чем немаловажное значение приобретает модернизация УПК РФ – разработка уголовно-процессуальных норм, регламентирующих порядок применения информационно-технических средств правоохранительными органами. Порядок применения электронного документооборота также должен быть урегулирован законом.

Считаем, что действующий УПК РФ, необходимо дополнить рядом нормативных положений, касающихся детальной регламентации порядка применения информационных технологий и технических средств, как в процессе осуществления предварительного расследования по делу, так и в ходе судебного заседания. Полагаем, что внедрение в деятельность следственных подразделений ОВД системы, работающей по принципу искусственного интеллекта позволило бы облегчить работу с массивом нормативно-правовых актов.

2 ОСОБЕННОСТИ ПРИМЕНЕНИЯ СЛЕДСТВЕННЫМИ ПОДРАЗДЕЛЕНИЯМИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ЦИФРОВЫХ ТЕХНОЛОГИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

2.1 Организация процесса расследования преступлений следственными подразделениями органов внутренних дел с использованием информационных технологий

Технологический прогресс, появление новейших информационных технологий, а также их развитие привело к тому, что на сегодняшний день уровень киберпреступности значительно возрос. Под киберпреступлениями следует понимать деяния, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Так, согласно статистическим данным за январь 2021 года рост общего количества зарегистрированных тяжких и особо тяжких преступлений (на 2,4%) обусловлен тем, что значительная часть криминальных деяний совершается с применением IT-технологий. В отчётном периоде их зарегистрировано на 32,2% больше, чем год назад, в том числе с использованием сети «Интернет» – на 51,3% и при помощи средств мобильной связи - на 39%. Если в январе 2020 года удельный вес преступлений в сфере информационных технологий составлял 17,7%, то в первом месяце текущего года он увеличился до 25%. При этом около половины преступлений в ИТ-сфере составляют мошенничества, в том числе с банковскими картами. Отметим также, что на фоне роста киберпреступлений имеет место тенденция снижения уровня раскрываемости преступлений правоохранными органами (в среднем на 2%), что является следствием вновь организующихся форм преступлений в этой области и недостатком применения мер по противодействию им¹.

¹ Информационно-аналитический портал правовой статистики Генеральной прокуратуры РФ. URL: <http://crimestat.ru/analytics> (дата обращения: 16.04.2021).

Итак, учитывая рост преступлений, связанных с использованием информационных технологий, а также имеющиеся недостатки в области противодействия таким преступлениям становятся актуальными вопросы, касающиеся организации процесса расследования преступлений с применением информационных технологий.

Говоря об организации процесса расследования преступлений с использованием информационных технологий необходимо отметить, что одним из направлений повышения качества правоохранительной деятельности является совершенствование информационного обеспечения предварительного расследования преступлений, понятие и сущность которого определяются характером и видом этой деятельности. Для каждой службы информационное обеспечение имеет свое назначение¹. Под информационным обеспечением предварительного расследования преступлений по мнению А.М. Ишина следует понимать «деятельность ряда подразделений и служб ОВД (следственных, оперативных и неоперативных аппаратов), направленная на получение из гласных и негласных источников криминалистически значимой информации, ее хранение, обработка, передача и использование в целях раскрытия и расследования преступлений»².

В настоящее время следователи ОВД РФ в процессе расследования преступлений применяют различные информационные и технические средства³. Информационные технологии, применяемые следователем в процессе организации расследования преступлений ставят своей целью решение следующих задач: во-первых, организовать труд следователя; во-вторых, способствуют организации и координации деятельности следователя в процессе расследования преступлений и в-третьих, выступают

¹ Гришин Д.А. Совершенствование применения информационных технологий в досудебных стадиях уголовного судопроизводства // Вестник Московского университета МВД России. 2019. № 3. С.122.

²Ишин А.М. Информационное обеспечение предварительного расследования преступлений: некоторые современные аспекты // Вестник Балтийского федерального университета им. И. Канта. 2016. № 4. С.22.

³ Зуев С.В. IT-справочник следователя. М.: Юрлитинформ, 2019. С.64.

способом накопления и выдачи необходимой информации о совершенных преступлениях, лицах их совершивших, об изъятых с мест происшествия следах и т. п.

К информационным технологиям и техническим средствам, используемыми сотрудниками следственных подразделений ОВД в процессе расследования преступлений относятся¹:

1. Стандартные программы для ЭВМ, предназначенные для оформления материалов уголовных дел и служебной документации: текстовые и гипертекстовые редакторы (MSWord и др.); редакторы электронных таблиц (MS Excel и др.); программы обработки фото и видеоизображений (MS PowerPoint); графические редакторы (для оформления приложений к протоколам следственных действий –планов, схем и чертежей);

2. Системы, предназначенные для получения консультационной правовой помощи и генерации бланков процессуальных документов: автоматизированные справочно-правовые системы «Гарант», «КонсультантПлюс», «Кодекс» и др.; официальные сайты в сети Интернет органов государственной власти (Государственной Думы РФ, Совета Федерации РФ, Президента РФ, Правительства РФ, Верховного Суда РФ, Генеральной прокуратуры РФ, Следственного комитета РФ, Министерства внутренних дел РФ и др.)²;

3. Устройства, предназначенные для обнаружения, фиксации, изъятия, предварительного и судебно-экспертного исследования вещественных доказательств по уголовным делам: мобильный комплекс следователя для работы в полевых условиях, состоящий из компьютера «Ноутбук», стандартного или специального программного обеспечения, портативного принтера, цифровой фото- или видеокамеры со съемной «флеш-памятью»,

¹ Зуев С.В. Развитие информационных технологий в уголовном судопроизводстве. С.117–119.

сотового радиотелефона и носимой гарнитуры (для оперативного наведения справок); передвижные криминалистические лаборатории, укомплектованные компьютерной техникой со специализированным программным обеспечением и соответствующими периферийными устройствами, предназначенные для работы со следами и доказательствами определенных категорий;

4. Информационные системы, предназначенные для сокращения сроков подготовки и производства отдельных процессуальных действий: автоматизированная информационная система специального назначения («СОРМ»), предназначенная для контроля и записи переговоров; автоматизированные информационно-поисковые системы (АИПС), информационные системы глобального позиционирования и навигации (GPS, ГЛОНАСС), радиопеленгации, предназначенные для распознавания образов личности или транспортного средства, например АИПС «Безопасный город», «Поток» и др¹ .;

5. Автоматизированные информационные системы, предназначенные для проведения криминалистических исследований: информационные системы, обеспечивающие исследование следов рук («Папилон» и «Сонда-Плюс»), обуви («FootwearTraces » и «OttiskSled»), шин транспортных средств («TrunkTraces»), габитоскопические исследования («Портретная экспертиза» и «Портрет»), подделки документов («FrontlineDocumentsSystem», «Валюта», «ExpressForensic PRO»); голоса человека («Диалект», «DUMP», «ИКАРЛаб», «Камертон»), электронных доказательств («UFED», «EnCaseForensicEdition», «MOBILedit» и «Мобильный криминалист»),

¹Постановление Правительства РФ «О Межведомственной комиссии по вопросам, связанным с внедрением и развитием систем аппаратно-программного комплекса технических средств «Безопасный город» от 20 января 2014 г. № 39 // СЗ РФ. 2014 г. № 5. Ст. 498; Аппаратно-программный комплекс «Поток» // Официальный сайт ЗАО «РОССИ»: URL: <http://www.rossi-potok.ru/ru/> (дата обращения: 16.04.2021).

баллистики («Арсенал» и «ТАИС»), восстановление прижизненного облика человека по его черепу или частям черепа («Реконструкция-2»)¹;

6. Межведомственные и ведомственные компьютерные сети, предназначенные для служебной переписки по находящимся в производстве уголовным делам, получения директивных, справочно-нормативных документов и методических материалов: (Единая информационно-телекоммуникационной система органов внутренних дел (ЕИТКС ОВД), информационная система обеспечения надзора за исполнением законов в органах прокуратуры Российской Федерации (ИСОП), автоматизированный информационный комплекс «Надзор» (АИК Надзор))²;

7. Использование автоматизированного рабочего места следователя (АРМ следователя) на базе автоматизированных методик расследования отдельных видов преступлений с формированием электронного уголовного дела;

8. Информационные ресурсы Государственной автоматизированной системы Российской Федерации «Правосудие», предназначенные для поиска судебных актов, в том числе по находившимся в производстве уголовным делам о преступлениях прошлых лет;

9. Использование электронных носителей и содержащейся в их памяти компьютерной информации в качестве доказательств по уголовным делам;

10. Использование Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак

² Постановление Правительства РФ «О единой системе межведомственного электронного взаимодействия» от 8 сентября 2010 г. № 697 // СЗ РФ. 2010 г. № 38. Ст.4823; Автоматизированный информационный комплекс «Надзор» // Официальный сайт ООО «Электронные офисные системы»: URL: <https://www.eos.ru/search/?q=%C0%C8%CA+%CD%E0%E4%E7%EE%F0&s=%CF%EE%E8%F1%EA> (дата обращения 18.04.2021).

наинформационные ресурсы Российской Федерации для обеспечения борьбы с преступлениями в сфере компьютерной информации¹.

По результатам анализа имеющихся в арсенале следователей ОВД РФ информационных и технических средств, используемых в качестве вспомогательных средств в процессе осуществления предварительного расследования по делу можно сделать вывод о том, что одним из направлений повышения качества правоохранительной деятельности является совершенствование имеющегося информационного обеспечения. С учётом вышеизложенного полагаем, что основой информационного обеспечения расследования преступлений являются автоматизированные рабочие места сотрудников правоохранительных органов, объединенные в межведомственные и ведомственные информационные системы специального назначения на базе информационно-телекоммуникационных сетей².

Организация процесса расследования преступлений следственными подразделениями ОВД РФ с применением информационных технологий включает в себя различные этапы –это и обработка соответствующей документированной информации по материалам доследственной проверки или уже расследуемому уголовному делу; анализ электронных документов, например, содержащихся в централизованных базах данных розыскных и криминалистических учетов; составление различных документов как процессуального, так и не процессуального характера; проведение следственных действий и оперативно-розыскных мероприятий с применением информационных и технических средств; получение и

¹ Указ Президента РФ «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» от 15 января 2013 г. № 31 // СЗ РФ. 2013 г. № 3. Ст. 178.

² Головкин Л.В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция? // Вестник экономической безопасности. 2019. № 1. С. 17.

дальнейшее использование электронных доказательств по делу¹. К указанному нами перечню можно отнести также аналитическую работу следователя по формированию решений и заключений на основе анализа имеющейся информации, а также взаимодействие следователей с федеральными органами государственной власти и с хозяйствующими субъектами, гражданами на основе использования современных информационных технологий².

На каждом из указанных нами этапов сталкивается с рядом проблем, связанных с применением информационных и технических средств. Так, например, в процессе осуществления расследования по делу сотруднику органа предварительного расследования необходимо переработать огромный массив информации, при этом выделяя наиболее криминалистически значимую, установить между отдельными ее блоками причинно-следственную связь, а также не допустить при этом ошибок, связанных как с недостатком этой информации и трудностями в ее получении, так и с дефицитом времени³. Известно, что молодые и неопытные сотрудники не обладают достаточно высоким профессиональным уровнем, в связи, с чем не могут объективно оценить полученную информацию, ее оперативную значимость, а также не представляют где и как следует организовывать работу по сбору необходимых сведений, с помощью каких сил, средств и методов необходимо в той или иной ситуации обеспечить поиск информации, представляющей оперативный интерес⁴. Отсутствие

¹Вехов В.Б., Васюков В.Ф. Получение компьютерной информации от организаторов ее распространения в сети Интернет при расследовании преступлений // Российский следователь.2018. №3. С.11.

²Бертовский Л.В. Криминалистика: учебник.М.:РГ-пресс,2018. С.216.

³Зайцев О.А., Пастухов П.С. Формирование новой стратегии расследования преступлений в эпоху цифровой трансформации // Вестник Пермского университета. 2019. № 46. С.754.

⁴Рясов А.А., Жигалова Г.Г., Аветисян А.Д. Особенности подготовки следователей, специализирующихся на расследовании преступлений, совершаемых с использованием современных информационно-коммуникационных технологий // Мир науки, культуры, образования, 2018. № 4 (71).С.72 .

необходимого профессионального уровня может привести к принятию неверных тактических решений¹.

Отметим также, что в процессе расследования по делу значительное время затрачивается следователем на рутинную работу по составлению различных документов как процессуального, так и непроцессуального характера: постановления, запросы, планы расследования, карточки уголовной статистики и др.². В настоящее время присутствует также дефицит актуальной специализированной литературы по раскрытию преступлений в сфере информационно-телекоммуникационных технологий, поскольку технологические средства, при помощи которых совершаются киберпреступления постоянно прогрессируют, а, следовательно, и методики их расследования устаревают.

В связи, с чем полагаем, что одной из проблем в обозначенной нами сфере является отсутствие достаточной профессиональной подготовки кадрового состава следственных подразделений ОВД по работе с информационно-техническими средствами³. Наличие данной проблемы по результатам проведённого социологического опроса среди 16 сотрудников Отдела по расследованию преступлений на территории, обслуживаемой отделом полиции «Центральный» СУ УМВД России по г. Челябинску подтвердила большая часть опрошенных. Так, в соответствии с полученными результатами 81,25% респондентов разделяют наше мнение о необходимости осуществления переподготовки и повышение квалификации кадрового состава следственных подразделений ОВД РФ для работы с информационно-техническими средствами, при этом 12,50% респондентов не поддержали нашу точку зрения и 6,25% проявили затруднение с выбором

¹Вехов В.Б. Основные направления использования компьютерных технологий в деятельности следователя // Информационная безопасность регионов. 2007. № 1 (1) .С.65.

²Гаврилин Ю.В., Балашова А.А. Совершенствование процессуального порядка собирания доказательственной информации, содержащейся в сетевых информационных системах // Криминалистика: вчера, сегодня, завтра. 2020. № 1 (13). С.135.

³ Богатырева Л.И Анализ основных кадровых тенденций в следственных подразделениях МВД России на современном этапе // Закон и право. 2019. № 4. С. 135.

ответа. Отметим также, что при ответе на представленный в анкете вопрос: «Нуждается ли Вы в повышении квалификации для работы с информационно-техническими средствами?» 87,50% респондентов подтвердили необходимость повышения личной квалификации в данной сфере и всего лишь 6,25% респондентов удовлетворены имеющимися у них навыками. Небольшой процент, а именно 6,25% проявили затруднение с выбором ответа (Результаты социологического опроса представлены в Приложении № 2).

Проблема недостаточности профессиональной подготовки кадрового состава, по мнению Н.Р. Шевково многом обусловлена тем, что «в настоящее время программы повышения квалификации в образовательных организациях системы МВД России по линии расследования киберпреступлений носят исключительно теоретический характер, практические занятия отсутствуют»¹. Решить озвученную проблему возможно путём организации осуществления обучения, переподготовки и повышения квалификации кадрового состава следственных подразделений ОВД РФ в образовательных учреждениях системы МВД России в целях овладения необходимыми навыками по использованию информационно-технических средств.

К проблемам организации процесса расследования преступлений следственными подразделениями ОВД РФ с использованием информационных технологий можно отнести и имеющийся на сегодняшний день недостаток технического оснащения указанных подразделений. К сожалению, в большинстве рассматриваемых нами подразделений ОВД РФ имеется недостаток таких элементарных технических средств, как персональные компьютеры, печатные устройства и прочей оргтехники. Это же касается и средств выемки аппаратного обеспечения, технических средств

¹Шевко Н.Р. Проблемы подготовки специалистов по раскрытию и расследованию и преступлений, совершенных с использованием современных информационных технологий, в образовательных организациях МВД России // Вестник Казанского юридического института МВД России. 2017. № 1 (27). С.89.

исследования электронных доказательств, обработки и расшифровки данных¹.

В связи с чем, становится очевидным, что одним из приоритетных направлений совершенствования качества правоохранительной деятельности является качественное техническое оснащение указанных подразделений. Так, по результатам проведенного социологического опроса 97,75% респондентов считают, что на сегодняшний день следственные подразделения имеют существенный недостаток в оснащении компьютерной техникой, при этом ни один сотрудник не говорит о достаточности технического оснащения (Результаты социологического опроса представлены в Приложении № 2). Считаем, что создание надежной системы обеспечения ОВД финансовыми средствами и материально-техническими ресурсами в соответствии с нормативами, а также реформирование системы организации снабжения материальными ресурсами ОВД с учетом возложенных на них новых задач, а также экономических, политических и других факторов сможет разрешить указанную проблему.

Подводя итог, хочется сделать вывод о том, что организация процесса расследования преступлений следственными подразделениями ОВД РФ настоятельно требует совершенствования, особенно в части использования информационных технологий. Рост киберпреступности, несмотря на, казалось бы, обилие информационно-технических средств во многом обусловлен имеющимися недостатками в области организации процесса расследования преступлений с применением информационных технологий.

На сегодняшний день становится очевидным, что существует достаточно много проблем, касающихся использования информационных технологий при расследовании преступлений – нехватка достаточного числа подготовленных сотрудников, которые обладали бы необходимыми

¹ Сарычев А.В., Архипцев И.Н. Современное состояние раскрытия и расследования преступлений, совершаемых с использованием информационных технологий // Проблемы правоохранительной деятельности. 2020. № 1 (39). С.38.

знаниями для работы с информационными технологиями; отсутствуют методики расследования инновационных преступлений; нет надежных и эффективных информационно-аналитических решений; наблюдается рутинный характер при составлении процессуальных и не процессуальных документов; отсутствует необходимое техническое оснащение следственных отделов.

Указанные проблемы можно решить посредством внедрения недостающих информационных технологий, которые могли бы быть использованы в ходе организации процесса расследования конкретного преступления, к примеру, таких как средства выемки аппаратного обеспечения и электронных доказательств, средства дистанционной экспертизы оборудования и ликвидации информации, средства обработки и расшифровки данных и др. Полагаем, что внедрение недостающих новейших информационных технологий позволит значительно сократить сроки производства по уголовному делу, а также позволит провести расследование более полно, объективно и в короткие сроки. Также, необходимо обозначить направления совершенствования организации аналитической работы по формированию решений и заключений на основе анализа имеющейся информации.

Немаловажное значение на эффективность процесса расследования преступлений окажет появление методик расследования преступлений в сфере компьютерной информации, а также профессиональная подготовка кадрового состава следственных подразделений ОВД РФ в образовательных учреждениях системы МВД России в целях овладения необходимыми навыками по применению информационно-технических средств в процессе осуществления расследования по делу.

По-нашему мнению, внедрение новых и совершенствование уже имеющихся информационных технологий будет способствовать: во-первых, освобождению следователей от рутинной работы за счет ее автоматизации; во-вторых, совершенствованию структуры потоков

информации и системы документооборота в органах предварительного следствия, а следовательно и уменьшению затрат на производство расследования по уголовному делу.

2.2 Применение информационных технологий при проведении следственных действий

Следователи ОВД обладают большим количеством процессуальных действий, направленных на собирание и проверку доказательств по уголовному делу. Важнейшее место среди всех осуществляемых процессуальных действий занимают следственные действия. Производство следственного действия преследует цель – получить необходимую информацию, имеющую значение для установления истины по делу¹. В настоящее время, вследствие развития информационных технологий во всех сферах общественной жизни, появляются новые, все более изощрённые способы совершения преступлений. Появление «новых» преступлений диктует необходимость применения следователем в своей деятельности современных научно-технических средств, необходимых для их расследования².

Действующим уголовно-процессуальным законодательством предусмотрена возможность осуществления следственных действий в ходе производства по уголовному делу, однако понятие «следственные действия» в УПК РФ не раскрывается³. В теории и на практике под «следственными действиями» следует понимать предусмотренные уголовно-процессуальным законодательством процессуальные действия органов предварительного

¹Стурова Н.А. Некоторые особенности тактики производства следственных действий, направленных на получение доказательств в электронной форме // Юристы-правоведы. 2019. № 2 (89). С. 226.

²Химичева О.В., Андреев А.В. Цифровизация как тренд развития современного уголовного процесса // Вестник Московского университета МВД России. 2020. № 3. С. 21.

³Муженская Н.Е., Костылева Г.В. Руководство для следователя и дознавателя по расследованию отдельных видов преступлений: практическое пособие: в 2 частях, Ч. I. М.: Проспект, 2015. С. 46-49.

расследования, направленные на собирание (обнаружение, фиксацию и изъятие) необходимых доказательств по уголовному делу, а также осуществление проверки полученных доказательств. Значение следственных действий заключается в том, что они являются практически основным способом собирания доказательств по уголовному делу. В ходе осуществления того, или иного следственного действия, следователь или иное уполномоченное лицо получает необходимые фактические данные, а также сведения об обстоятельствах, подлежащих доказыванию по делу. Полученные сведения в результате их фиксирования в соответствии с требованиями процессуальной формы приобретают статус доказательств по уголовному делу¹.

Правовую основу применения информационных технологий и технических средств в рамках осуществления следственных действий составляют нормы уголовно-процессуального законодательства, касающиеся правил производства следственных действий². Так, ст.164 УПК РФ регламентирует общие правила производства следственных действий, при этом ч.6 ст.164 УПК РФ содержит норму, которая предписывает возможность применения в ходе проведения следственных действий технических средств и способов обнаружения, фиксации и изъятия следов преступления и вещественных доказательств³. Рассматривая положения указанной нормы, отметим, что следователь, или приглашенный им для участия в следственном действии специалист, оперативный работник всегда применяют технические средства в определённой очередности: сначала применяются те технические средства, которые обеспечивают сохранность следа в первоначальном виде, а уже затем оставшиеся. Например, при

¹ Леонов А.И., Смагин П.Г. Использование информационных технологий при производстве следственных действий, в том числе связанных с ограничением конституционных прав граждан. С. 345.

² Балакшин В.С., Литвин И.И. Современные технические средства и проблемы их применения в доказывании на досудебных стадиях уголовного судопроизводства. М.: Юрлитинформ, 2020. С.21.

³ Зуев С.В. Цифровизация судопроизводства. Научно-практический (постатейный) комментарий правовых актов С.78.

обнаружении следа обуви он сначала будет подвергнут узловой и детальной фотосъемке, а уже затем будет изъят полностью или в части. Отметим также что, установленные данной статьей правила подлежат применению при производстве тех следственных действий, при осуществлении которых предусмотрена законом возможность использовать технические средства или информационные технологии.

К нормам, регулирующим общие правила использования информационных и технических средств можно также отнести положение ч.2 ст.166 УПК РФ, которая гласит, что «протокол может быть написан от руки или изготовлен с помощью технических средств¹. При производстве следственного действия могут также применяться стенографирование, фотографирование, киносъемка, аудио- и (или) видеозапись. Стенограмма и стенографическая запись, фотографические негативы и снимки, материалы аудио-и видеозаписи хранятся при уголовном деле». Проанализировав указанную норму можно говорить о том, что УПК РФ предусматривает возможность составления протокола следственного действия с использованием находящихся у следователя технических средств. Под техническими средствами в данном случае следует понимать ПК, печатающие устройства и иную подобную оргтехнику. Отметим, что применение тех или иных технических средств, позволяющих фиксировать процесс проведения следственных действий оказывает существенную помощь следователю при расследовании преступлений². Полученные в результате применения указанных технических средств фотографии, аудио, видеозаписи и т. д., во-первых, дополняют протокол следственного действия, а во-вторых, служат гарантией законности при их проведении³. В этой связи необходимо рассмотреть и положение ч.1.1 ст. 170 УПК РФ, в соответствии с

¹Зуев С.В. Цифровизация судопроизводства. Научно-практический (постатейный) комментарий правовых актов.С.84.

²Воскобитова Л.А. Уголовное судопроизводство и цифровые технологии: проблемы совместимости // Lexrussia. 2019. № 5 (150). С.98.

³ Овчинникова О.В. Дистанционные следственные действия: современное состояние и перспективы//Юридическая наука и правоохранительная практика. № 1 (47). 2019. С.110.

которой при проведении таких следственных действий, как осмотр (ст.177 УПК РФ), осмотр трупа, эксгумация (ст.178 УПК РФ), следственный эксперимент (ст.181 УПК РФ), выемка (за исключением выемки электронных носителей информации) (ст.183.УПК РФ), наложение ареста на почтово-телеграфные отправления (ст. 185 УПК РФ), контроль и запись переговоров (ст.186 УПК РФ), проверка показаний на месте (ст.194 УПК РФ) по усмотрению следователя участие понятых может быть заменено техническими средствами, фиксирующими ход и результаты следственного действия. Если же в ходе следственного действия применение технических средств невозможно, то следователь делает в протоколе соответствующую запись¹. Считаем, что наиболее предпочтительно в случае отсутствия понятых использовать именно видеозапись, поскольку она позволяет зафиксировать следственное действие в динамике, что особенно ценно при производстве следственного эксперимента и проверки показаний на месте. Видеозапись также примечательна тем, что позволяет воссоздать как всю картину проведённого следственного действия, так и отдельные элементы в целях проверки правомерности и допустимости действий лиц, участвующих в нем, а также оценки достоверности полученных результатов². Несмотря на явное преимущество видеозаписи, тем не менее, уровень её распространения относительно невысок, что связано с недостаточным обеспечением территориальных подразделений ОВД техническими средствами.

Итак, нами были озвучены общие положения УПК РФ, касающиеся применения информационных технологий и технических средств при производстве следственных действий. Далее предлагаем привести детальную характеристику порядка использования информационных технологий и технических средств на примереконкретных следственных действий.

¹ Зуев С.В. Цифровизация судопроизводства. Научно-практический (постатейный) комментарий правовых актов. С.86.

² Зуев С.В. Развитие информационных технологий в уголовном судопроизводстве.С.127.

Как уже было ранее отмечено, информационные технологии и технические средства могут применяться при производстве тех следственных действий, при осуществлении которых предусмотрена законом возможность их использования. Одним из таких следственных действий является допрос – следственное действие, заключающееся в получении от потерпевшего, подозреваемого, обвиняемого, свидетеля, эксперта, специалиста показаний, касающихся обстоятельств, подлежащих доказыванию по уголовному делу, а также иных обстоятельств, имеющих значения для расследования преступления (ст. 187–191 УПК РФ). В соответствии с ч.4 ст.189 УПК РФ «по инициативе следователя или по ходатайству допрашиваемого лица в ходе допроса могут быть проведены фотографирование, аудио- и (или) видеозапись, киносъемка, материалы которых хранятся при уголовном деле и по окончании предварительного следствия опечатываются». Рассматривая данное положение, отметим, что фотографирование, аудио- и (или) видеозапись, киносъемка применяются следователем при наличии в его распоряжении одного из двух поводов, указанных в ч.4 ст.189 УПК РФ, а именно: при наличии собственной инициативы следователя (или иного должностного лица, уполномоченного осуществлять следственные действия), или же при наличии ходатайства допрашиваемого лица, представителей (в том числе законных представителей) потерпевшего, обвиняемого. Необходимо также учесть то обстоятельство, что в ч.4 ст. 189 УПК РФ применяется словосочетание «могут быть использованы», поэтому применять те или иные технические средства и информационные технологии в ходе производства допроса является правом следователя. Обратим внимание и на положение ч.4 ст. 190 УПК РФ, которая указывает на содержательную составляющую протокола допроса. Указанная норма обязует при составлении протоколе допроса осуществлять воспроизведение материалов аудио-и (или) видеозаписи, киносъемки. Так, при воспроизведении указанных материалов также

применяются технические средства, применение которых регламентируется нормами УПК РФ¹.

В соответствии с ч.6 ст.192 УПК РФ при производстве очной ставки соблюдаются общие правила, установленные для допроса участвующих в ней лиц. Под очной ставкой следует понимать - следственное действие, по своей природе представляющее разновидность допроса и заключающееся в одновременном допросе по одним и тем же обстоятельствам двух ранее допрошенных лиц для выяснения причин существенных противоречий в показаниях допрашиваемых и их устранения в целях установления истины по делу. Часть 4 ст.192 УПК РФ предусматривает возможность воспроизведения аудио- и (или) видеозаписи, киносъемки ранее данных по делу показаний допрашиваемых лиц при помощи различных технических средств (ПК, магнитофон, видеоманитофон и т.д.), порядок применения которых регламентируется общими нормами УПК РФ, предусматривающими возможность использования информационно-технических средств при производстве следственных действий².

Предъявление для опознания также представляет собой разновидность следственного действия, в ходе которого применяются информационно-технические средства и, заключающееся в опознании опознающим лицом в предусмотренном законом порядке образа ранее наблюдаемого лица или объекта с лицами или объектами, представленными следователем. Так, в соответствии с ч.5 ст.192 УПК РФ «при невозможности предъявления лица опознание может быть произведено по его фотографии, предъявляемой одновременно с фотографиями других лиц, внешне сходных с опознаваемым лицом. Количество фотографий должно быть не менее трёх»³. Следовательно, в данном случае технические средства применяются для

¹ Зуев С.В. Цифровизация судопроизводства. Научно-практический (постатейный) комментарий правовых актов. С.98.

²Зуев С.В. Цифровизация судопроизводства. Научно-практический (постатейный) комментарий правовых актов.С.101.

³Там же. С.102.

изготовления необходимых фотографий. Такими техническими средствами могут быть ПК, программы-редакторы изображения, печатающие устройства.

Получение информации о соединениях между абонентами и (или) абонентскими устройствами (ст. 186.1 УПК РФ) является в достаточной степени новым видом следственного действия и заключается в фиксации информации о соединениях между абонентами и (или) абонентскими устройствами в установленном законодательством порядке и представлении ее (либо представлении указанной информации зафиксированной в установленном порядке ранее вне связи с производством по уголовному делу) следователю на любом материальном носителе, осмотр следователем представленных документов в целях получения сведений, имеющих значение для уголовного дела¹. Это следственное действие неразрывно связано с применением информационно-технических средств, поскольку осуществляется в целях обнаружения доказательств в электронной форме, а именно получение сведений о дате, времени, продолжительности соединений между абонентами и (или) абонентскими устройствами (пользовательским оборудованием), номерах абонентов, а также других данных, позволяющих идентифицировать абонентов, а также сведений о номерах и месте расположения приемопередающих базовых станций. В настоящее время получение информации о соединениях между абонентами и (или) абонентскими устройствами активно используется не только при расследовании преступлений, осуществляемых посредством применения сети Интернет, но и при расследовании общеуголовных преступлений, таких как кражи, убийства и многих других. Несмотря на относительную новизну данного следственного действия, тем не менее, в техническое оборудование и системы операторов сотовой связи с каждым днём внедряются всё более новое технологическое оборудование, которое способно предоставлять не

¹ Зуев С.В. Цифровизация судопроизводства. Научно-практический (постатейный) комментарий правовых актов. С.97.

только сведения, указанные нами ранее, но и множество иных сведений о личности преступника. В связи с чем, возникает проблема, связанная с надлежащей уголовно-процессуальной регламентацией «иных сведений», поскольку ставится под сомнение приобщение полученных электронных доказательств к материалам уголовного дела. Согласимся с мнением В.Ю. Стельмаха о том, что в УПК РФ, в частности в п. 24.1 ст. 5 необходимо установить возможность получения и других сведений, не указанных в данном пункте, фиксируемых аппаратурой операторов связи¹.

Информационные технологии применяются и при производстве такого следственного действия, как наложение ареста на почтово-телеграфные отправления, их осмотр и выемка (ст.185 УПК РФ)². Под выемкой почтово-телеграфной корреспонденции понимаются действия по изъятию электронной почты, адресованной абоненту у провайдера (оператора связи). Электронная форма почтового сообщения классифицируется как доказательство, полученное в электронной форме. Следователь при получении данного рода доказательства применяет также технические средства для его воспроизведения, например ПК, печатающее устройство, аудио- и (или) видеозаписи или средства копирования, например флеш-носитель, жёсткий диск и т. д.

Применение технических средств и информационных технологий при производстве иных следственных действий в случае, если законодателем установлена возможность применения информационно-технических средств проводится по общим правилам, предусмотренным УПК РФ.

Повсеместное развитие информационных технологий, а также появление новых преступлений с использованием новейших информационных технологий требуют совершенствования деятельности

¹ Стельмах В.Ю. Проблемы процессуальной регламентации следственных действий, направленных на получение сведений, передаваемых по средствам электросвязи // Юридическая наука и правоохранительная практика.2013.№ 3 (25).С.111.

²Зуев, С.В. Цифровизация судопроизводства. Научно-практический (постатейный) комментарий правовых актов. С.90.

органов предварительного расследования в этой области. Так, на сегодняшний день уголовно-процессуальная регламентация порядка применения технических средств и информационных технологий при производстве следственных действий настоятельно требует совершенствования¹. Вызывают сомнение нормы УПК РФ, касающиеся следственных действий, связанных с изъятием «электронных носителей информации»². По смыслу действующего законодательства и, руководствуясь положениями статей 81, 81.1, 182, 183 УПК РФ под «электронным носителем информации» следует понимать внутренний накопитель на жестком магнитном диске, оптические диски различных видов, магнитно-оптические диски, карты памяти различных форматов, USB флеш-накопители, гибкие магнитные диски, интегральная микросхема памяти и иные носители³. В ходе производства следственных действий выделяют такие способы получения цифровой информации, как изъятие электронных носителей информации и их последующее исследование или же копирование на электронные носители цифровой информации, представляющей интерес для уголовного дела⁴. Основным способом получения цифровой информации в процессе осуществления следственного действия выступает изъятие электронных носителей информации, он производится в 96% случаев. Копирование же цифровой информации на электронные носители применяется всего лишь в 4% случаев⁵. Отметим также, что действующим уголовно-процессуальным законодательством

¹ Александров А.С., Андреева О.М., Зайцев О.А. О перспективах развития российского уголовного судопроизводства в условиях цифровизации // Вестник Томского государственного университета. 2019. № 488. С.205.

² Лозовский Д.Н., Ахриев М.Т. Особенности производства обыска (выемки), связанного с изъятием электронных носителей информации // Гуманитарные, социально-экономические и общественные науки. 2018. № 7. С.120.

³ Добровлянина О.В. Некоторые аспекты о процессуальном изъятии (копировании) электронных носителей информации // Пермский юридический альманах. 2019. № 2. С.645.

⁴ Зуев С.В. Развитие информационных технологий в уголовном судопроизводстве. С.168

⁵ Крюкова Т.С. Некоторые вопросы изъятия электронных носителей информации в ходе производства следственных действий: анализ судебной практики // Правопорядок: история, теория, практика. 2016. № 4 (11). С.61.

предусмотрена обязанность следователя привлекать специалиста только при изъятии электронного носителя информации (ст.164.1 УПК РФ), при этом следователь вправе произвести копирование информации с электронного носителя самостоятельно без его изъятия¹.

Обязательность участие специалиста при изъятии электронных носителей информации, несмотря на императивное указание в законе носит весьма спорный характер. Анализ судебной практики по вопросам необходимости участия специалиста по мнению Т.С Крюковой указывает, что, «только в 10% судебных решений отсутствие специалиста было признано существенным нарушением порядка производства следственных действий, связанных с изъятием электронных носителей информации и повлекло за собой признание протоколов следственных действий недопустимыми доказательствами, в остальных же случаях, несмотря на предписанное положение, суд признал доказательства допустимыми»². Так, суды при рассмотрении дел о нарушении порядка производства следственных действий, связанных с изъятием электронных носителей информации придерживаются позиции, в соответствии с которой изъятие электронного носителя информации в процессе производства следственного действия правомерно осуществляться и без участия специалиста, если копирование информации, содержащейся на нем, не производится, либо изъятие не представляет сложности и не требует специальных знаний и навыков. Участие специалиста считается обязательным только в случае возникновения необходимости в применении специальных знаний и угрозе потери хранящейся на носителе информации.

Интересен следующий пример из судебной практики. Гражданин Я. Советским районным судом г. Орскабыл признан виновным в совершении

¹ Зуев С.В., Черкасов В.С. Новые правила изъятия электронных носителей и копирования информации (статья 164.1 УПК РФ) преимущества и недостатки новеллы // Сибирское юридическое обозрение. 2019. № 2. С. 193.

² Крюкова Т.С. Некоторые вопросы изъятия электронных носителей информации в ходе производства следственных действий: анализ судебной практики. С.62.

преступления, предусмотренного ч. 3 ст. 30, п. «г» ч. 4 ст. 228.1 УК РФ (покушение на сбыт наркотических средств в крупном размере). Гражданин Я. представил апелляционную жалобу и просил отменить приговор, ссылаясь на тот факт, что изъятие у него мобильного телефона, являющегося электронным носителем информации, было произведено сотрудниками Линейного отдела МВД России на транспорте без участия специалиста, в связи с чем были нарушены нормы ч. 3.1. ст. 183 УПК РФ. Апелляционный суд в свою очередь посчитал доводы, представленные гражданином Я. необоснованными и пояснил, что по смыслу ч. 3.1. ст. 183 УПК РФ участие специалиста при производстве выемки в ходе изъятия электронных носителей информации требуется при наличии нуждаемости в данном специалисте, когда имеется необходимость применить специальные познания и навыки. В частности, если при производстве выемки производится копирование информации на другие электронные носители информации, участие специалиста обязательно, так как это связано с риском утраты или изменения информации. Также, в материалах дела было указано, что при выемке следователь пользовался обычными функциями просмотра телефона, не прибегая к необходимости поиска и открытия, закрытых для общего доступа файлов¹.

Противоположная позиция судебных органов получила отражение в апелляционном постановлении, принятом 17 октября 2017 г. Соликамским городским судом Пермского края, где по жалобе защитника был признан в качестве недопустимого доказательства CD-диск, в связи с тем, что его изъятие проходило без участия специалиста. Суд посчитал, что, отсутствие специалиста является нарушением требований ч. 2 ст. 164.1 УПК РФ².

¹ Апелляционное определение Судебной коллегии по уголовным делам Оренбургского областного суда № 22-4229/2016 от 03 ноября 2016 г. URL: <https://base.garant.ru/144577943/> (дата обращения 20.03.2021).

² Апелляционное постановление Соликамского городского суда Пермского края № 10-83/2017 от 17 октября 2017 г. URL: <http://sudact.ru> (дата обращения: 20.03.2021).

В приведённых примерах из судебной практики явная противоречивость обусловлена, прежде всего, отсутствием должной правовой регламентации надлежащего порядка привлечения специалиста к процедуре изъятия электронного носителя и копирования информации¹. Полагаем, что отсутствие необходимой правовой регламентации механизма привлечения специалиста к процедуре изъятия электронного носителя информации приводит к проблеме приобщения такого носителя к материалам дела в качестве доказательства.

Согласимся с мнением С.В. Зуева и В.С. Черкасова о том, что «императивное требование о привлечении специалиста для изъятия электронных носителей информации не соответствует современному уровню технического развития. По нашему мнению, современные информационные технологии настолько просты в обращении, что практически не требуют специальных умений и знаний для их применения»². Отметим также, что на отсутствие необходимости обязательного участия специалиста при изъятии электронного носителя информации неоднократно указывалось в юридической литературе. Так, О.В. Овчинникова указывает, что «95% опрошенных следователей отметили, что участие специалиста при изъятии электронных носителей информации нарушает принцип процессуальной экономии: 5% опрошенных согласились с целесообразностью участия специалиста при необходимости отсоединения носителей от сети либо демонтажа устройства для изъятия его составных частей»³.

На основании вышесказанного считаем, что требование законодателя об обязательном участии специалиста при изъятии электронных носителей информации настоятельно требует изменения, поскольку многие электронные носители используются повсеместно и не требуют специальных

¹ Зуев С.В., Черкасов В.С. Новые правила изъятия электронных носителей и копирования информации (статья 1641 УПК РФ): преимущества и недостатки новеллы. С. 194.

² Там же. С.195.

³ Овчинникова О.В. Собираение электронных доказательств, размещенных в сети Интернет // Правопорядок: история, теория и практика. 2016. № 4. С. 69.

познаний (CD-RW, флеш-накопители и т.д.), а также ставит под сомнение процессуальную самостоятельность следователя как субъекта предварительного расследования. Полагаем, что в действующем законодательстве необходимо закрепить положение, в соответствии с которым следователь будет иметь право самостоятельно привлекать специалиста для изъятия электронных носителей информации, в случае, если требуются специальные познания.

Представленное нами предложение об изменении ч.2 ст.164.1 УПК РФ посредством внесения положения, предоставляющее возможность следователю самостоятельно привлекать специалиста для изъятия электронных носителей информации, в случае, если требуются специальные познания по результатам проведенного нами анкетирования среди сотрудников Отдела по расследованию преступлений на территории, обслуживаемой отделом полиции «Центральный» СУ УМВД России по г. Челябинску поддержало 62,50% респондентов, при этом 25,00% респондентов предложили оставить это положение без изменений и 12,5% проявили затруднение с выбором ответа (полученный результат представлен в Приложении № 2 к выпускной квалификационной работе).

На основании полученных результатов считаем целесообразным предложить проект Федерального закона «О внесении изменений в УПК РФ», а именно внести изменение в ч.2 ст.164.1 УПК РФ (Приложение № 3).

Таким образом, вопросы применения информационных технологий и технических средств при проведении следственных действий приобретают всю большую значимость не только вследствие технологического прогресса, но и в связи с ростом компьютерной преступности. Сегодня следователю в рамках осуществления предварительного расследования по уголовному делу необходимо обладать не просто навыками производства различных процессуальных действий, в том числе навыками производства следственных действий, но и уметь применять технические и информационные средства в процессе расследования по уголовному делу. Применение информационно-технических средств при производстве следственных

действий оказывает значительную помощь в раскрытии и расследовании преступлений.

В настоящее время уголовно-процессуальная регламентация порядка применения технических средств и информационных технологий при производстве следственных действий настоятельно требует правового совершенствования. Нормы УПК РФ, регламентирующие изъятие «электронных носителей информации» вызывают сомнение, что связано с отсутствием должной правовой регламентации надлежащего порядка привлечения специалиста к процедуре изъятия электронного носителя и копирования информации, предусмотренного ст.164.1 УПК РФ.

Недостатки правовой регламентации процессуального порядка получения доказательственной информации на электронных носителях отражаются на качестве расследования уголовных дел, правильности сбора и оформления доказательств в виде информации на электронных носителях. Так, по мнению П.В. Козловского и П.В. Седельникова «в современных условиях, когда скорость изменений в науке и технике высока, необходимо отказаться от попыток обязать органы расследования применять специальные знания в определенных случаях и конкретным способом. Как показала практика, это создает неоправданные формальные препятствия при производстве расследования. Закон должен содержать нормы общего характера, оставляя правоприменителю возможность самостоятельно определять потребность и форму их использования»¹.

Проведя анализ юридической литературы и материалов судебной практики по данному вопросу, считаем, что необходимость предоставления следователю возможности самостоятельно привлекать специалиста для изъятия электронных носителей информации, в случае, если требуются специальные познания – очевидна. Разрешить имеющийся спорный момент возможно посредством внесения изменений в ч.2 ст.164.1 УПК РФ.

¹Козловский П.В., Седельников П.В. Участие специалиста в изъятии электронных носителей // Научный вестник Омской академии МВД России.2014. № 1 (52).С.19.

2.3 Перспективы развития информационных технологий в деятельности следственных подразделений органов внутренних дел Российской Федерации

В последние годы в нашей стране ведется интенсивное внедрение новейших информационных технологий во все сферы общественной жизни, в том числе в правоохранительную¹. Отметим, что значительный удельный вес информационных функций является характерной особенностью деятельности ОВД РФ. Эпоха интенсивного развития информационных технологий характеризуется также ростом новых, всё более изощрённых способов совершения преступлений в сфере компьютерной информации, которые в настоящий момент можно отнести к разряду труднораскрываемых². Повысить эффективность деятельности следственных подразделений ОВД РФ по раскрытию преступлений, связанных с использованием информационных технологий возможно посредством внедрения в деятельность указанных подразделений современных информационных технологий, базирующихся на средствах электронно-вычислительной техники, электросвязи и телекоммуникации, программах для ЭВМ, базах данных, а также средствах цифровой фотографии, видео- и звукозаписи³.

Говоря о перспективах развития информационных технологий в деятельности следственных подразделений ОВД РФ, несомненно, интерес вызывают информационные технологии в уголовном процессе зарубежных стран, анализ которых позволяет сформировать наиболее целостное представление о существующем положении дел. Отметим также, что существующие информационные технологии и нормы законодательства их, регулирующие в уголовном процессе зарубежных стран, безусловно, могут

¹Хабриева Т.Я., Черногор Н.Н. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1 (253). С.87.

²Вехов В.Б., Зуев С.В. Расследование преступлений в сфере компьютерной информации и электронных средств платежа: учебное пособие для вузов М.: Юрайт, 2021. С.144.

³Белозеров О.И., Андрейченко П.М. Тенденции развития информационных технологий в системе правоохранительной деятельности // Научный журнал. 2019. № 10 (44). С.10.

служить возможной моделью развития информационных технологий в уголовном процессе Российской Федерации¹.

Так, например интересен опыт США в части использования в уголовном процессе системы электронного документооборота. Вся деятельность по управлению электронным документооборотом по уголовным делам в США регламентируется правилами, руководствами, регламентами судов и иных правоохранительных органов. К примеру, прокуроры и другие участники уголовного процесса могут подать в суд посредством использования системы электронного документооборота уголовное дело в электронном виде для дальнейшего его рассмотрения федеральными судами. Современные системы электронного документооборота во всех штатах закрепляют права сторон представлять документы в электронной форме по уголовным делам, при этом помимо официальных документов, созданных вне рамок уголовного судопроизводства, стороны могут сами создавать документы, в которых фиксируют доказательственную информацию, имеющую значение для дела².

Системы электронного документооборота повсеместно внедряются и во многих других государствах, например в Канаде, Германии, Саудовской Аравии, Бельгии, в которой ещё в 2005 году был создан проект электронного правосудия «Рнешх», в рамках которого помимо системы электронного документооборота «электронный файл» мог пополняться полицией, адвокатом, сторонами и судом. Вопрос аутентификации решался использованием электронного паспорта (eШ)³.

¹Сарапулов А.А. Информационные технологии в уголовном процессе: история, современное состояние, перспективы //Вестник Южно-Уральского государственного университета. 2013. № 2. С.107.

² Зуев С.В. Информационные технологии в уголовном процессе зарубежных стран.М.: Юрлитинформ, 2020. С.19.

³ Зуев С.В. Электронное уголовное дело: за и против // Правопорядок: история, теория, практика. 2018. № 4 (19). С. 6.

Учитывая повсеместное распространение среди зарубежных стран систем электронного документооборота полагаем, что электронная форма ведения уголовного дела является в достаточной степени перспективной и подлежит внедрению в деятельность следственных подразделений ОВД РФ. Представляется, что развитие информационных технологий в Российской Федерации достигло необходимого уровня для внедрения на досудебных стадиях уголовного процесса электронного документооборота и как следствие, внедрения «электронного уголовного дела», которое будет представлять собой кульминацию в развитии электронного документооборота¹. Представленную точку зрения разделяют многие исследователи. Так, например А.Ф. Абдулвалиев считает, что «модернизация уголовного судопроизводства должна заключаться в отказе от бумажных процессуальных документов и переходе на ведение уголовного дела в электронной форме». При этом, по мнению автора переход на электронную форму производства по уголовному делу должен в первую очередь упростить соби́рание доказательств и составление процессуальных документов по уголовному делу².

Под электронным уголовным делом следует понимать, прежде всего, содержащиеся на материальном носителе в электронном виде документы, отражающие ход расследования по уголовному делу³. При соблюдении мер, исключающих несанкционированный доступ посторонних лиц и обеспечивающих сохранность файлов, возможно хранение документов электронного уголовного дела в облачных хранилищах. Считаем, что придать данному электронному документу необходимую юридическую силу возможно при помощи электронной цифровой подписи⁴.

¹ Зуев С.В. Развитие информационных технологий в уголовном судопроизводстве. С.169.

² Абдулвалиев А.Ф. Опять про электронное уголовное дело // Право и политика. 2013. № 1. С.17.

³ Долгов А.М. Электронное уголовное дело в досудебных стадиях уголовного процесса в России // Общество: политика, экономика, право. 2018. № 9 (62). С. 30.

⁴ Гридюшко П.В., Бушкевич Н.С. Об электронной форме ведения уголовного процесса // Вестник Академии МВД Республики Беларусь. 2017. № 2 (34). С.69.

По-нашему мнению, «электронное уголовное дело» в детальности следственных подразделений ОВД РФ будет способствовать как оптимизации уголовного судопроизводства и сокращению сроков расследования преступлений, так и позволит повсеместно применять математические методы и алгоритмизации в поддержке принятия процессуальных решений¹. Инициативу о внедрении в деятельность следственных подразделений «электронного уголовного дела» по результатам проведенного анкетирования среди сотрудников Отдела по расследованию преступлений на территории, обслуживаемой отделом полиции «Центральный» СУ УМВД России по г. Челябинску поддержало более половины сотрудников (68,75%), не поддержали инициативу 18,75% и 12,50 % сотрудников проявили затруднение при ответе на данный вопрос. По результатам данного опроса, можно предположить, что в настоящее время сотрудники следственных подразделений ОВД явно заинтересованы во внедрении электронного документооборота на досудебных стадиях производства по уголовному делу.

Говоря о перспективе внедрения «электронного уголовного дела» в деятельность следственных подразделений ОВД РФ нельзя не отметить и перспективу внедрения искусственного интеллекта, как одной из передовых информационных технологий.

На сегодняшний день более 30 стран имеют национальные стратегии развития систем искусственного интеллекта во многих сферах деятельности, в свою очередь Правительство РФ также намерено утвердить «Национальную стратегию развития системы искусственного интеллекта в РФ» и «Дорожную карту развития искусственного интеллекта».

В США и Европе активно действует «умная полиция», работа которой заключается в патрулировании уже известных зон с высокой степенью криминальной активности. Благодаря способности интеллектуальных систем обрабатывать большое количество данных работа

¹ Зуев С.В. Электронное уголовное дело: за и против. С.9.

по поиску таких зон выполняется автоматически. Интеллектуальные системы в деятельности «умной полиции» США способны самостоятельно сопоставлять релевантную информацию и делать из нее выводы о повышении криминальной активности в тех или иных районах или о связях определенных людей с криминальными организациями¹.

Интересен опыт Китайской народной республики, которая реализовала проект системы искусственного интеллекта под названием «Золотой щит». Предназначение «Золотого щита» заключается в профилактике отдельных видов информационной преступности, которая достигается посредством усиления борьбы с преступностью со стороны спецслужб и повышения оперативности их реакции, наряду с увеличением продуктивности и эффективности работы полиции. «Золотой щит» способен осуществлять фильтрацию DNS-запросов и их переадресацию, блокировку интернет-адресов (URL) и IP-адресов, блокировку соединений, осуществляемых через VPN многое другое².

В деятельности следственных подразделений ОВД РФ на сегодняшний день широко применяются информационные базы данных, содержащие сведения о преступлениях и различных категориях лиц, представляющих интерес для правоохранительных органов. Такого рода информация содержится в Главном информационно - аналитическом центре МВД России, информационных центрах на региональном уровне, а также в экспертно-криминалистических подразделениях на территориальном, региональном, межрегиональном и федеральном уровнях и в подразделениях оперативно-розыскной информации. Можно с уверенностью утверждать, что имеющиеся на сегодняшний день базы данных по своей сути являются разрозненными. Данная ситуация может привести к потере оперативности

¹Овчинский В.С. Виртуальный щит и меч: США, Великобритания, Китай в цифровых войнах будущего. М.: Кн. мир. 2018. С.34.

²Кузьмин И.А Искусственные нейронные сети: перспективы использования в правоохранительной деятельности //Криминалистика: вчера, сегодня, завтра. 2018. № 4(8). С.110.

при проведении следственных действий и оперативно-розыскных мероприятий. Полагаем, что для удобства пользования сотрудниками следственных подразделений ОВД РФ обозначенными информационными базами, в том числе при работе с информацией, содержащейся в сети «Интернет» необходимо создать систему, которая бы позволила объединить множество разобренных баз в единый ресурс и была способна осуществить помощь с выбором необходимой информации по конкретному уголовному делу.

Нельзя сказать, что на сегодняшний день система, подобная системе искусственного интеллекта вовсе отсутствует в практике ОВД РФ. Например, широко применяется оборудование и программное обеспечение компании АО «Папилон», которая кроме реализации функций идентификации, способна автоматизировать дактилоскопические и криминалистические учёты, формируемые в рамках выполнения Федерального закона от 25.07.1998 г. №128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации»¹. На базе АДИС «Папилон» построены все крупнейшие автоматизированные банки данных дактилоскопической информации федерального, межрегионального и регионального уровня. Отметим также, что в электронный формат «Папилон» переведены почти все бумажные дактилоскопические учеты страны.

Учитывая повсеместное применение систем искусственного интеллекта в зарубежных странах, считаем возможным и необходимым внедрить подобную систему и в деятельность следственных подразделений ОВД, в связи с чем предлагаем: во-первых, создать систему искусственного интеллекта, которая в ходе осуществления предварительного расследования будет способна определять возможные направления расследования, т. е формировать версии о событиях с учетом различных источников информации, осуществлять выбор наиболее вероятных направлений

¹ Федеральный закон «О государственной дактилоскопической регистрации в Российской Федерации» от 25 июля 1998 г. № 128-ФЗ // СЗ РФ. 1998. № 31. Ст.3806.

деятельности, а также предоставлять пользователю рекомендации относительно дальнейших действий, например назначение экспертиз, проведение оперативно-розыскных мероприятий и следственных действий. По нашему мнению, создание такой системы может способствовать оптимизации уголовно-процессуальной деятельности, уменьшению нагрузки на субъектов расследования, а также сокращению следственных ошибок в ходе производства по уголовному делу. Полагаем, что предложенная нами система искусственного интеллекта может быть создана по принципу глубинного обучения нейронных сетей, который заключается в постепенном обучении системы распознавать изображения, понимать речь и даже самостоятельно принимать решения¹.

Во-вторых, учитывая рост экономических преступлений в стране, связанных с хищением денежных средств при помощи компьютерных систем, считаем необходимым внедрить в деятельность следственных подразделений аналог действующей в настоящий момент в США системы искусственного интеллекта «Mayhem». Система искусственного интеллекта «Mayhem» способна распознавать индивидуальный почерк хакеров и хакерских группировок, а также преследовать хакеров, вплоть до установления их локаций². Учитывая тот факт, что в нашем государстве большинство хакерских атак осуществляются посредством социальных сетей, то предлагаем взять за основу основные функции «Mayhem», но адаптировать алгоритм ее действия с учетом возможного вредоносного софта в социальной сети и архитектуры алгоритма ее построения³. Создание такой системы по-нашему мнению будет способствовать экономии времени и

¹ Афанасьев А.Ю. Искусственный интеллект или интеллект субъектов выявления, раскрытия и расследования преступлений: что победит? // Научный журнал. 2018. № 3 (38). С. 29; Кузьмин И.А. Искусственные нейронные сети: перспективы использования в правоохранительной деятельности // Криминалистика: вчера, сегодня, завтра. 2018. № 4 (8). С. 115.

² Суходолов А.П., Бычкова А.М. Искусственный интеллект в противодействии преступности, ее прогнозировании, предупреждении и эволюции // Всероссийский криминологический журнал. 2018. № 6. С. 753.

³ Жданов Ю.Н., Овчинский В.С. Полиция будущего. М.Кн. мир, 2018. С.22.

увеличению своевременности выявления хакерских атак, которые из-за недостатка времени укрываются от следственных подразделений.

По результатам проведенного анкетирования среди сотрудников Отдела по расследованию преступлений на территории, обслуживаемой отделом полиции «Центральный» СУ УМВД России по г. Челябинску предложение о внедрении в деятельность следственных подразделений ОВД системы искусственного интеллекта поддержали 75,00% респондентов, 12,50% респондентов не разделяют нашу точку зрения и такой же процент респондентов выбрали вариант ответа «затрудняюсь ответить».

На основании полученных результатов считаем, что развитие системы искусственного интеллекта является перспективным направлением деятельности, которое может способствовать оптимизации уголовно-процессуальной деятельности, уменьшению нагрузки на субъекты расследования, а также сокращению следственных ошибок в ходе производства по уголовному делу.

Подводя итог, хочется отметить, что возможности информационных технологий в настоящее время достаточно многообразны, однако их специфический вклад необходимо строго увязать с требованиями уголовно-процессуального закона. Данное требование необходимо реализовать с учетом перспектив их развития в будущем.

Анализ имеющихся на сегодняшний день возможностей информационных технологий в уголовном процессе США, Китая и других стран позволил сделать вывод о том, что наиболее перспективными направлениями совершенствования информационных технологий в деятельности следственных подразделений ОВД РФ являются электронный документооборот, в частности «электронное уголовное дело» и искусственный интеллект.

По-нашему мнению, «Электронное уголовное дело» позволит значительно сократить сроки расследования преступлений, поскольку работа в «электронном виде» будет вестись намного быстрее, а также будет

способствовать оптимизации уголовно-процессуальной деятельности в целом. Придать электронному документу необходимую юридическую силу возможно при помощи электронной цифровой подписи. Считаем, что учитывая нарастающую динамику развития информационных технологий отказ от бумажного уголовного дела в пользу электронного, скорее всего, будет неизбежным уже в самом ближайшем будущем. Предполагаем, что внедрению «электронного уголовного дела» должна предшествовать основательная разработка, унификация и законодательное закрепление правил, регламентирующих вопросы применения «электронного уголовного дела». Согласимся с мнением С.ВЗуева, который считает, что «для внедрения электронного документооборота в стране необходимо регулирование, в первую очередь, основных начал проведения следственных действий и иной деятельности с использованием информационных технологий и электронных документов, путем формулирования норм о гарантиях подлинности электронных доказательств, защите от возможных посягательств и доступности для последующего изучения, депонировании электронных копий, обязательном участии специалиста при проведении следственных или судебных действий, связанных с копированием, депонированием, осмотром, изъятием электронной информации».

Что же касается внедрения в деятельность следственных подразделений системы, работающей по принципу искусственного интеллекта, считаем, что внедрение такой системы будет способствовать не только оптимизации уголовно-процессуальной деятельности и уменьшению нагрузки на субъекты расследования, но и сократит количество допускаемых следственных ошибок в процессе осуществления производства по уголовному делу. Предполагаемая возможность сокращения следственных ошибок имеет принципиальное значение, поскольку как уже ранее было отмечено, в настоящий момент одной из проблем в деятельности следственных подразделений ОВД РФ является недостающий уровень у

сотрудников ОВД РФ умений и навыков, необходимых для работы с информационными технологиями и техническими средствами.

Учитывая тот факт, что в Российской Федерации большинство хакерских атак осуществляются посредством социальных сетей, то предлагаем взять за основу основные функции системы искусственного интеллекта «Mayhem», но адаптировать алгоритм ее действия с учетом возможного вредоносного софта в социальных сетях РФи применять на практике в деятельности следственных подразделений ОВД РФ.

Выводы по второй главе. Организация процесса расследования преступлений, равно как и производство следственных действий в части применения информационных технологий и технических средств следственными подразделениями ОВД РФ настоятельно требуют правового совершенствования.

Проблемными аспектами организации процесса расследования преступлений с применением информационно-технических средств являются: нехватка достаточного числа подготовленных сотрудников, которые обладали бы необходимыми знаниями, умениями и навыками для работы с информационными технологиями и техническими средствами; отсутствуют методики расследования инновационных преступлений; наблюдается рутинный характер при составлении процессуальных и не процессуальных документов, а также отсутствует необходимое материально-техническое оснащение следственных отделов. Обозначенные проблемы можно разрешить путем внедрения недостающих информационных технологий, которые могли бы быть использованы в ходе организации процесса расследования конкретного преступления, к примеру, таких как средства выемки аппаратного обеспечения и электронных доказательств, средства дистанционной экспертизы оборудования и ликвидации информации, средства обработки и расшифровки данных и др. Обучение сотрудников необходимым тактическим приемам в образовательных организациях системы МВД России и совершенствование

методик расследования преступлений в сфере компьютерной информации окажет немаловажное значение на эффективность процесса расследования преступлений. Проблему нехватки материально-технического оснащения указанных подразделений можно разрешить за счет перераспределения как финансовых средств на уровне субъекта, так и на уровне федерального бюджета. Рутинный характер при составлении процессуальных и не процессуальных документов также находится в прямой зависимости от имеющихся в арсенале следователей информационно-технических средств.

Уголовно-процессуальная регламентация порядка применения информационно-технических средств при производстве следственных действий нуждается в правовом совершенствовании в части изъятия «электронных носителей информации». В действующей редакции УПК РФ отсутствует должная правовая регламентация надлежащего порядка привлечения специалиста к процедуре изъятия электронного носителя и копирования информации на таком носителе.

Считаем, что императивное требование о привлечении специалиста для изъятия электронных носителей информации, предусмотренное ч.2 ст. 164.1 УК РФ не соответствует современному уровню технического развития и настоятельно требует изменения, поскольку многие электронные носители используются повсеместно и не требуют специальных познаний (CD-RW, флеш-накопители и т.д.), а также ставит под сомнение процессуальную самостоятельность следователя как субъекта предварительного расследования. Стоит учесть, что недостатки правовой регламентации процессуального порядка получения доказательственной информации на электронных носителях отражаются на качестве расследования уголовных дел, правильности сбора и оформления доказательств в виде информации на электронных носителях. В связи с чем предлагаем внести соответствующее изменение в ч.2 ст.164.1 УПК РФ, а именно предоставить возможность следователю самостоятельно привлекать специалиста для изъятия

электронных носителей информации, в случае, если требуются специальные познания.

Перспективными направлениями развития информационных технологий в деятельности следственных подразделений ОВД РФ являются электронный документооборот в частности «электронное уголовное дело» и искусственный интеллект. Систему, работающую по принципу искусственного интеллекта предлагаем внедрить по аналогии с действующей в США «MauiNet», но адаптировать алгоритм ее действия с учетом возможного вредоносного софта в социальных сетях РФ и применять на практике в деятельности следственных подразделений ОВД РФ.

Внедрение в деятельность указанных нововведений по-нашему мнению будет способствовать оптимизации уголовно-процессуальной деятельности и уменьшению нагрузки на субъекты расследования, что в конечном итоге приведет к сокращению количества допускаемых следственных ошибок в ходе производства по уголовному делу.

ЗАКЛЮЧЕНИЕ

Результаты проведенного исследования позволяют сделать следующие выводы.

В настоящее время информационные технологии достаточно быстрыми темпами внедряются в деятельность следственных подразделений ОВД РФ, в связи, с чем немаловажное значение приобретает как отечественная, так и международно-правовая регламентация данного процесса. Считаем, что в условиях современной действительности законодателю необходимо обратить пристальное внимание на имеющуюся нормативно-правовую базу в данной сфере. Так, практическая значимость таких международных правовых актов, как Конвенция против транснациональной организованной преступности, Окинавская хартия глобального информационного общества, Декларация принципов «Построение информационного общества и др. заключается в том, что они представляют собой стандарты применения механизмов и процедур, связанных с процессами цифровизации в правоохранительной деятельности. В свою очередь отечественное законодательство призвано регламентировать процессы внедрения и применения информационно-технических средств, основываясь на нормах международного права.

Действующее уголовно-процессуальное законодательство также требует совершенствования по вопросам регулирования порядка применения информационных технологий в деятельности следственных подразделений ОВД РФ. Так, в действующей редакции УПК РФ отсутствует понятие информационных технологий и технических средств, также отсутствует и прямое упоминание о компьютере, что приводит к затруднительной оценке порядка применения указанных средств в правоохранительной деятельности.

Считаем также, что уголовно-процессуальное законодательство в области регулирования информационных технологий и технических средств носит пока лишь фрагментарный и непоследовательный характер, а содержащиеся в УПК РФ положения о применении информационных

технологий и технических средств не соответствуют современному уровню развития информационных технологий. Многие моменты не учтены и остаются без практического применения, отсутствуют общие положения об использовании информационных технологий, само понятие технических средств, критерии допустимости использования технических средств за редкими исключениями также не находят своего отражения в процессуальном законодательстве. По-нашему мнению, необходимо дополнить УПК РФ рядом норм, конкретизирующих порядок применения правоохранительными органами информационных технологий и технических средств в рамках осуществления досудебного производства по делу и на судебной стадии рассмотрения дела.

Считаем, что организация процесса расследования преступлений следственными подразделениями ОВД РФ в части применения информационных технологий также нуждается в правовом совершенствовании со стороны законодателя. Это связано с наличием такого рода проблем, как: нехватка достаточного числа подготовленных сотрудников, которые обладали бы необходимыми знаниями, умениями и навыками для работы с информационными технологиями; отсутствуют методики расследования инновационных преступлений; нет надежных и эффективных информационно-аналитических решений; наблюдается рутинный характер при составлении процессуальных и не процессуальных документов; отсутствует необходимое материально-техническое оснащение следственных отделов.

Организация процесса расследования преступлений непрерывно связана и с осуществлением следственных действий в рамках того или иного уголовного дела, поэтому следователю необходимо обладать не просто навыками производства различных процессуальных действий, в том числе навыками производства следственных действий, но и уметь применять технические и информационные средства.

Уголовно-процессуальная регламентация порядка применения технических средств и информационных технологий при производстве следственных действий также нуждается в правовом совершенствовании. Так, нормы УПК РФ, регламентирующие изъятие «электронных носителей информации» вызывают сомнение, что связано с отсутствием должной правовой регламентации надлежащего порядка привлечения специалиста к процедуре изъятия электронного носителя и копирования информации, предусмотренного ст.164.1 УПК РФ, что в свою очередь отражается на качестве расследования уголовных дел, правильности сбора и оформления доказательств в виде информации на электронных носителях.

Полагаем, что решить озвученные проблемы можно следующими способами:

1. Осуществить обучение, переподготовку и повышение квалификации кадрового состава следственных подразделений ОВД РФ в образовательных учреждениях системы МВД России в целях овладения необходимыми знаниями, умениями и навыками по работе с информационно-техническими средствами. Немаловажное значение на эффективность процесса расследования преступлений окажет появление методик расследования преступлений в сфере компьютерной информации;

2. Оснастить следственные подразделения ОВД РФ достаточным количеством недостающих информационно-технических средств, которые могут быть полезны в процессе расследования конкретного преступления, к примеру, такими средствами как: средства выемки аппаратного обеспечения и электронных доказательств, средства дистанционной экспертизы оборудования и ликвидации информации, средства обработки и расшифровки данных и др., также необходимо обозначить направления совершенствования организации аналитической работы по формированию решений и заключений на основе анализа имеющейся информации. Считаем, что создание надежной системы обеспечения ОВД финансовыми средствами и материально-техническими ресурсами в соответствии с нормативами, а

также реформирование системы организации снабжения материальными ресурсами ОВД с учетом возложенных на них новых задач, а также экономических, политических и других факторов сможет разрешить проблему с ненадлежащим материально-техническим обеспечением следственных отделов.

3. Внести изменения в ч.2 ст.164.1 УПК РФ, а именно предоставить следователю возможность самостоятельно привлекать специалиста для изъятия электронных носителей информации, в случае, если требуются специальные познания. Считаем уместным рекомендовать проект Федерального закона «О внесении изменений в УПК РФ» (Приложение № 3).

4. Разработать «Электронное уголовное дело» и внедрить его на всех стадиях производства по уголовному делу. Внедрение в деятельность следственных подразделений ОВД РФ «электронного уголовного дела» позволит значительно сократить сроки расследования преступлений, поскольку работа в «электронном виде» будет вестись намного быстрее, а также будет способствовать оптимизации уголовно-процессуальной деятельности в целом. Придать электронному документу необходимую юридическую силу следует при помощи электронной цифровой подписи.

5. Внедрить в деятельность следственных подразделений ОВД РФ новое программное обеспечение, работающее по принципу системы искусственного интеллекта, широко применяемой в США системы «MauiNet». При этом, учитывая, что в Российской Федерации большинство хакерских атак осуществляются посредством социальных сетей, то предлагаем взять за основу основные функции данной системы, но адаптировать алгоритм ее действия с учетом возможного вредоносного софта в социальных сетях и применять на практике в деятельности следственных подразделений ОВД РФ. Внедрение системы искусственного интеллекта также будет способствовать повышению процента расследования сложных многоэпизодных преступлений и оптимизации уголовно-процессуальной деятельности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

РАЗДЕЛ 1 НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ И ИНЫЕ ОФИЦИАЛЬНЫЕ АКТЫ

- 1 «Конвенция о защите физических лиц при автоматизированной обработке персональных данных» от 28 января 1981г. Конвенция ратифицирована Федеральным законом 19 декабря 2005 г. №160-ФЗ. Конвенция вступила в силу для России 1 сентября 2003 г. //СЗ РФ. 2014. № 5.Ст.419.
- 2 Миланский план действий от 29 ноября 1985 г. (г. Милан) // Советская юстиция. 1992. № 13–14; № 15–16.
- 3 Окинавская хартия глобального информационного общества от 22 июля 2000 г. // Дипломатический вестник. 2000 г. № 8.
- 4 «Конвенция против транснациональной организованной преступности» от 15 ноября 2000 г. (г. Нью-Йорк) Конвенция ратифицирована Федеральным законом от 26 апреля 2004 г. № 26-ФЗ. Вступила в силу для России с 25 июня 2004 г. //СЗ РФ. 2004. № 40. Ст. 3882.
- 5 Декларация принципов «Построение информационного общества - глобальная задача в новом тысячелетии» принята 12 декабря 2003 г. // Законодательство и практика масс-медиа. 2004. № 1.
- 6 Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 177-ФЗ // СЗ РФ. 2001. № 51. Ст. 4921.
- 7 Федеральный закон «Об оперативно-розыскной деятельности» от 12 августа 1995 г. №144-ФЗ // СЗ РФ.1995. № 33. Ст. 3349.
- 8 Федеральный закон «О государственной дактилоскопической регистрации в Российской Федерации» от 25 июля 1998 г. № 128-ФЗ // СЗ РФ.1998.№31. Ст. 3806.
- 9 Федеральный закон «О связи» от 7 июля 2003 г. № 126 – ФЗ // СЗ РФ. 2003. № 28. Ст. 2895.

- 10 Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 № 149-ФЗ // СЗ РФ. 2006. № 31. Ст. 3448.
- 11 Федеральный закон «О полиции» от 7 февраля 2011 г. № 3-ФЗ // Российская газета. 2011. № 25.
- 12 Указ Президента РФ «Об упорядочении организации и проведения оперативно-розыскных мероприятий с использованием технических средств» от 1 сентября 1995 г. № 891 // СЗ РФ. 1999 г. № 24. Ст. 2954.
- 13 Указ Президента РФ «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» от 15 января 2013 г. № 31 // СЗ РФ. 2013 г. № 3. Ст. 178.
- 14 Указ Президента РФ «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы» от 9 мая 2017 г. № 203 // СЗ РФ. 2017. № 20. Ст. 2901.
- 15 Указ Президента РФ «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») от 10 октября 2019 г. № 490 // СЗ РФ. 2019. № 27. Ст. 2987.
- 16 Постановление Правительства РФ «Об утверждении Положения о ввозе в Российскую Федерацию и вывозе из Российской Федерации специальных технических средств, предназначенных для негласного получения информации, и списка видов специальных технических средств, предназначенных для негласного получения информации, ввоз и вывоз которых подлежат лицензированию» от 10 марта 2000 г. № 214 // СЗ РФ. 2000 г. № 12. Ст. 1292.
- 17 Постановление Правительства РФ «О единой системе межведомственного электронного взаимодействия» от 8 сентября 2010 г. № 697 // СЗ РФ. 2010 г. № 38. Ст. 4823.

- 18 Постановление Правительства РФ «О Межведомственной комиссии по вопросам, связанным с внедрением и развитием систем аппаратно-программного комплекса технических средств «Безопасный город» (с изменениями и дополнениями)» от 20 января 2014 г. № 39 // СЗ РФ. 2014 г. № 5. Ст. 498.
- 19 Информационно-аналитический портал правовой статистики Генеральной прокуратуры РФ. URL: <http://crimestat.ru/analytics> (дата обращения: 16.04.2021).

РАЗДЕЛ II ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

- 1 Абдулвалиев, А.Ф. Опять про электронное уголовное дело / А.Ф. Абдулвалиев // Право и политика. 2013. № 1. С. 15–18.
- 2 Автоматизированный информационный комплекс «Надзор» // Официальный сайт ООО «Электронные офисные системы»: URL: <https://www.eos.ru/search/?q=%C0%C8%CA+%CD%E0%E4%E7%EE%F0&s=%CF%EE%E8%F1%EA> (дата обращения 18.04.2021).
- 3 Александров, А.С., Андреева, О.М., Зайцев, О.А. О перспективах развития российского уголовного судопроизводства в условиях цифровизации / А.С. Александров, О.М. Андреева, О.А. Зайцев // Вестник Томского государственного университета. 2019. № 488. С.199–207.
- 4 Аппаратно-программный комплекс «Поток» // Официальный сайт ЗАО «РОССИ»: URL: <http://www.rossi-potok.ru/ru/> (дата обращения: 16.04.2021).
- 5 Афанасьев, А.Ю. Искусственный интеллект или интеллект субъектов выявления, раскрытия и расследования преступлений: что победит? / А.Ю. Афанасьев // Научный журнал. 2018. № 3 (38). С. 28–34.
- 6 Балакшин, В.С., Литвин, И.И. Современные технические средства и проблемы их применения в доказывании на досудебных стадиях

- уголовного судопроизводства / В.С. Балакшин, И.И. Литвин. М.: Юрлитинформ, 2020. 168 с.
- 7 Баринов, Н.А. Гражданско-правовые проблемы удовлетворения имущественных потребностей советских граждан: автореф. дис. ... докт. юрид. наук / Н.А. Баринов. М., 1988. 33 с.
 - 8 Белозеров, О.И., Андрейченко П.М. Тенденции развития информационных технологий в системе правоохранительной деятельности / О.И. Белозеров, П.М. Андрейченко // Научный журнал. 2019. № 10 (44). С.10–13.
 - 9 Бертовский, Л.В. Криминалистика: учебник / Л.В. Бертовский. М.: РГ-пресс, 2018. 960 с.
 - 10 Богатырева, Л.И. Анализ основных кадровых тенденций в следственных подразделениях МВД России на современном этапе / Л.И. Богатырева // Закон и право. 2019. № 4. С. 133–136.
 - 11 Вехов, В.Б. Основные направления использования компьютерных технологий в деятельности следователя / В.Б. Вехов // Информационная безопасность регионов. 2007. № 1(1). С.59–65.
 - 12 Вехов, В.Б., Васюков, В.Ф. Получение компьютерной информации от организаторов ее распространения в сети Интернет при расследовании преступлений / В.Б. Вехов, В.Ф. Васюков // Российский следователь. 2018. № 3. С.11–15
 - 13 Вехов, В.Б., Зуев, С.В. Расследование преступлений в сфере компьютерной информации и электронных средств платежа: учебное пособие для вузов / В. Б. Вехов, С. В. Зуев. М.: Юрайт, 2021. 243 с.
 - 14 Воскобитова, Л.А. Уголовное судопроизводство и цифровые технологии: проблемы совместимости / Л.А. Воскобитова // Lexrussica. 2019. № 5 (150). С. 91–104.
 - 15 Гаврилин, Ю.В., Балашова, А.А. Совершенствование процессуального порядка собирания доказательственной информации, содержащейся в

- сетевых информационных системах / Ю.В. Гаврилин, А.А. Балашова // Криминалистика: вчера, сегодня, завтра. 2020. № 1 (13). С. 129–137.
- 16 Головкин, Л.В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция? / Л.В. Головкин // Вестник экономической безопасности. 2019. № 1. С.15–25.
- 17 Гриднева, О.В. Гражданское право: учебное пособие / под ред. О.В. Гриднева, Л.И. Кулешова, М.Р. Мегрелидзе / О.В. Гриднева. М.: Юриспруденция, 2012. 158 с.
- 18 Гридюшко, П.В., Бушкевич Н.С. Об электронной форме ведения уголовного процесса / П.В. Гридюшко, Н.С. Бушкевич // Вестник Академии МВД Республики Беларусь. 2017. № 2 (34). С. 67–73.
- 19 Гришин, Д.А. Совершенствование применения информационных технологий в досудебных стадиях уголовного судопроизводства / Д.А. Гришин // Вестник Московского университета МВД России. 2019. № 3. С.119–122.
- 20 Давыдов, В.А., Качалова, О.В. Современные тенденции развития российского уголовного судопроизводства / В.А. Давыдов, О.В. Качалова // Вестник Томского государственного университета. 2018. № 29. С.69–78.
- 21 Добровлянина, О.В. Некоторые аспекты о процессуальном изъятии (копировании) электронных носителей информации / О.В. Добровлянина // Пермский юридический альманах. 2019. № 2. С.641–649.
- 22 Долгов, А.М. Электронное уголовное дело в досудебных стадиях уголовного процесса в России / А.М. Долгов // Общество: политика, экономика, право. 2018. № 9 (62). С. 30–33.
- 23 Дремлюга, Р.И. Компьютерная информация как предмет посягательства при неправомерном доступе: сравнительный анализ законодательства США и России / Р.И. Дремлюга // Журнал зарубежного и сравнительного правоведения. 2018. № 6 (73). С. 84–92.

- 24 Жданов, Ю.Н., Овчинский, В.С. Полиция будущего / Ю.Н. Жданов, В.С. Овчинский. М.: Международные отношения, 2018. 166 с.
- 25 Зазулин, А.И. Правовые и методологические основы использования цифровой информации в доказывании по уголовным делам: дис. ... канд. юрид. наук / А.И. Зазулин. Екатеринбург, 2018. 251 с.
- 26 Зайцев, О.А., Пастухов П.С. Формирование новой стратегии расследования преступлений в эпоху цифровой трансформации / О.А. Зайцев, П.С. Пастухов // Вестник Пермского университета. Юридические науки. 2019. № 46. С.752–777.
- 27 Зуев, С.В. IT-справочник следователя / С.В. Зуев [и др.]. М.: Юрлитинформ, 2019. 232 с.
- 28 Зуев, С.В. Информационные технологии в уголовном процессе зарубежных стран / С.В. Зуев [и др.]. М.: Юрлитинформ, 2020. 216 с.
- 29 Зуев, С.В. Основы теории электронных доказательств / С.В. Зуев [и др.]. М.: Юрлитинформ, 2019, 400 с.
- 30 Зуев, С.В. Развитие информационных технологий в уголовном судопроизводстве / С.В. Зуев [и др.]. М.: Юрлитинформ, 2018. 248 с.
- 31 Зуев, С.В. Цифровизация судопроизводства. Научно-практический (постатейный) комментарий правовых актов / С.В. Зуев [и др.]. М.: Юрлитинформ, 2020. 320 с.
- 32 Зуев, С.В. Электронное уголовное дело: за и против / С.В. Зуев // Правопорядок: история, теория, практика. 2018. № 4 (19). С. 6–12.
- 33 Зуев, С.В., Черкасов В.С. Новые правила изъятия электронных носителей и копирования информации / С.В. Зуев, В.С. Черкасов // Законность. 2019. № 5 (1015). С. 40–43.
- 34 Зуев, С.В., Черкасов В.С. Новые правила изъятия электронных носителей и копирования информации (статья 1641 УПК РФ): преимущества и недостатки новеллы / С.В. Зуев, В.С. Черкасов // Сибирское юридическое обозрение. 2019. № 16 (2). С. 193–197.

- 35 Зуев, С.В., Черкасов, В.С. Новые правила изъятия электронных носителей и копирования информации (статья 1641 УПК РФ) преимущества и недостатки новеллы / С.В. Зуев, В.С. Черкасов // Сибирское юридическое обозрение.2019.№ 2.С.193–197.
- 36 Ишин,А.М. Информационное обеспечение предварительного расследования преступлений: некоторые современные аспекты// Вестник Балтийского федерального университета им. И. Канта. Серия: Гуманитарные и общественные науки.2016.№ 4.С.21–28.
- 37 Козловский, П.В., Седельников, П.В. Участие специалиста в изъятии электронных носителей / П.В. Козловский, П.В. Седельников // Научный вестник Омской академии МВД России.2014. № 1 (52). С.17–19.
- 38 Крюкова, Т.С. Некоторые вопросы изъятия электронных носителей информации в ходе производства следственных действий: анализ судебной практики / Т.С. Крюкова // Правопорядок: история, теория, практика. 2016. № 4 (11). С.61–63.
- 39 Кузьмин, И.А. Искусственные нейронные сети: перспективы использования в правоохранительной деятельности / И.А. Кузьмин// Криминалистика: вчера, сегодня, завтра. 2018. № 4 (8). С. 109– 116.
- 40 Кузьмин, И.А. Искусственные нейронные сети: перспективы использования в правоохранительной деятельности / И.А. Кузьмин //Криминалистика: вчера, сегодня, завтра. 2018.№ 4(8).С.109–116.
- 41 Ленов, А.И., Смагин, П.Г. Использование информационных технологий при производстве следственных действий, в том числе связанных с ограничением конституционных прав граждан / А.И. Ленов, П.Г. Смагин // Вестник Тамбовского университета. 2011.№ 9 (101).С.345–349.
- 42 Леонов, А.И., Смагин, П.Г. Использование информационных технологий при производстве следственных действий, в том числе связанных с ограничением конституционных прав граждан / А.И.

- Леонов, П.Г. Смагин // Вестник Тамбовского университета. 2011. № 9 (101). С. 345–349.
- 43 Лозовский, Д.Н., Ахриев, М.Т. Особенности производства обыска (выемки), связанного с изъятием электронных носителей информации / Д.Н. Лозовский, М.Т. Ахриев // Гуманитарные, социально-экономические и общественные науки. 2018. № 7. С. 120. С. 117–120.
- 44 Медведева, М.О. Уголовно-процессуальная форма информационных технологий: современное состояние и основные направления развития: дис. ... канд. юрид. наук. М., 2018. 250 с.
- 45 Муженская, Н.Е., Костылева, Г.В. Руководство для следователя и дознавателя по расследованию отдельных видов преступлений: практическое пособие: в 2 частях, Ч. I. М.: Проспект, 2015. 640 с.
- 46 Муратова, Н.Г., Сергеев М.С. Правовое регулирование применения электронной информации и электронных носителей информации в уголовном судопроизводстве: отечественный и зарубежный опыт: монография / Н.Г. Муратова, М.С. Сергеев. М.: Юрлитинформ, 2019. 264 с.
- 47 Овчинникова, О.В. Дистанционные следственные действия: современное состояние и перспективы / О.В. Овчинникова // Юридическая наука и правоохранительная практика. № 1 (47). 2019. С. 108–116.
- 48 Овчинникова, О.В. Собираение электронных доказательств, размещенных в сети Интернет / О.В. Овчинникова // Правопорядок: история, теория и практика. 2016. № 4 (11). С. 67–70.
- 49 Овчинский, В.С. Виртуальный щит и меч: США, Великобритания, Китай в цифровых войнах будущего / В.С. Овчинский. М.: Книжный мир, 2018. 320 с.
- 50 Олиндер, Н.В. К вопросу о доказательствах, содержащих цифровую информацию / Н.В. Олиндер // Юридический вестник Самарского университета. 2017. № 3. С. 107–110.

- 51 Осипенко, А.Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт / А.Л. Осипенко. М.: Норма, 2004. 432 с.
- 52 Рясов, А.А., Жигалова, Г.Г., Аветисян, А.Д. Особенности подготовки следователей, специализирующихся на расследовании преступлений, совершаемых с использованием современных информационно-коммуникационных технологий / А.А. Рясов, Г.Г. Жигалова, А.Д. Аветисян // Мир науки, культуры, образования, 2018.№ 4 (71) . С.67–72.
- 53 Сарапулов, А.А. Информационные технологии в уголовном процессе: история, современное состояние, перспективы/А.А. Сарапулов // Вестник Южно-Уральского государственного университета. 2013. № 2. С.107–108.
- 54 Сарапулов, А.А. Информационные технологии в уголовном процессе: история, современное состояние, перспективы / А.А. Сарапулов //Вестник Южно-Уральского государственного университета. 2013. № 2.С.107–108.
- 55 Сарычев, А.В., Архипцев И.Н. Современное состояние раскрытия и расследования преступлений, совершаемых с использованием информационных технологий / А.В. Сарычев, И.Н. Архипцев // Проблемы правоохранительной деятельности.2020. № 1(39). С.36–41.
- 56 Смарин, В.И., Луцик, В.В. Уголовный процесс европейских государств: монография / В.И. Смарин, В.В Луцик. М.: Проспект, 2018.752 с.
- 57 Стельмах, В.Ю. Проблемы процессуальной регламентации следственных действий, направленных на получение сведений, передаваемых по средствам электросвязи / В.Ю. Стельмах // Юридическая наука и правоохранительная практика.2013.№ 3 (25).С.108–113.
- 58 Стурова, Н.А. Некоторые особенности тактики производства следственных действий, направленных на получение доказательств в

- электронной форме / Н.А. Стурова // Юристъ-правоведь.2019. № 2 (89). С. 226–231.
- 59 Суходолов, А.П., Бычкова А.М. Искусственный интеллект в противодействии преступности, ее прогнозировании, предупреждении и эволюции / А.П. Суходолов, А.М. Бычкова // Всероссийский криминологический журнал. 2018. № 6. С. 753–756.
- 60 Тарасов, М.А. О некоторых проблемах правового регулирования применения технических средств в уголовном судопроизводстве / М.А. Тарасов // Вестник Южно-Уральского государственного университета. 2009. № 40(173). С.71–77.
- 61 Трефилов, А.А. Уголовный процесс зарубежных стран / А.А. Трефилов. М.: НИПКЦ Восход-А, 2019. 1024 с.
- 62 Федюнин, А.Е. Правовое регулирование технических средств в уголовном процессе: автореф. дис. ... докт. юрид. наук. / А.Е. Федюнин. Саратов, 2008. 46 с.
- 63 Хабриева, Т.Я., Черногор, Н.Н. Право в условиях цифровой реальности / Т.Я. Хабриева, Н.Н. Черногор // Журнал российского права. 2018. № 1 (253). С.85–102.
- 64 Химичева, О.В., Андреев, А.В. Цифровизация как тренд развития современного уголовного процесса / О.В. Химичева, А.В. Андреев // Вестник Московского университета МВД России.2020.№ 3.С.21–23.
- 65 Шевко, Н.Р. Проблемы подготовки специалистов по раскрытию и расследованию и преступлений, совершенных с использованием современных информационных технологий, в образовательных организациях МВД России / Н.Р. Шевко // Вестник Казанского юридического института МВД России. 2017. № 1 (27). С.87–89.

РАЗДЕЛ III ПОСТАНОВЛЕНИЯ ВЫСШИХ СУДЕБНЫХ ИНСТАНЦИЙ И
МАТЕРИАЛЫ ЮРИДИЧЕСКОЙ ПРАКТИКИ

- 1 Апелляционное определение Судебной коллегии по уголовным делам Оренбургского областного суда № 22–4229/2016 от 03 ноября 2016 г. URL:<https://base.garant.ru/144577943/> (дата обращения 20.03.2021).
- 2 Апелляционное постановление Соликамского городского суда Пермского края № 10–83/2017 от 17 октября 2017 г. URL:<http://sudact.ru> (дата обращения: 20.03.2021).

Анкета для сотрудников ОВД.

Уважаемые сотрудники правоохранительных органов!

Юридический институт Южно-Уральского государственного университета проводит исследование на тему: «Цифровизация деятельности следственных подразделений органов внутренних дел» с целью разработки комплекса мер по повышению эффективности правоохранительной деятельности и совершенствованию законодательства в сфере информационно-цифровых технологий. Просим Вас принять участие в анкетировании и ответить на предложенные вопросы.

1. Считаете ли Вы целесообразным дополнить УПК РФ рядом норм, конкретизирующих порядок использования информационных технологий и технических средств?

а) Да;

б) Нет;

в) Затрудняюсь ответить.

2. Согласны ли Вы с тем, что следователю необходимо предоставить возможность самостоятельно привлекать специалиста для изъятия электронных носителей информации, в случае, если требуются специальные познания?

а) Да, согласен;

б) Нет, не согласен;

в) Затрудняюсь ответить.

3. Считаете ли Вы, что на сегодняшний день отсутствует достаточная профессиональная подготовка кадрового состава следственных подразделений ОВД по работе с информационно-техническими средствами?

а) Да, считаю;

б) Нет, считаю, что сотрудники обладают достаточными навыками;

в) Затрудняюсь ответить.

4. Как Вы считаете, окажет ли существенную помощь в расследовании преступлений внедрение системы искусственного интеллекта?

а) Да;

б) Нет;

в) Затрудняюсь ответить.

5. Нуждаетесь ли Вы в повышении квалификации для работы с информационно-техническими средствами?

а) Да;

б) Нет;

в) Затрудняюсь ответить.

6. Как Вы считаете, на сегодняшний день в следственных подразделениях ОВД присутствует дефицит материально-технического оснащения?

а) Да;

б) Нет;

в) Затрудняюсь ответить.

7. Считаете ли Вы необходимым внедрить «Электронное уголовное дело» в целях оптимизации уголовно-процессуальной деятельности следователя?

а) Да;

б) Нет;

в) Затрудняюсь ответить.

Спасибо за участие!

Анализ результатов анкетирования

В ходе научного исследования проблем, обозначенных в выпускной квалификационной работе, был проведён социологический опрос среди сотрудников Отдела по расследованию преступлений на территории, обслуживаемой отделом полиции «Центральный» СУ УМВД России по г. Челябинску на тему: «Цифровизация деятельности следственных подразделений органов внутренних дел» в связи с разработкой комплекса эффективных мер по повышению эффективности правоохранительной деятельности и совершенствованию законодательства в сфере информационно-цифровых технологий. Всего было опрошено 16 человек, находящихся в должности следователей.

По результатам проведенного исследования большинство респондентов поддержали разработанные нами предложения по изменению законодательства и повышению эффективности правоохранительной деятельности в сфере информационно-цифровых технологий.

Детальный анализ результатов опроса представлен на соответствующих диаграммах.

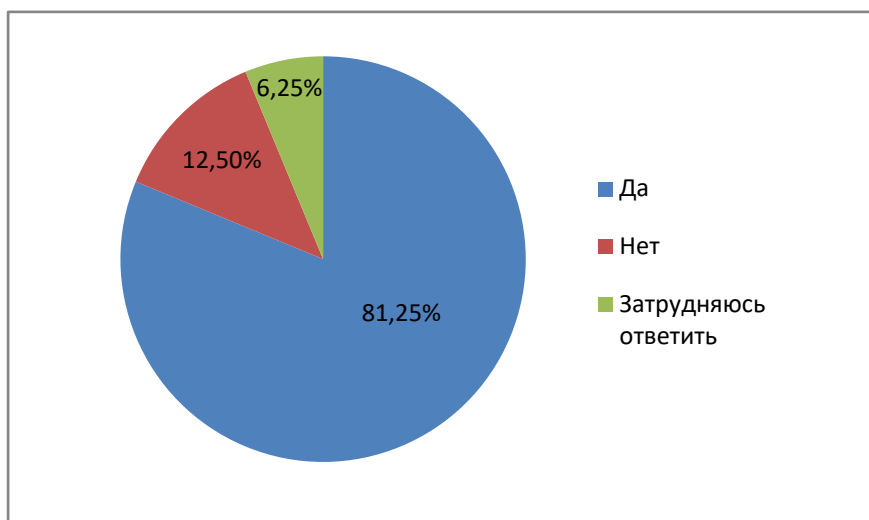


Рисунок 1 – Диаграмма, отражающая результаты опроса по поводу дополнения УПК РФ рядом норм, конкретизирующих порядок использования информационных технологий и технических средств (Вопрос №1).

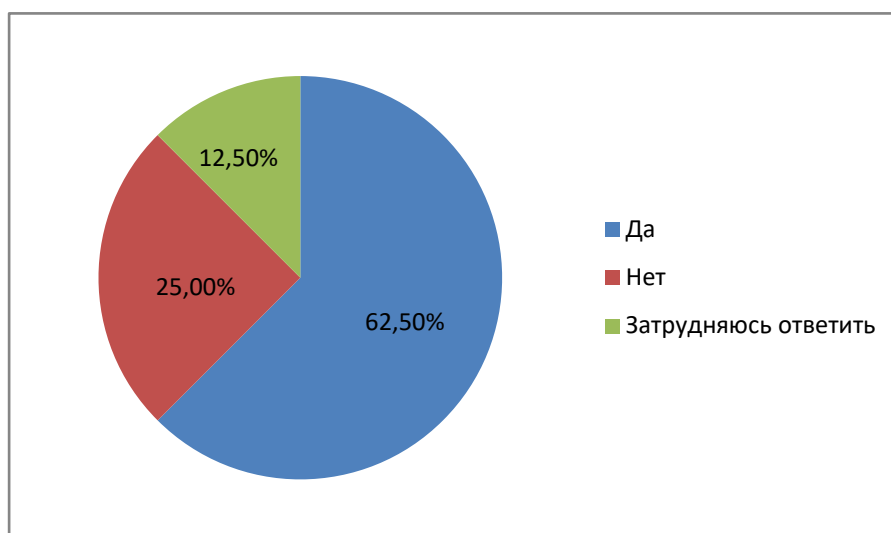


Рисунок 2 – Диаграмма, отражающая мнение респондентов относительно возможности предоставления следователю права самостоятельно привлекать специалиста для изъятия электронных носителей информации, в случае, если требуются специальные познания(Вопрос №2).

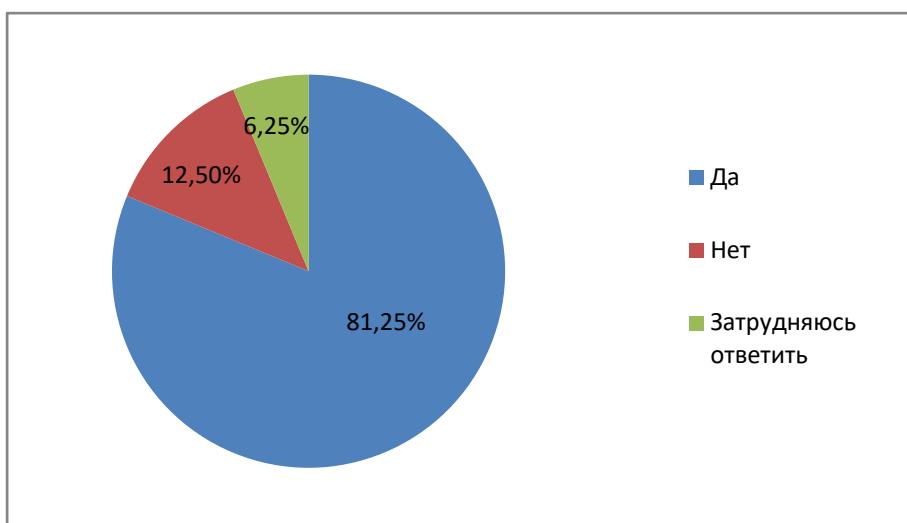


Рисунок 3 – Диаграмма, отражающая мнение респондентов о достаточности профессиональной подготовки кадрового состава следственных подразделений ОВД по работе с информационно-техническими средствами (Вопрос №3).

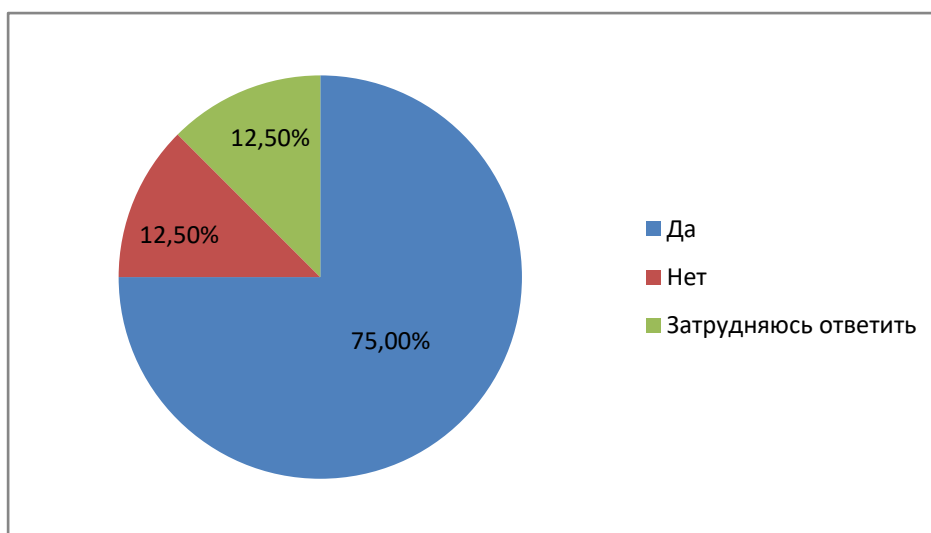


Рисунок 4 – Диаграмма, отражающая мнение респондентов относительно внедрения в правоохранительную деятельность системы искусственного интеллекта (Вопрос №4).

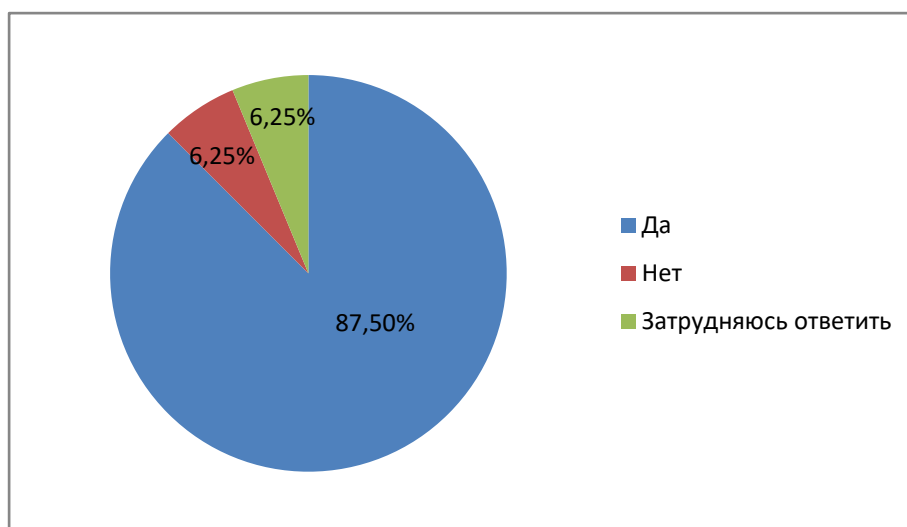


Рисунок 5 – Диаграмма, отражающая мнение респондентов относительно нуждемости в повышении квалификации для работы с информационно-техническими средствами(Вопрос №5).

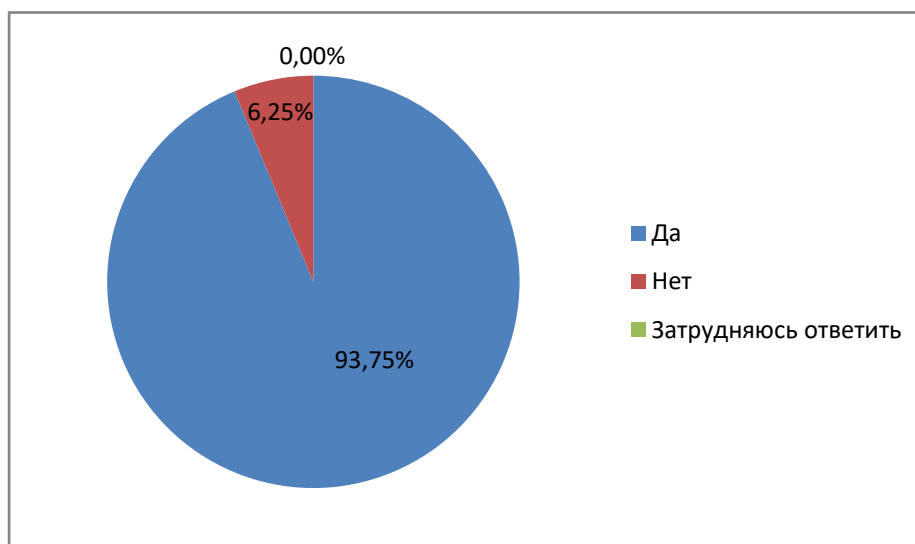


Рисунок 6 – Диаграмма, отражающая результаты опроса о наличии дефицита материально-технического оснащения в следственных подразделениях ОВД РФ(Вопрос №6).

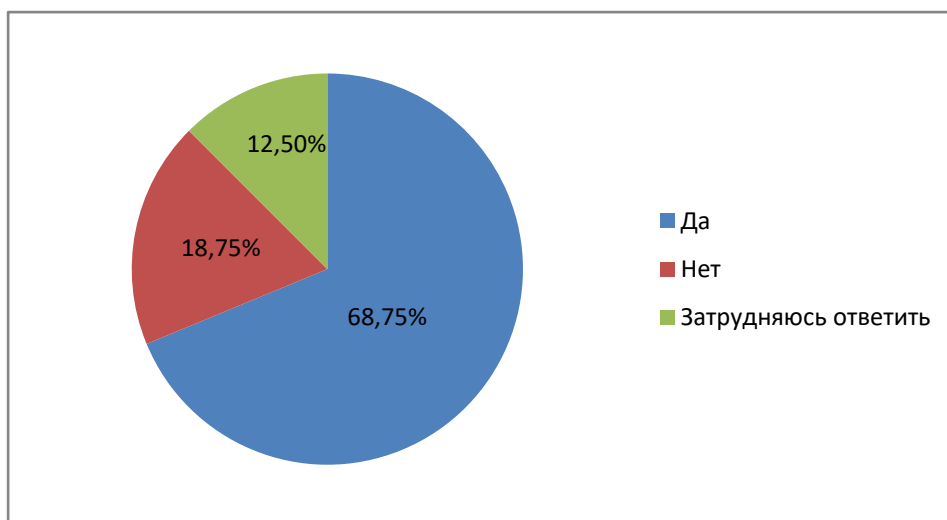


Рисунок 7 – Диаграмма, отражающая мнение респондентов по поводу необходимости внедрения «электронного уголовного дела» в деятельность следственных подразделений ОВД РФ (Вопрос №7).

ПРОЕКТ ФЕДЕРАЛЬНОГО ЗАКОНА
РОССИЙСКАЯ ФЕДЕРАЦИЯ
ФЕДЕРАЛЬНЫЙ ЗАКОН О ВНЕСЕНИИ ИЗМЕНЕНИЙ В УПК РФ от
18.12.2001 г. № 174-ФЗ

Статья 1. Внести в часть 2 статьи 164.1 УПК РФ следующее изменение:

1. Изменить в статье положение, предусмотренное частью 2 статьи 164.1 УПК в следующей формулировке: «Электронные носители информации изымаются в ходе производства следственных действий следователем самостоятельно в случае, если не требуются специальные познания для их изъятия».

2. Изложить часть 2 статьи 164.1 УПК РФ в следующей редакции:

«2. Электронные носители информации изымаются в ходе производства следственных действий следователем самостоятельно в случае, если не требуются специальные познания для их изъятия. По ходатайству законного владельца изымаемых электронных носителей информации или обладателя содержащейся на них информации специалистом, участвующим в следственном действии, в присутствии понятых с изымаемых электронных носителей информации осуществляется копирование информации. Копирование информации осуществляется на другие электронные носители информации, предоставленные законным владельцем изымаемых электронных носителей информации или обладателем содержащейся на них информации. Копирование информации не осуществляется при наличии обстоятельств, указанных в пункте 3 части первой настоящей статьи. Электронные носители информации, содержащие скопированную информацию, передаются законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации. Об осуществлении копирования информации и о передаче электронных

носителей информации, содержащих скопированную информацию, законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации в протоколе следственного действия делается запись».

Статья 2. Настоящий Федеральный закон вступает в силу со дня его официального опубликования.

Президент

Российской Федерации