

Министерство внутренних дел Российской Федерации

Федеральное государственное казенное образовательное учреждение
высшего образования «Казанский юридический институт Министерства
внутренних дел Российской Федерации»

Кафедра уголовного процесса

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

**на тему: «Уголовно-процессуальные аспекты использования
электронных носителей информации в уголовном судопроизводстве»**

Выполнил: Веселова Анна Олеговна
(фамилия, имя, отчество)

Правоохранительная деятельность,
2015 года набора, 051 учебная группа
(специальность, год набора, № группы)

Руководитель:
к.ю.н., старший преподаватель кафедры
уголовного процесса КЮИ МВД России
капитан полиции
(ученая степень, ученое звание, должность)

Гарипов Тимур Ильгизович
(фамилия, имя, отчество)

Рецензент:
Начальник ОУР ОП №16 «Япеева»
УМВД России по г.Казани
подполковник полиции
(должность, специальное звание)

Газизов Ильшат Наилевич
(фамилия, имя, отчество)

Начальник кафедры _____

Дата защиты: «__» _____ 2020 г. Оценка _____

Рег. № _____ «__» _____ 2020г.

Казань 2020

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	3
ГЛАВА 1. ЭЛЕКТРОННАЯ ИНФОРМАЦИЯ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ КАК ИСТОЧНИК ДОКАЗАТЕЛЬСТВ: ПОНЯТИЕ И СУЩНОСТЬ	8
§1. Правовая регламентация применения электронной информации и электронных носителей информации в уголовно-процессуальном законодательстве РФ.....	8
§2. Зарубежный опыт использования электронной информации в уголовном судопроизводстве в качестве доказательства.....	23
ГЛАВА 2. УГОЛОВНО-ПРОЦЕССУАЛЬНЫЕ И ОРГАНИЗАЦИОННЫЕ АСПЕКТЫ ОБНАРУЖЕНИЯ, ИЗЪЯТИЯ И ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ИНФОРМАЦИИ ПРИ ПРОИЗВОДСТВЕ ПО УГОЛОВНОМУ ДЕЛУ	38
§1. Уголовно-процессуальная форма и способы получения информации, содержащейся в электронных носителях и электронных сообщениях.....	38
§2. Процессуальные и организационные аспекты производства по уголовному делу в электронном виде.....	48
ЗАКЛЮЧЕНИЕ	58
СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ	65
ПРИЛОЖЕНИЯ.....	71

ВВЕДЕНИЕ

Сегодня с уверенностью можно сказать, что информационные технологии все больше и больше внедряются в современное сознание людей. С каждым днем возникает необходимость все более усовершенствовать коммуникации в сфере информационных технологий. Искусственный интеллект, виртуальная реальность, новейшие разработки – все это доступно нашему обществу на сегодняшний день.

Значительную роль в системе доказывания по уголовным делам играет применение инструментов познания касательно электронной информации.

Правоохранительными органами в целях расследования и раскрытия преступлений используются записи с камер видеонаблюдения, расположенных в различных учреждениях и организациях. Криминалистика также не стоит на месте и уже становится доступным фиксировать следы преступления с помощью цифровых технологий, а также использовать распознавание голоса, внешности преступника, тем самым повышая эффективность раскрытия преступлений.

С использованием новейших компьютерных технологий преступники придумывают все более новые способы совершения преступлений против собственности. Уголовным Кодексом Российской Федерации (далее – УК РФ)¹ закреплён перечень преступных деяний, совершенных с использованием средств вычислительной техники.

В течение последних 8 лет в УК РФ наряду с имеющимися статьями по «информационным» составам преступлений (ст. 146, 183, 187, 242, 242.1, 272 - 274 УК РФ) появились статьи 128.1, 137, 138.1, 159.6, 171.1, 185.3, 228.1, где предусматривается ответственность за использование для совершения преступления электронных, информационно-телекоммуникационных сетей (включая сеть Интернет). Однако, особое внимание необходимо обратить на

¹ Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // СЗ РФ. 1996. № 25. Ст. 2954.

активную деятельность законодателя с июня 2017 года до настоящего момента, выражающуюся в принятии целого ряда новых статей УК РФ - ст. 110, 110.1, 110.2, 151.2, что, безусловно, свидетельствует о повышении уровня государственной защиты правоотношений с информационными элементами

В свою очередь, Уголовно-процессуальный кодекс РФ (далее – УПК РФ)¹ как нормативный акт, направленный на реализацию уголовно-правовых норм, также вводит новые нормы, предусматривающие раскрытие преступлений, совершаемых с использованием информационно-телекоммуникационных средств. Так, УПК РФ был дополнен ст.164.1, предусматривающей особенности изъятия электронных носителей информации (далее – ЭНИ). Кроме того, в сфере уголовного судопроизводства накоплен немалый опыт применения технических средств, например, аудио- и видеозаписи, позволяющих объективно и точно фиксировать весь процесс доказывания. Базовой правовой нормой в данном случае можно рассматривать ч. 6 ст. 164 УПК РФ, которая предусматривает применение технических средств и способов обнаружения, фиксации и изъятия следов преступления и вещественных доказательств при производстве следственных действий.

Развитие новейших технологий подталкивает к внесению изменений в Российское законодательство, так как нет определенных норм, регулирующих использование электронных доказательств в рамках уголовного дела, а также систематизированного ведения материалов уголовного дела в электронной форме.

Несмотря на то, что сам факт установления процессуальной регламентации использования ЭНИ в уголовном судопроизводстве, бесспорно, является позитивным моментом, со дня принятия Федерального закона от 17.04.2017 № 73-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» до настоящего времени остается неразрешенным ряд вопросов и достаточно очевидных противоречий.

¹ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 24.04.2020) // СЗ РФ. 2001. № 52 (ч. I). Ст. 4921.

Во-первых, на законодательном уровне не разрешен вопрос о понятии электронных носителей информации. При таких обстоятельствах большинство авторов, исследующих данный вопрос¹, используют определение, содержащееся в п. 3.1.9. ГОСТ 2.051-2013 «Единая система конструкторской документации. Электронные документы. Общие положения», согласно которому под электронным носителем понимается «материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники». При этом не трудно заметить, что под данное определение попадает абсолютно любое микропроцессорное устройство.²

Во-вторых, остается нерешенным вопрос – следует ли относить электронные (цифровые) доказательства к отдельному виду доказательств, либо к иным документам?

В-третьих, нет должного процессуального регулирования вопросов, касающихся собирания, закрепления и оценки цифровой информации в процессе досудебного расследования по уголовному делу. Также нет определенной систематизации всех доказательств, полученных на основе использования электронных носителей информации в единую базу.

Исходя из этого, выбранный курс исследования помогает найти направление реформирования и модернизации уголовно-процессуального законодательства с учетом Указа Президента РФ от 09.05.2017 № 203 «О стратегии развития информационного общества в Российской Федерации на 2017-2030 годы»³.

Необходимость исследования проблем закрепления информационных технологий в уголовно-процессуальной деятельности, а также разработки

¹ Васюков В.Ф., Булыжкин А. В. Изъятие электронных носителей информации при расследовании преступлений: нерешенные проблемы правового регулирования и правоприменения // Российский следователь. 2016. № 6.

² Кучин О. С. Электронные носители информации в криминалистике. М., 2017. С. 67

³ О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы: Указ Президента РФ от 9 мая 2017 г. № 203 // Доступ из справ.-правовой системы «КонсультантПлюс».

возможности внедрения современных информационных технологий были подтверждены результатами проведенного нами анкетирования следователей, дознавателей, а также сотрудников уголовного розыска.

Обозначенные проблемы обуславливают **актуальность** темы исследования и подталкивают к необходимости формирования теоретической базы, которая позволила бы российскому законодательству подстраиваться в будущем под изменения в сфере высоких технологий.

Цель исследования состоит в изучении правовых и процессуальных аспектов электронной информации и ее носителей в уголовном судопроизводстве России.

Задачи исследования:

- рассмотреть правовую регламентацию информационных процессов в РФ,
- охарактеризовать доказательственное значение электронной информации и ее носителей в уголовном процессе,
- выявить особенности процессуального порядка производства следственных действий, направленных на получение электронной доказательственной информации,
- рассмотреть формы использования специальных знаний в ходе досудебного производства процессуальных действий в отношении электронных носителей информации.

Объект исследования – общественные отношения, возникающие при использовании электронной информации на электронных носителях в уголовном судопроизводстве.

Предмет исследования – представляет собой нормы уголовно-процессуального права, регулирующие использование электронной информации и их носителей в уголовном судопроизводстве, материалы следственно-судебной практики, научная литература.

Общие теоретические положения об уголовно-процессуальной форме информационных технологий в уголовном процессе были исследованы в

трудах А.Р.Белкина, А.В. Бойчука, А.В.Булыжкина, В.Ф.Васюкова, В.Н.Григорьева, Е.В.Горкина, К.Е. Демина, О.А.Зайцева, О.С.Кучина и др.

Методология и методика научного исследования основана на диалектическом принципе научного познания, позволяющем применить общенаучные и специальные методы. Общенаучные методы такие, как синтез, анализ, обобщение, статистическая обработка. Специальные методы такие, как историко-правовой, сравнительно-правовой, формально-логический, и метод анкетирования.

Эмпирическая основа исследования. В ходе исследования изучены материалы следственно-судебной практики, проведен социологический опрос практических работников, использованы данные судебной статистики.

Структура работы состоит из введения, двух глав, заключения, списка литературы.

ГЛАВА 1. ЭЛЕКТРОННАЯ ИНФОРМАЦИЯ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ КАК ИСТОЧНИК ДОКАЗАТЕЛЬСТВ: ПОНЯТИЕ И СУЩНОСТЬ

§1. Правовая регламентация применения электронной информации и электронных носителей информации в уголовно-процессуальном законодательстве РФ

Активное развитие информационных и коммуникационных технологий позволяют преступникам использовать все более усовершенствованные способы совершения преступлений, прежде всего экономической направленности, против общественной безопасности и общественного порядка и др.¹ Большинство граждан переходят от бумажных денежных средств к электронным, что позволяет совершать преступникам мошеннические действия с банковскими картами. С помощью банкоматов, терминалов, мобильных устройств осуществляется перевод денежных средств.

Изучая статистические данные, за киберпреступления в 2014 году были осуждены 218 человек, в 2015 году – 235, в 2016 году – 185, в 2017 году 203 человека.²

Так, согласно п. 19 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» существует такое понятие как электронное средство платежа - это средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверить и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей

¹ Гаврилин Ю. В. Расследование преступлений, посягающих на информационную безопасность в сфере экономики: теоретические, организационно-тактические и методические основы: автореф. дис. ... д-ра юрид. наук. М., 2010. С.135

² Преступность и правонарушения (2013 - 2017 гг.): Стат. сборник. МВД России. М., 2018. С. 156.

информации, в том числе платежных карт, а также иных технических устройств¹.

За январь – август 2019 г. правоохранными органами Российской Федерации зарегистрировано 180 153 (+66,8 %) преступления, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, предварительно расследовано – 42 212 (+49 %). Ущерб от преступлений (по оконченным и приостановленным уголовным делам и материалам об отказе в возбуждении уголовного дела по нереабилитирующим основаниям) составил 438 558 450 тыс. рублей, что на 9,8 % больше аналогичного показателя прошлого года.²

Однако так же необходимо учитывать высокий уровень латентности указанного вида преступлений. Большая часть преступлений, совершенных с использованием информационно-телекоммуникационных технологий, совершаются исключительно из корыстных побуждений, что означает их повышенную опасность для общества.

На сегодняшний день отмечается высокий рост производства компьютерной техники. Планшеты, смартфоны, компьютеры все больше и больше завладевают сознанием людей, особенно подрастающего поколения, что в свою очередь ставит под угрозу информационную безопасность Российской Федерации.

С момента принятия УПК РФ и по настоящее время законодателем проводится реформирование нормативного регулирования использования информационных технологий в уголовном процессе. Нормы УПК не успевают подстраиваться под современные реалии, и многие вопросы, касающиеся электронных носителей информации, не остаются рассмотренными. Все изменения в современном информационном обществе постоянно требуют

¹ О национальной платежной системе: Федеральный закон от 27.06.2011 № 161-ФЗ (ред. от 03.07.2016) (с изм. и доп., вступ. в силу с 17.07.2017) // Доступ из справ.-правовой системы «Консультант Плюс».

² Статистический сборник «Состояние преступности в России за август 2019 г.» // Стат. сборник. МВД России. М., 2019. С. 112.

пристального внимания со стороны законодателя и необходимостью разработки положений связанных с изъятием, хранением, обработкой, передачей электронной информации, а также представления и направления ее в суд в качестве электронного доказательства. В связи с этим необходимо закрепить базовые понятия, которые касаются места и роли электронных носителей информации в уголовном судопроизводстве.

В Уголовно-процессуальном кодексе Российской Федерации не содержится таких понятий, как информационные технологии, технические средства, электронное доказательство, электронные носители информации. Фактически можно сказать, что процессуальные нормы не соответствуют реальности использования в обществе информационных технологий.

Все технические средства функционируют на основе двух процессов – аналоговых и цифровых. Передача информации от одного субъекта к другому, передача закодированного сигнала в информационно - телекоммуникационную сеть «Интернет» происходит посредством информационных технологий.

Федеральный закон «Об информации, информационных технологиях и о защите информации»¹ содержит легальное определение «информационной технологии», определяемой как «процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов».

Ю.Г. Коротенков рассматривает информационные технологии как: «атрибуты, являющиеся совокупностью методов, способов и средств и обеспечивающие информационный процесс, представляющий последовательность действий с информацией для получения заранее определенного результата»².

¹ Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ // Собрание законодательства РФ, 31.07.2006, N 31 (1 ч.), ст. 3448

² Коротенков, Ю.Г. Информационные процессы и технологии как объекты информатики и обучения информатике / Ю.Г. Коротенков // Вестн. Моск. городского пед. ун-та. Сер.: Информатика и информатизация образования. - 2004. - №3. - С. 98-106.

Процессуалист Ю.Н. Соколов, справедливо отмечая необходимость регламентации в ст. 5 УПК РФ понятия «информационных технологий» в уголовном судопроизводстве, под таковыми понимает: «совокупность процессов сбора, фиксации, обработки, накопления, хранения, поиска и представления процессуальной и не процессуальной информации, а также способов и методов их существования, протекающих в соответствии с назначением уголовного судопроизводства»¹.

Необходимо процессуальное закрепление в Уголовно - процессуальный кодекс определение «информационные технологии».

Под информационными технологиями в уголовном процессе следует понимать совокупность приемов, средств, методов обнаружения, фиксации, собирания, обработки, передачи сотрудниками правоохранительных органов оперативно значимой информации о событиях или действиях, которые впоследствии помогут установить наличие или отсутствие обстоятельств, подлежащих доказыванию, а также иных обстоятельств, имеющих значение для расследования конкретного уголовного дела.

Основными направлениями использования информационных технологий в ходе расследования уголовных дел, являются:

1. Структурирование информации, касающейся хода расследования уголовного дела, а именно, распределение по времени, месту, объекту преступного посягательства, а также подозреваемых лиц. Это поможет сохранить логическую цепочку расследования серийных и многоэпизодных преступлений;

2. Объективная оценка полученной информации и последующий ее анализ в целях выбора наиболее эффективной тактики расследования конкретного уголовного дела.

Внедрение информационных технологий, обусловленное не только фактическим использованием технических средств, но и соответствием

¹ Соколов, Ю.Н. Информационные технологии в уголовном судопроизводстве (Монография) / Ю.Н. Соколов. – Екатеринбург: Изд-во «Телекоммуникационное право, 2010. – С. 40.

нормативно-правового регулирования уже существующему положению, в отечественное государственное управление, в частности в уголовно-процессуальную деятельность, началось в начале XXI века. Использование информационных технологий в судебной деятельности было обусловлено принятием Федеральной целевой программы «Развитие судебной системы России» на 2002-2006 гг.,¹ главной целью которой являлось обеспечение судебной системы информационными технологиями и которая послужила впоследствии основой для утверждения Концепции Федеральной целевой программы «Развитие судебной системы России» на 2007-2011 гг.,² в свою очередь, в продолжение последней Распоряжением Правительства РФ от 20.09.2012 №1735-р была утверждена Концепция федеральной целевой программы «Развитие судебной системы России на 2013 - 2020 годы»³.

Пожалуй, одной из самых востребованных информационных технологий является видеоконференц-связь. Но при повсеместном внедрении обозначенной технологии и в отечественном уголовно-процессуальном законодательстве, и в международных договорах, ратифицированных Российской Федерацией, отсутствует конкретное определение термина «видеоконференц-связь».

На наш взгляд, необходимо проанализировать понятие, данное профессором А.Г. Волеводзом: «под видеоконференц-связью понимается всякая передача или прием изображений, звуков, обмен информацией между ЭВМ с использованием технологии видеоконференции, представляющей собой

¹ О федеральной целевой программе «Развитие судебной системы России» на 2002-2006 годы: Постановление Правительства РФ от 21.09.2006 № 583 // Собр. законодательства Рос. Федерации. - 2001. - № 49, ст. 4623.

² О Концепции Федеральной целевой программы «Развитие судебной системы» на 2007 - 2011 гг.: Распоряжение Правительства Российской Федерации от 04.08.2006 г. № 1082-р // Собр. законодательства Рос. Федерации. - 2006. - № 33, ст. 3652.

³ О федеральной целевой программе «Развитие судебной системы России на 2013 - 2020 годы»: Постановление Правительства РФ от 27.12.2012 № 1406 (ред. от 14.12.2017) // Собр. законодательства Рос. Федерации. - 2013. - № 1, ст. 13; 2017. - № 52 (Часть I), ст. 8135.

компьютерную технологию, позволяющую осуществление взаимодействия двух и более пользователей в режиме реального времени».¹

В судебной практике уже введена система видеоконференц-связи в ходе проведения судебного заседания. Необходимо отметить, что и в уголовном судопроизводстве целесообразно использовать данную технологию, что позволило бы сократить сроки производства по уголовному делу, а также обеспечить безопасности всех участников уголовного судопроизводства.

В системе МВД России также было создано специализированное подразделение – Департамент информационных технологий, связи и защиты информации МВД России, основной задачей которого является разработка и реализация государственной политики в области внедрения и совершенствования использования информационных технологий в уголовном процессе, информационно-телекоммуникационного обеспечения уголовного процесса.

В связи с постоянно меняющимся характером преступности законодателю необходимо быстро реагировать и подстраиваться под современное изменение информационного общества. Так, например, в последнее время УК РФ наряду с имеющимися «техническими» составами (ст. 146, 183, 187, 242, 242.1, 272 - 274 УК РФ) был дополнен ст. 159.6, 185.3, 228.1, в которых указывается использование для совершения преступления электронных, информационно-телекоммуникационных сетей, включая сеть-Интернет.

В свою очередь, УПК РФ как нормативный акт, нацеленный на реализацию уголовно-правовых норм, вводит новые нормы, направленные на борьбу с преступностью, опосредуемой информационно телекоммуникационными средствами. Так, ст. 186, 186.1 УПК РФ, предусмотренные для собирания информационных доказательств, были дополнены нормами об обыске и изъятии электронных доказательств (п. 9.1 ст.

¹ Волеводз, А.Г. Правовое регулирование новых направлений международного сотрудничества в сфере уголовного процесса. / А.Г. Волеводз. - М.: Юрлитинформ, 2002. - С. 390.

182, п. 3.1 ст. 183 УПК). Также необходимо отметить, что в декабре 2018 года была введена «Статья 164.1. Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий».

В ч. 2 ст. 259 УПК РФ содержится указание на возможность применения технических средств с целью обеспечения полноты протокола судебного заседания, а согласно ч. 5 ст. 241 УПК РФ все лица, присутствующие на открытом судебном заседании, с разрешения председательствующего судьи вправе осуществлять фото-, киносъемку и видеозапись. Использование аудиозаписи лицами, присутствующими на открытом судебном заседании, возможно и без разрешения председательствующего судьи, однако необходимо отметить, что реализация обозначенного права часто сталкивается с трудностями в условиях реального правоприменения. Безусловно, прогрессивной нормой является положение ч. 5 ст. 259 УПК РФ, регламентирующее обязательную отметку в протоколе судебного заседания о проведении фотографирования, аудио - и (или) видеозаписи, киносъемки допросов с приложением результатов применения технических средств к материалам уголовного дела.¹

В этой связи не вполне понятно, почему, во-первых, сказанное касается только допросов, а во-вторых, имеет ли данное положение отношение к аудиозаписям и другим материалам, полученным лицами, присутствующими в судебном заседании в соответствии с положениями ч. 5 ст. 241 УПК РФ². В связи с этим целесообразно внедрить обязательную фиксацию всего процесса судебного заседания, что позволит открыть широкие возможности для ускорения судопроизводства.

¹ Рыжаков, А.П. Разъяснение обязательных требований к оформлению любого и каждого протокола следственного действия / А.П. Рыжаков // СПС «Консультант Плюс» (дата обращения: 13.04.2020).- С. 56-67.

² Баев, О.Я. Криминалистический комментарий к процессуальному порядку производства следственных действий по УПК России / О.Я. Баев // СПС «КонсультантПлюс» (Дата обращения: 13.04.2020).- С.87 -90.

В соответствии с ч. 1 ст. 259 Уголовно-процессуального кодекса РФ каждое судебное заседание протоколируется с использованием средств аудиозаписи (аудиопротоколирование).

Федеральный закон от 22.12.2008 № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» закрепляет основополагающие начала, способы обеспечения доступа к информации о деятельности судов, правовом положении участников процесса, организации доступа к информации о деятельности судов, порядка предоставления такой информации, регламентирующий порядок взаимодействия судебных органов с редакциями средств массовой информации, а также определяет права на доступ к информации о деятельности судов и контроль за обеспечением доступа к информации об их деятельности.

Таким образом, правовое регулирование электронной информации, а также электронных доказательств вызывает необходимость их правового закрепления в уголовно-процессуальном законодательстве. В связи, с чем вызвало необходимость определения места и роли электронных носителей информации в уголовно процессуальном законодательстве.

На сегодняшний день вопрос о понятии электронных носителей информации является дискуссионным. Законодательное формулирование электронной информации и электронных носителей информации в системе доказательств с формальной точки зрения отсутствует. Среди научных обсуждений нет единого мнения касательно сути информационного доказательства. Что является информационным доказательством – сам факт электронного носителя информации или сведения о них? Каким требованиям они должны соответствовать, чтобы считаться доказательством в уголовном судопроизводстве? На какой стадии уголовного процесса собранная информация может считаться доказательством?¹

¹ Доля Е.А. Формирование доказательств на основании результатов оперативно-розыскной деятельности: монография. М., 2013. С. 64-65.

В теории уголовно-процессуального права научные деятели выработали единое понятие доказательства, которое признается большинством юристов. Под доказательствами понимаются сведения об обстоятельствах реальной действительности, полученные в предусмотренном законом порядке¹. Однако законодательно закрепленного понятия «электронные носители информации» не закреплено в Российском законодательстве.

Большинство научных публикаций, касающихся использования электронных носителей информации в качестве доказательств по уголовному делу, носят в большей степени описательный характер. Значительную часть составляют комментарии к Российскому законодательству, которые не затрагивают вопросы о правовой природе «электронных доказательств».

Исходя из этого, представляется целесообразным выделить несколько существующих точек зрения по вопросам правовой природы «электронных доказательств».

Первая позиция состоит в том, что доказательства, выраженные в электронном виде, вводятся в процесс посредством их отнесения к традиционным видам доказательств (средствам доказывания). Так, С.П. Ворожбит, применительно к гражданско-процессуальному праву указывает, что «в зависимости от того, какие из данных, сохраненных в электронной форме, имеют доказательственное значение, т.е. содержат сведения, необходимые для установления обстоятельств дела, будет зависеть отнесение их к письменным, вещественным доказательствам, аудио- или видеозаписи».²

В уголовно-процессуальном праве «электронные доказательства» чаще всего относят либо к вещественным доказательствам, либо к иным документам. Некоторые исследователи указывают, что разграничение электронных носителей информации на вещественные доказательства и иные документы должно происходить по классическому для доказательственного права критерию – если значимая для дела информация определяется исходя из

¹ Уголовно-процессуальное право РФ: учебник / Под ред. П.А. Лупинской. М., 2009. С. 296.

² Ворожбит С.П. Электронные средства доказывания в уголовном и гражданском процессе: автореф. дисс. ... канд. юрид. наук. СПб., 2011. С. 8.

физических свойств и качеств объекта материального мира, то соответствующий предмет или документ необходимо приобщить к делу в качестве вещественного доказательства; если же правовое значение имеет смысловое содержание объекта, то его необходимо рассматривать в качестве иного документа.¹

Согласно второй точке зрения, «электронные доказательства» представляют собой особые группы в рамках уже существующих видов доказательств, а потому должны наделяться специальным правовым статусом, учитывающим их особенности. К примеру, Ю.Н. Соколов пишет: «Информация в электронной форме, выраженная в виде вещественного доказательства, обладает определенной спецификой – доказательственное значение здесь имеет не сам материальный носитель, но та информация, которая на нем содержится».²

Третья точка зрения предполагает, что электронные данные – это совершенно новый вид доказательств наряду с другими, обозначенными в ч. 4 ст. 74 УПК РФ. В частности Н.А. Зигура и А.В. Кудрявцева отмечают: «Компьютерная информация должна пониматься как отдельный вид доказательств исходя из того, что она обладает особыми специфическими свойствами, отличающими ее, с одной стороны, от вещественного доказательства, а с другой, – от иного документа».³

На наш взгляд, электронные доказательства обладают высокой ценностью и в свою очередь являются предметом преступного посягательства.

Под «электронным доказательством» понимается электронный носитель информации, содержащий сведения о значимых обстоятельствах по конкретному уголовному делу и обладающий следующими юридически значимыми признаками:

¹ Тушев А.А., Назаров Н.А. Информация как основа всех видов доказательств в уголовном процессе // Общество и право. 2012. № 3. С. 196-197.

² Соколов Ю.Н. Информационные технологии в уголовном судопроизводстве: монография. Екатеринбург, 2010. С. 116.

³ Зигура Н.А., Кудрявцева А.В. Компьютерная информация как вид доказательства в уголовном процессе России: монография. М., 2011. С. 30.

- а) значительным объемом памяти;
- б) простотой передачи и копирования сведений с одного электронного носителя информации на другой;
- в) возможностью удаленного доступа к содержанию электронного носителя и информационно-телекоммуникационным системам (в частности к сети Интернет);
- г) относительностью и неочевидностью содержания.

Исходя из этого, предлагаем законодательно закрепить понятие «электронное доказательство». Под указанным термином следует понимать сведения, содержащиеся на электронных носителях информации или в телекоммуникационной сети «Интернет», имеющие значение для уголовного дела и собранные в порядке предусмотренным настоящим Кодексом».

В связи с этим, считаем целесообразным дополнить статью 74 Уголовно-процессуального кодекса новым видом доказательств – «электронное доказательство».

Кроме этого, законодательство должно содержать указание на равную юридическую силу доказательств, включая электронные документы, составляемые сторонами в ходе досудебного производства в связи с фиксацией хода и результатов совершаемых ими действий, направленных на получение доказательственной информации. При этом необходимо отметить, что любой способ документирования допустим, если он обеспечивает надежность сохранения и передачи доказательственной информации, представленной в электронном виде, и возможность исследовать и оценить аутентичность этой информации и верифицировать ее.¹

Электронные носители информации, в свою очередь, это материальные объекты, обладающие определенной ценностью, которые могут выступать в качестве предмета преступного посягательства против собственности. Это в первую очередь относится к различным телекоммуникационным устройствам

¹ Кувычков, С. И. Использование в доказывании по уголовным делам информации, представленной в электронном виде: автореф. дис. ... канд. юр. наук./ Кувычков Сергей Иванович. - Нижний Новгород, 2016. – С.12-14

(сотовые телефоны) и малогабаритным переносным компьютерным устройствам (ноутбуки, планшеты, электронные книги и т. п.), а также фото видеоаппаратуре (цифровые фотоаппараты и видеокамеры). Но и в данном случае потерпевшему причиняется вред, связанный с утратой информации, ценность которой зачастую значительно превышает стоимость самого предмета.

Понятие «электронный носитель информации» возможно рассматривать с различных точек зрения, многие авторы трактуют этот термин по-разному, но суть остается одна. Однако существует ГОСТ 2.051-2013 в котором дается более четкое объяснение данному термину. Электронный носитель - материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемых с помощью средств вычислительной техники¹.

Появление термина «электронный носитель информации» в УПК РФ следует рассматривать как некий промежуточный шаг на пути к возможному появлению в российском процессуальном праве термина «электронные доказательства».

В настоящее же время отечественный законодатель занимает двойственную позицию – в силу бурного развития средств вычислительной техники, их огромного влияния на общественную и личную жизнь граждан эти средства не могут вовсе игнорироваться правом, однако низкая степень осмысления данного влияния в науке и правоприменительной деятельности не позволяет выработать последовательное и системное регулирование в указанной области, включить в законодательство фундаментально новые понятия и принципы².

¹ ГОСТ 2.051-2013 Единая система конструкторской документации. Электронные документы. Общие положения. URL: <http://www.gostbaza.ru/?gost=4288> (дата обращения: 12.10.2019). С.35

² Оконенко Р.И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации // Современная российская наука глазами молодых исследователей: Сборник статей, 2016. С. 108-113

Также представляется целесообразным дополнить УПК РФ определением ЭНИ следующего содержания: «Электронный носитель информации – это устройство, конструктивно предназначенное для постоянного или временного хранения информации в виде, пригодном для использования в электронных вычислительных машинах, а также для ее передачи по информационно-телекоммуникационным сетям или обработки в информационных системах».

Под материальными носителями информации чаще всего мы подразумеваем сим-карты, флэш накопители, жесткие диски, дискеты, CD, DVD, BLU-Ray диски, магнитные ленты и другие информативные электронные устройства. Однако с каждым днем появляются все более усовершенствованные модели и правильным будет отнести так же и мобильные устройства: смартфоны, планшеты, умные часы, электронные книги. С их помощью можно получить самую разную информацию. Например, текстовые сообщения, файлы Word документов, чеки о выполнении операции, связанной с переводом денежных средств, переписки между людьми в различных социальных сетях. Также на мобильном устройстве могут храниться голосовые сообщения, фотографии, видеоролики.

Большую роль в нашей жизни играют компьютеры, ноутбуки, нэтбуки. При производстве следственных действий именно в них мы можем получить интересующую правоохранительные органы информацию. В ходе расследования уголовного дела необходимо вести учет электронных носителей информации. В таком случае должен заводиться журнал, в котором прописываются все устройства.

Однако определенного перечня устройств, относящихся к электронным носителям информации, нигде юридически не закреплено. В связи с этим, мы предлагаем внести перечень устройств, которые могут быть использованы в рамках уголовного дела, в Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации» статьей 2.1. следующего содержания: «К электронным носителям информации могут быть отнесены:

1. Компьютерные системы – компьютер, ноутбук, нэтбук, айпад, планшет, жесткий диск;
2. Оптические устройства - лазерный диск, компакт-диск, мини-диски, Blu-ray, HD-DVD;
3. Флеш-накопители и SSD-диски;
4. SMART устройства – смартфон, смарт-телевизор, умные часы, фитнес-трекер, смарт-брелки;
5. Иные устройства, содержащие электронную информацию».

Таким образом, можно сформулировать следующие выводы:

1. Необходимо процессуальное закрепление в Уголовно-процессуальный кодекс определение понятия «информационные технологии». Предлагаем дополнить пунктом 63 статью 5 Уголовно-процессуального кодекса РФ «Основные понятия, используемые в настоящем Кодексе» следующего содержания: «Информационные технологии в уголовном процессе - совокупность приемов, средств, методов обнаружения, фиксации, собирания, обработки, передачи сотрудниками правоохранительных органов оперативно значимой информации о событиях или действиях, которые впоследствии помогут установить наличие или отсутствие обстоятельств, подлежащих доказыванию, а также иных обстоятельств, имеющих значение для расследования конкретного уголовного дела».

2. Основными направлениями использования информационных технологий в ходе расследования уголовных дел, являются:

- структурирование информации, касающейся хода расследования уголовного дела, а именно, распределение по времени, месту, объекту преступного посягательства, а также подозреваемых лиц. Это поможет сохранить логическую цепочку расследования серийных и многоэпизодных преступлений;
- объективная оценка полученной информации и последующий ее анализ в целях выбора наиболее эффективной тактики расследования конкретного уголовного дела.

Появление термина «электронный носитель информации» в УПК РФ следует рассматривать как некий промежуточный шаг на пути к возможному появлению в российском процессуальном праве термина «электронные доказательства».

3. Предлагаем дополнить пунктом 64 статью 5 Уголовно-процессуального кодекса РФ «Основные понятия, используемые в настоящем Кодексе» следующего содержания: «электронное доказательство – это сведения, содержащиеся на электронных носителях информации или в телекоммуникационной сети «Интернет», имеющие значение для уголовного дела и собранные в порядке предусмотренным настоящим Кодексом».

Исходя из этого, считаем целесообразным добавить в статью 74 часть 2 пунктом 4.1 Уголовно-процессуального кодекса РФ «Доказательства» новым видом доказательств – «электронное доказательство» и изложить ее в следующей редакции:

«1. Доказательствами по уголовному делу являются любые сведения, на основе которых суд, прокурор, следователь, дознаватель в порядке, определенном настоящим Кодексом, устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела.

2. В качестве доказательств допускаются:

- 1) показания подозреваемого, обвиняемого;
- 2) показания потерпевшего, свидетеля;
- 3) заключение и показания эксперта;
- 3.1) заключение и показания специалиста;
- 4) вещественные доказательства;
- 4.1) электронные доказательства».

4. Также предлагаем дополнить пунктом 65 статью 5 Уголовно-процессуального кодекса РФ «Основные понятия, используемые в настоящем Кодексе» следующего содержания:

«Электронный носитель информации – это устройство, конструктивно предназначенное для постоянного или временного хранения информации в виде, пригодном для использования в электронных вычислительных машинах, а также для ее передачи по информационно-телекоммуникационным сетям или обработки в информационных системах».

5. В связи с тем, что нормативное определение электронных носителей не содержит конкретного перечня устройств, которые следует относить к данному понятию, предлагаем внести перечень устройств, которые могут быть использованы в рамках уголовного дела, в Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации» статьей 2.1. следующего содержания: «К электронным носителям информации могут быть отнесены:

- Компьютерные системы – компьютер, ноутбук, нэтбук, айпад, планшет, жесткий диск;
- Оптические устройства - лазерный диск, компакт-диск, мини-диски, Blu-ray, HD-DVD;
- Флеш-накопители и SSD-диски;
- SMART устройства – смартфон, смарт-телевизор, умные часы, фитнес-трекер, смарт-брелки;
- Иные устройства, содержащие электронную информацию».

§2. Зарубежный опыт использования электронной информации в уголовном судопроизводстве в качестве доказательства

Электронная информация - это нематериальный носитель, который представляет собой не что иное, как последовательность нулей и единиц. В отличие от физических вещей, владелец электронной информации сохраняет исходный набор данных и передает его копию либо в электронном виде на устройстве хранения данных, либо в виде распечатки на бумаге. С технической

точки зрения, доступ к электронным носителям информации можно получить доступ из любой точки мира, если они доступны через Интернет. ЭНИ могут передаваться по сети Интернет со скоростью света независимо от каких-либо национальных границ, и в таком случае решающим фактором остается время. Не менее важным остается тот факт, что по сравнению с физическими вещами, электронную информацию можно создавать, обрабатывать и передавать анонимно, в таком случае следы от киберпреступности можно скрыть гораздо лучше. После того, как правоохранительные органы получили электронные данные, которые являются потенциальными доказательствами, их, как правило, необходимо преобразовать в совместимый читаемый формат для дальнейшей обработки. Это подразумевает риск преднамеренного, непреднамеренного и даже незамеченного манипулирования исходной информацией.

На сегодняшний день электронная информация становится все более актуальной в расследовании уголовных дел. В странах Европейского Союза существуют лишь некоторые аспекты, нацеленные на конкретные проблемы связанные с электронным документооборотом в уголовном расследовании. В таких странах, как Германия и США достаточно развиты правовые положения уголовного процесса, касающиеся изъятия электронных носителей информации.

Изучение зарубежного опыта нормативного регулирования информационных технологий в уголовном процессе на сегодняшний день значимо не только с точки зрения оценки возможной рецепции каких-либо институтов и совершенствования действующих институтов, но и с точки зрения актуализации нормативного регулирования существующим реалиям научно-технического прогресса. Например, обсуждение возможностей нормативно-правового регулирования в законодательстве Российской Федерации появляющихся научно-технических разработок. Одними из самых дискуссионных на сегодняшний день вопросов являются - «электронный судья», видео-протокол судебного заседания, тензометрическая платформа для оценки стрессового психофизического состояния человека. Отмеченные

достижения научно-технического прогресса являются предметом обсуждения в теоретическом и практическом аспектах, а нормативно-правовое регулирование указанных вопросов в законодательстве РФ на сегодняшний день отсутствует.

Видеоконференц-связь является распространённым в мировой практике техническим средством, используемым в уголовном процессе. Самое широкое распространение использование видеоконференц-связи получило в США, Великобритании, Германии, Швеции, Франции, что, в свою очередь, с одной стороны, обусловлено, а с другой стороны, вызывает необходимость детальной нормативно-правовой регламентации применения обсуждаемой технологии и критериев допустимости доказательств, полученных посредством ее применения. Кроме того, немаловажное значение использования видеоконференц-связи с целью обеспечения безопасности свидетелей, потерпевших и обвиняемых прямо указано в уголовно-процессуальном законодательстве Италии, Бельгии, Латвии, Франции и Украины¹.

В настоящее время научными и практическими работниками достаточно активно обсуждается вопрос о возможности внедрения в практику видео-протоколов и ведения аудиозаписи судебного заседания.² С октября прошлого года в России уже производится аудиопротоколирование судебных заседаний по уголовным делам. На наш взгляд, к достоинствам аудиофиксации следует отнести то, что его невозможно сфальсифицировать и переписать под приговор.

Конвенция о киберпреступности, подписанная 23 ноября 2001 года в г. Будапешт, является первым международным договором, который направлен на борьбу с компьютерной преступностью, а также на борьбу с совершением преступных действий в информационно-телекоммуникационной сети «Интернет». Конвенция была разработана Советом Европы в Страсбурге при активном участии таких стран, как Канада, Япония, Филиппины, Южная Африка и Соединенные Штаты. Данный международный договор в первую очередь направлен на предоставление полномочий правоохранительным

¹ Дудин Н. Инновационный проект // Законность. - 2010. - № 1. - С. 58.

² Ландау, И.Л. Некоторые аспекты использования научно-технических средств в уголовном процессе / И.Л. Ландау // Судебная власть и уголовный процесс. - 2016. - № 1. - С. 79.

органам для расследования преступлений, связанных с компьютерной информацией, которая впоследствии может стать доказательством по расследуемому уголовному делу, а также быстрого и эффективного сотрудничества между государствами.

Конвенция требует от стран, ее подписавших, применять определенные механизмы в рамках своих законодательных документов. Например, правоохранительным органам должно быть предоставлено право заставлять Интернет-провайдера отслеживать действия человека в режиме онлайн в реальном времени. Наконец, Конвенция требует, чтобы подписавшие государства обеспечивали международное сотрудничество в максимально возможной степени для расследования уголовных дел, связанных с использованием компьютерной информации в целях совершения преступления¹.

На национальном уровне были приняты положения, касающиеся удаленного сбора информации через сеть Интернет в таких странах, как Бельгия, Германия и Австрия. Также в марте 2018 года в США был разработан Закон «Об облачности», который специально направлен на получение электронной информации, хранящейся «в облаке», тем не менее, указанный закон охватывает лишь некоторые проблемы, касающиеся изъятие электронной информации².

Особый интерес вызывает правоприменительный опыт Соединенных Штатов Америки, где данное юридическое явление возникло раньше и к настоящему времени представляет целую систему электронного доказательственного права.

В большинстве случаев электронные устройства, содержащие в себе сведения, имеющие значение для расследования уголовного дела могут быть

¹ Electronic Privacy Information Center The Council of Europe's Convention on Cybercrime. URL: <http://epic.org/privacy/intl/senateletter-072605.pdf> (дата обращения 20.03.2020)

² Директива 2013/40 / EU о нападениях на информационные системы (OJ L 218, 14.8.2013, 8) и ст. 1 (b) Конвенции Совета Европы о киберпреступности (ETS 185). Ст.2 URL: <http://internetinside.ru/soglasovannaya-direktivaes-po-kiberb/>. (дата обращения 14.05.2020)

изъяты с помощью специальных инструментов и материалов для изъятия. Сотрудники правоохранительных органов при первичном изъятии электронных носителей информации должны соблюдать осторожность при сборе, обработке и хранении цифровых устройств во избежание их повреждения либо уничтожения.¹ Также необходимо отметить, что сотрудники правоохранительных органов США проходят специальное обучение по сбору цифровых доказательств. В целом, для изъятия электронных носителей информации, у офицера должны быть при себе следующие инструменты и материалы для сбора:

- фото и видеокамеры, картонные коробки; блокноты; перчатки, журналы инвентаризации доказательств, специальная лента, бумажные пакеты, наклейки, этикетки, бирки с указанием даты и времени изъятия цифровых устройств; маркеры. Также у лиц, занимающихся изъятием цифровых устройств, при себе должна быть и радиочастотная защита. К ней можно отнести «щит Фарадея» либо алюминиевая фольга для обертки сотовых телефонов, смартфонов и других мобильных устройств.

Федеральное законодательство США не содержит исчерпывающий перечень видов доказательств, каждое доказательство подлежит оценке его относимости, допустимости, достоверности, достаточности и веса. В соответствии с установленными Федеральным законом правилами о доказательствах² можно условно выделить следующие электронные доказательства в системе доказательств США, основанной на прецедентной судебной практике:

1. аудиозапись;
2. фотография;
3. видеозапись;
4. электронный документ;

¹В.Купс и М. Гудвин, Киберпространство, Облако и трансграничное уголовное расследование. Пределы и возможности международного права, 2014. С. 23-48

² Federal Rules of Evidence, 1975 // Federal Evidence Review. – URL: <http://federalevidence.com/downloads/rules.of.evidence.pdf> (дата обращения: 09.03.2020).

5. мобильное устройство связи;
6. текстовые сообщения;
7. электронный носитель информации;
8. электронная корреспонденция;
9. данные Интернет-трафика.¹

При осмотре места происшествия, если есть необходимость изъятия электронных носителей информации, необходимо все тщательно задокументировать. Важно точно описать местоположение осмотра места происшествия, состояние компьютеров, электронных носителей, мобильных телефонов, смартфонов и других устройств хранения электронных данных.

Первоначальная документация осмотра места происшествия должна включать в себя записи с использованием фото- и видеосъемок. Все действия и процессы на экранах монитора компьютера или иного цифрового устройства должны быть полностью пошагово задокументированы.

Также необходимо внимательно осмотреть место происшествия, возможно рядом находятся листы бумаги с паролями, рукописными заметками, руководство по программному обеспечению, материалы, напечатанные с компьютера, которые могут помочь найти информации, являющуюся доказательством по уголовному делу. Эти формы доказательств также необходимо задокументировать и изъять.

Особое внимание необходимо уделить транспортировке и хранению электронных носителей информации. При упаковке цифровых доказательств для транспортировки необходимо придерживаться следующих правил: убедиться, что все цифровые доказательства правильно задокументированы, нанести все метки, опознающие знаки, сфотографировать. Также необходимо помнить, что цифровые доказательства могут иметь на себе следы преступления, либо иные биологические доказательства, поэтому работать следует в перчатках.

¹ United States v. MacEwan, 445 F.3d 237, 245 (3d Cir. 2006) // Justia. – URL: <http://law.justia.com/cases/federal/appellate-courts/F3/445/237/602722/> (дата обращения: 09.03.2020).

Изъятые с электронных носителей отпечатки пальцев, микроследы, микрочастицы, биологические следы и так далее должны быть направлены на экспертизу.

При назначении экспертизы сотрудник правоохранительных органов должен передать эксперту следующие материалы:

- фабулу уголовного дела;
- изъятые пароли к электронным носителям информации;
- предварительные отчеты и документы;
- списки ключевых слов.

Таким образом, анализируя опыт Соединенных Штатов Америки, мы приходим к выводу, что необходимо разработать инструкцию для сотрудников правоохранительных органов России по изъятию электронных носителей информации.

В начале 2019 года США и Великобритания подписали соглашение, которое позволяет сотрудникам правоохранительных органов обеих стран требовать от технологических компаний другой страны предоставления электронных файлов для использования их в качестве доказательства по уголовному делу.

Соглашение между двумя странами значительно ускоряет расследование, устраняя правовые барьеры, для своевременного и эффективного сбора электронных доказательств. Пакт позволяет следователям получать доступ к данным о серьезных преступлениях, таких как терроризм, сексуальное насилие над детьми и киберпреступность, не сталкиваясь с юридическими препятствиями.

Закон CLOUD, который означает «Закон о разъяснении законного использования данных за рубежом» обновил правила для следователей расследующих уголовные дела. Он позволяет США заключать соглашения об отправке информации с серверов США следователям по уголовным делам в другие страны с ограниченным рассмотрением запросов.

Пакт заменяет нынешний процесс обмена информацией о пользователях Интернета между странами, который называется MLAT или договором о взаимной правовой помощи, который требует от сотрудников правоохранительных органов получить разрешение суда перед тем, как обращаться в технологические компании.

Британская цифровая модель системы уголовной юстиции провозглашает ее поэтапное осуществление в виде цифровой сквозной системы с использованием так называемой Общей платформы (Common Platform)¹, в которой информация, полученная первоначально сотрудником полиции, отвечающим за расследование преступления, затем передается другим органам системы уголовной юстиции без дублирования или изменений. Эти этапы предполагают ввод информации о материалах дела и доказательствах, обмен файлами уголовных дел между соответствующими органами, защитой, подготовку дела для суда, представление дела в суде, а также итоговое решение по уголовному делу.

Например, сотрудники полиции должны быть оснащены инструментами, необходимыми им для того, чтобы иметь возможность набирать доказательства в цифровом виде на месте преступления, принимать заявления и загружать информацию о цифровых делах при помощи мобильных устройств без необходимости возвращаться в полицейский участок. Полиция фиксирует показания свидетелей и жертв преступлений в электронном виде на своем мобильном устройстве или путем видеофиксации места преступления (если есть такая возможность), пока события преступления еще свежи в памяти потерпевшего или свидетелей.

Использование цифровой модели означает, что полиция для принятия решения о предъявлении обвинения напрямую будет связываться с Королевской прокурорской службой, сотрудники которой получают доступ к информации и как можно быстрее примут такое решение. Информация о

¹ Early progress in transforming courts and tribunals. Report by the Comptroller and Auditor General. 9 may 2018. URL: <https://www.nao.org.uk/wp-content/uploads/2018/05/Early-progress-in-transforming-courts-and-tribunals.pdf>. (дата обращения: 12.12.19)

происшествия больше не будет дублироваться в бумажной форме. Кроме того, подозреваемые и обвиняемые, находящиеся под стражей, станут участвовать в досудебных слушаниях с помощью видеоконференц-связи, что позволит уменьшить транспортные расходы и ускорить процесс отправления правосудия.

К настоящему времени процесс формирования Общей платформы не завершен. В ноябре 2016 г. время выполнения программы реформ было продлено с четырех до шести лет без дополнительного финансирования. Создание Общей платформы изначально должно было завершиться в июле 2018 г., однако из-за проблем, связанных с координацией действий участвующих в ней трех организаций (полиции, Королевской прокурорской службы и Службы Ее Величества по вопросам судов и трибуналов), технологических сложностей и создания новой собственной команды для разработки программного обеспечения ее завершение отложено до июня 2020 г.¹

К компетенции Суда Короны отнесено рассмотрение наиболее сложных и серьезных дел о преступлениях, преследуемых по обвинительному акту, составляемому на основании документов, подготовленных в магистратских судах². С 2016 года в Суде Короны Англии и Уэльса после успешных испытаний повсеместно начала применяться онлайн-Система цифровых дел (The Crown Court Digital Case System - CCDCS, название которой обычно сокращается до DCS), позволяющая прокурорам, представителям защиты и судам осуществлять загрузку и доступ к информации, хранящейся на одном портале. В первую очередь ее создание диктовалось потребностью отказа от бумажных методов совместного использования и сопоставления документов, а также необходимостью экономии времени прохождения уголовного дела.

¹ Early progress in transforming courts and tribunals. Report by the Comptroller and Auditor General. 9 may 2018. URL: <https://www.nao.org.uk/wp-content/uploads/2018/05/Early-progress-in-transforming-courts-and-tribunals.pdf>. (дата обращения: 14.12.19).

² Власов, И.М. Системы уголовного правосудия зарубежных государств (суды первой и второй инстанции) / Отв. ред. И.С. Власов. М., 2008. С. 86 - 126

Цифровая система DCS представляет собой веб-платформу, которая позволяет пользователям просматривать и распечатывать документы, загруженные на нее ранее. Каждое уголовное дело в Суде Короны имеет собственный цифровой файл, доступ к которому разрешен только зарегистрированным пользователям. Для регистрации пользователя требуется безопасный адрес в системе электронной почты CJSM, который имеется у всех адвокатов по уголовным делам. Доступ к отдельному файлу уголовного дела возможен по приглашению любого человека с доступом. Служба CJSM специализируется на безопасной передаче электронной почты между связанными партнерами в системе правосудия, является важной частью процесса присоединения к системе правосудия в Англии и Уэльсе и за ее пределами, позволяет людям, работающим в системе правосудия, включая общественные, частные и добровольные организации, отправлять электронные письма с информацией безопасным способом.

В каждом файле уголовного дела DCS есть разделы для загрузки необходимых документов, включая обвинительные заключения, свидетельские показания, вещественные доказательства, приложения. Как только пользователи получают доступ к файлу, они могут загружать новые документы в соответствующие разделы. Каждый документ датируется системой, чтобы сразу можно было увидеть, когда он был загружен. В настоящее время в Суде Короны крайне мало уголовных дел, которые не размещались бы в системе DCS, и судьи обычно неохотно идут на это, поскольку отказ от регистрации может сказаться на эффективности рассмотрения дела.

Развитие электронного правосудия в Германии происходит под влиянием целого ряда особенностей национальной правовой системы, к числу которых относятся членство в Европейском союзе, федеративное государственное устройство, наличие судов шести видов юрисдикции. Само электронное правосудие понимается в немецкой доктрине широко и охватывает различное использование информационно-коммуникационных технологий в судебной деятельности. Среди его элементов выделяют, в частности, ведение судами

электронных реестров, использование видеоконференцсвязи, размещение в открытом доступе судебных решений и др. К числу главных элементов электронного правосудия, находящихся в центре внимания статьи, относятся электронный правовой оборот (*elektronischer Rechtsverkehr*) и электронные дела (*elektronische Akte*).

Начальной стадией законодательно закреплённого электронного уголовного судопроизводства в Германии принято считать 2001 год. В указанный год были приняты два законодательных акта, касающихся электронного взаимодействия между судьями и правоохранительными органами, а также введено в законодательство понятие электронного документа и определены условия, при которых он может использоваться в качестве доказательства по уголовному делу.

В Германии разработана система электронного уголовного судопроизводства. Принцип его работы достаточно прост, все документы, поступающие в правоохранительные органы, хранятся централизованно в электронном архиве. Электронные файлы подлежат ознакомлению любому сотруднику правоохранительных органов. Таким образом, в один клик полицейский может ознакомиться с уголовным делом и всеми сопутствующими документами.

Все документы созданные в информационном архиве автоматически сортируются по различным критериям в один соответствующий файл. Структура информационного архива состоит из файлов, содержащихся в правоохранительных органах, которая содержит всю информацию о правонарушениях и совершенных преступлениях. Это позволяет сотрудникам правоохранительных органов не заходить в архив картотек, а получить информацию по уголовным делам за считанные минуты в цифровом виде прямо на своем рабочем месте. Благодаря электронным уголовным делам работа сотрудников правоохранительных органов становится намного проще и быстрее.

Также в Германии широко развито взаимодействие между судами и правоохранительными органами. К такому взаимодействию могут относиться: электронные судебные дела, а равно размещение решений по уголовным делам в электронный банк данных судебных решений; размещение в сети Интернет информации о судах; использование видеоконференцсвязи во время проведения судебного заседания, а также ряд других элементов.¹ Электронная коммуникация между правоохранительными органами и судами способствует усовершенствованию правовой системы Германии. А именно к 1 января 2026 года коммуникация со всеми немецкими судами по электронным каналам связи даст возможность так же вести уголовные дела в электронном виде.²

В Японии создана отдельная отрасль права, как цифровая криминалистика. Как и в криминалистике существуют конкретные правила, принципы, процедуры, которые должны соблюдаться для достижения поставленной задачи. Исходя из этого, мы делаем вывод о том, что при изъятии электронных носителей информации необходимо придерживаться следующих правил: электронные данные не должны быть изменены; должны быть созданы криминалистически обоснованные дубликаты оригинала исходной информации; экспертиза электронных носителей информации должна проводиться компетентными лицами.

Конвенция о киберпреступности предполагает, что электронные носители информации могут быть изъяты следующим образом: информация, имеющая значение для уголовного дела, может быть напечатана с компьютера и приобщена к материалам уголовного дела; может быть изъят сам материальный носитель информации; или могут быть сделаны дубликаты с цифрового носителя, который подтверждается экспертом-криминалистом³.

¹ Mehrjähriger Aktionsplan für die europäische E-Justiz (2014–2018) v. 6.06.2014 2014/C 182/02 // Official Journal of the European Union. S. 182. (дата обращения 16.05.2020)

² Handelsgesetzbuch v. 10.05.1897 zul. geändert am 18.7.2017 // RGBI. I S. 219; BGBI. 2017. I. Nr. 52. S. 2745. (дата обращения 16.05.2020)

³ Council of Europe 2001. URL: http://www.oas.org/juridico/english/cyb_pry_coe.pdf 33 (дата обращения 16.05.2020)

Подводя итог рассмотрению зарубежного опыта нормативного регулирования информационных технологий в уголовном процессе, считаем необходимым проанализировать перспективы их применения в России.

1. В таких странах, как США, Великобритания, Германия, Швеция, Франция, широко распространено использование видеоконференц-связи в процессе расследования преступлений. Также в Италии, Бельгии, Латвии, Франции и Украине сотрудники правоохранительных органов в процессе своей служебной деятельности используют видеоконференц-связь с целью обеспечения безопасности свидетелей, потерпевших и обвиняемых. Несомненно, перенять Россией данный опыт у зарубежных стран было бы целесообразно, так как в настоящий момент цифровые технологии все больше поглощают современную жизнь общества. Использование видеоконференц-связи необходимо не только на стадии судебных заседаний, но и сотрудниками органов дознания, следствия, уголовного розыска на стадии предварительного расследования уголовных дел.

2. В США законодательно закреплён исчерпывающий перечень электронных доказательств, которые подлежат оценке их относимости, достоверности и достаточности. В связи с чем, считаем необходимым внести в перечень доказательств УПК и электронные доказательства.

3. Разработанный в США Закон «Об облачности», который направлен на получение электронной информации из «Облака», находящегося в единой информационной телекоммуникационной сети «Интернет» может оказать положительное влияние и на российское законодательство. Нельзя забывать о том, что информация содержится не только на электронных носителях информации, но также в сети «Интернет». Так же необходимо и российскому законодателю не упускать из вида тот момент, что в настоящее время большая доля преступлений совершается в информационно-телекоммуникационной сети Интернет.

4. Изучив опыт США, считаем необходимым предпринять попытки к созданию инструкции для правоохранительных органов России по правильному

изъятию электронных носителей информации, чтобы в дальнейшем использовать полученные сведения в качестве доказательств по расследуемым уголовным делам.

5. Достаточно интересной для России является Британская онлайн-Система цифровых дел. Указанная модель позволяет участникам уголовного судопроизводства осуществлять загрузку и доступ к оперативной информации, хранящейся на одном портале. Сотрудники полиции в Британии оснащены всеми необходимыми инструментами для изъятия электронных носителей информации на месте преступления, а также принимать заявления от граждан в электронном виде и загружать всю необходимую информацию, касающуюся расследования уголовных дел, при помощи мобильных устройств в единый электронный портал.

6. Положительной чертой Германии, которую может позаимствовать Российская Федерация, является система электронного судопроизводства, которая позволяет передавать данные в считанные секунды, а также осуществляется быстрое взаимодействие между следователями, судами и прокуратурой. Принцип работы электронного уголовного дела Германии заключается в том, что все поступающие в правоохранительные органы материалы и документы, касающиеся расследования уголовных дел, хранятся централизованно в едином электронном архиве.

7. В Японии создана отдельная отрасль права, как цифровая криминалистика. Сотрудники правоохранительных органов изучают ее положения и нормы с целью обучения правильному изъятию электронных носителей информации на месте совершения преступления. Исходя из этого, мы делаем вывод о том, что при изъятии электронных носителей информации необходимо придерживаться следующих правил: электронные данные не должны быть изменены; должны быть созданы криминалистически обоснованные дубликаты оригинала исходной информации; экспертиза электронных носителей информации должна проводиться компетентными лицами.

ГЛАВА 2. УГОЛОВНО-ПРОЦЕССУАЛЬНЫЕ И ОРГАНИЗАЦИОННЫЕ АСПЕКТЫ ОБНАРУЖЕНИЯ, ИЗЪЯТИЯ И ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ИНФОРМАЦИИ ПРИ ПРОИЗВОДСТВЕ ПО УГОЛОВНОМУ ДЕЛУ

§1. Уголовно-процессуальная форма и способы получения информации, содержащейся в электронных носителях и электронных сообщениях

Проводя анализ Уголовно-процессуального кодекса РФ, нормативно-правовых актов, комментарии к отдельным статьям Уголовно-процессуального кодекса Российской Федерации, можно сказать, что существует ряд проблем касательно изъятия электронных носителей информации. Следователи, дознаватели, а также сотрудники оперативных подразделений каждый день сталкиваются с необходимостью работы с информационными технологиями, а также изъятием информации с различных электронных носителей. Ежегодно следственные органы предоставляют отчетную документацию, однако в ней есть отрицательные моменты, касательно роста совершенных преступлений в сфере высоких технологий. Чем больше развиваются новейшие технологические разработки, тем более изощренные способы совершения преступлений придумывают преступники. Возможность работать удаленно, не выходя из дома, подталкивает людей совершать компьютерные преступления все больше и больше. Исходя из этого, законодательство Российской Федерации не успевает идти в ногу с развитием компьютерных технологий, и возникают пробелы в правоприменительной практике.

При производстве таких следственных действий, как обыск и выемка следователю, дознавателю необходимо учитывать тот факт, что различные манипуляции с электронными носителями информации могут непреднамеренно привести к повреждению или уничтожению электронного файла. Это грозит тем, что их будет невозможно использовать в дальнейшем в качестве доказательства по уголовному делу. Поэтому необходимо обеспечить

пристальный контроль над сохранностью электронных носителей информации до приезда специалиста.

Практика сотрудников правоохранительных органов показывает, что процедура изъятия электронных доказательств является наиболее распространённой и сложной. Производство изъятия электронных носителей информации возможно как в форме обыска, так и в форме выемки.

До 2019 года в нормах Уголовно-процессуального кодекса было закреплено, что производство изъятия ЭНИ осуществляется только с участием специалиста (ч. 9.1 ст. 182 и ч. 3.1 ст. 183). На практике положения данных статей исполнять не совсем удавалось, и они утратили свою силу, однако участие специалиста также остается обязательным в соответствии с нормами положений ст. 164.1 УПК РФ.

Кроме того, в ходе анкетирования сотрудников следственных органов и органов дознания, было выявлено, что 49% считают, что участие специалиста является необходимым и важным условием, и другие 49% считают, что привлечение специалиста необходимо, но по усмотрению следователя, дознавателя. (См. приложение 1,2)

На наш взгляд, считаем целесообразным дать право следователю, дознавателю самому принимать решение об участии специалиста в ходе обыска, выемки, если есть необходимость изымать электронные носители информации.

Особенно актуальным встает вопрос об изъятии электронной информации, передаваемой посредством электронной почты. В настоящее время такие мессенджеры, как Viber, WhatsApp, Telegram, WeChat все больше пользуются популярностью у людей. Также приложение Instagram дает возможность своим пользователям общаться в чате, отправлять голосовые сообщения, делиться публикациями, и передавать какую-либо медиа-информацию.

Представляется ситуация, когда сотрудники оперативных подразделений обнаружили переписку в телефоне подозреваемого, которая может служить

доказательством по уголовному делу. В таком случае как изымать данную информацию? Обязательно ли приглашать специалиста для изъятия? Возможно, в данном случае оперуполномоченный делает скриншоты экрана с перепиской и предоставляет результаты органу дознания либо следователю рапортом с приложением указанных скриншотов. Тогда в данном случае не обязательно приглашать специалиста.

Каждое положение, которое вносится законодательством в процессуальные документы, вызвано определенными предпосылками, которые требуют определенных уточнений и разъяснений в законе. Многие научные деятели, юристы приводят достаточно убедительные доводы касаясь определенных изменений в законодательство.

По мнению А.В. Победкина и Ю.В. Гаврилина существуют отдельные недостатки существующей уголовно-процессуальной регламентации порядка работы с электронными носителями информации в уголовном процессе. К ним они относят «неоправданность императивно установленного требования об участии специалиста во всех без исключения случаях изъятия электронных носителей информации в ходе обыска или выемки»¹.

Требование участия специалиста в ходе изъятия электронных носителей информации во время проведения следственных действий не совсем оправдано. Не было дано отдельных комментариев, которые бы разъяснили, какими познаниями должен обладать специалист.

Законодатель совершил некий прорыв в области изъятия электронных носителей информации, а именно была введена статья 164.1 УПК РФ Федеральным законом от 27.12.2018 года № 533-ФЗ. «Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий».

Данная статья гласит, что:

¹ Гаврилин Ю.В., Победкин А.В. Собираание доказательств в виде сведений на электронных носителях в уголовном судопроизводстве России: необходимо совершенствование процессуальной формы // Труды Академии управления МВД России. - 2018. - N 3 (47). - С. 109.

«1. При производстве по уголовным делам, указанным в ч. 4.1 ст. 164 настоящего Кодекса, изъятие электронных носителей информации не допускается, за исключением случаев, когда:

- 1) вынесено постановление о назначении судебной экспертизы в отношении электронных носителей информации;
- 2) изъятие электронных носителей информации производится на основании судебного решения;
- 3) на электронных носителях информации содержится информация, полномочиями на хранение и использование которой владелец электронного носителя информации не обладает, либо которая может быть использована для совершения новых преступлений, либо копирование которой, по заявлению специалиста, может повлечь за собой ее утрату или изменение.

2. Электронные носители информации изымаются в ходе производства следственных действий с участием специалиста. 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 п. 3 ч. 1 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.

3. Следователь в ходе производства следственного действия вправе осуществить копирование информации, содержащейся на электронном носителе информации. В протоколе следственного действия должны быть указаны технические средства, примененные при осуществлении копирования информации, порядок их применения, электронные носители информации, к которым эти средства были применены, и полученные результаты. К протоколу прилагаются электронные носители информации, содержащие информацию, скопированную с других электронных носителей информации в ходе производства следственного действия».¹

Нормы, закрепленные в статье ч.1 ст. 164.1 УПК РФ указывают, что при производстве следственных действий, когда существует необходимость изъятия электронных носителей информации, необходимо вынести постановление о назначении судебной экспертизы. Однако на практике это вызывает некоторые сложности, так как согласно ст. 195 УПК РФ «Порядок назначения судебной экспертизы» в п.4 ч.1 в распоряжение эксперта предоставляются все необходимые материалы, имеющиеся у следователя, а именно электронные носители информации. Именно в этот момент возникает проблема, как можно назначить судебную экспертизу, если ЭНИ не изъяты (документально не закреплены)? Исходя из этого, считаем, что указанную статью необходимо доработать. Следователь не сможет вынести постановление о назначении судебной экспертизы, если ему нечего будет передать эксперту, иначе данная ситуация может расцениваться, как фальсификация.

Изучая п.2 ч.1 ст. 164.1 УПК РФ можно сделать вывод, что изъятие электронных носителей информации производится только на основе судебного решения.

Однако в ч.2 ст.29 УПК РФ, определяющей полномочия суда, полномочия по принятию решения об изъятии электронных носителей информации в данном перечне не содержится. Из чего можно предположить,

¹ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 17.04.2017) // СЗ РФ. 2001. № 52 (ч. I). Ст. 4921.

что применительно к ч. 1 п. 2 ст. 164.1 УПК РФ имелись в виду общие решения суда, указанные в п. 5 ст. 29 УПК РФ - о производстве обыска и (или) выемки в жилище (в ходе которых необходимо изъять электронные носители информации) и п. 7 ст. 29 УПК РФ о производстве выемки предметов и документов, содержащих государственную или иную охраняемую федеральным законом тайну, а также предметов и документов, содержащих информацию о вкладах и счетах граждан в банках и иных кредитных организациях (которые могут содержаться на электронных носителях информации, в связи с чем подлежат изъятию).

Полагаем, что необходимо уточнение в ч. 1 п. 2 ст. 164.1 УПК РФ: на производство какого следственного действия получено судебное решение, либо на внесение дополнения в перечень полномочий суда, а именно - п. 14 ч. 2 ст. 29 УПК РФ - о производстве изъятия электронных носителей информации.

Следователям, дознавателям при производстве следственных действий, касающихся изъятия электронных носителей информации, необходимо руководствоваться статьями 182, 183 УПК РФ. Для того чтобы принять решение об изъятии ЭНИ необходимо присутствие специалиста, обладающего специальными познаниями в области информационных технологий. Также необходимо учитывать необходимость присутствия понятых, собственника носителя электронной информации – это общие правила закрепленные законодательно.

Лицо, которое осуществило изъятие ЭНИ, должно соблюдать все правила обращения с информацией, а именно не разглашать сведения, находящиеся на изъятом носителе. Только законный владелец, собственник съемного носителя, на котором находится интересующая правоохранительные органы информация, может дать разрешение на создание копий. Также необходимо учитывать тот факт, что информация во время копирования может повредиться, либо часть информации утеряться. Если была передана копия информации, находящейся на электронном носителе информации, собственник данного съемного носителя имеет право оригинал оставить себе.

Казалось бы, законодатель учел все правила, касающиеся изъятия электронных носителей информации, однако место и роль в доказательственной базе он не определил.

Сотрудники оперативных подразделений так же в своей профессиональной деятельности могут изымать электронные носители информации. Однако их полномочия расширены, так как изымать их они могут не только во время проведения обыска и выемки, но и в ходе осмотра места происшествия.

Электронными носителями, полученными в ходе оперативно-розыскной деятельности являются:

- результаты прослушивания телефонных переговоров,
- снятие информации с технических каналов связи,
- средства электронного наблюдения,
- аудио и видеозаписи различных ОРМ как опроса, проверочной закупки, оперативного эксперимента и т.д.¹

В работе оперативного сотрудника большую роль играет не выявление электронных носителей информации, а обеспечение возможности их использования в дальнейшем расследовании уголовного дела.

Согласно ст. 11 Федерального закона «Об оперативно-розыскной деятельности»², представление результатов оперативно-розыскной деятельности органу дознания, следователю или в суд осуществляется на основании постановления руководителя органа, осуществляющего оперативно - розыскную деятельность, в порядке, предусмотренном ведомственными нормативными актами. В свою очередь в п.п. 16 и 17 Инструкции о порядке представления результатов оперативно-розыскной деятельности органу

¹ Кучин О. С. Электронные носители информации в криминалистике: монография. М., 2017. С.98.

² Федеральный закон от 12.08.1995 N 144-ФЗ (ред. 02.08.2019) «Об оперативно-розыскной деятельности»// Собрание законодательства РФ. – 1995. - N 33. - Ст. 3349.

дознания, следователю или в суд от 27 сентября 2013 г.¹ указано, что к передаваемым документам, полученным в процессе оперативно-розыскной деятельности прилагаются (при наличии) полученные (выполненные) при проведении ОРМ материалы фото- и киносъемки, аудио- и видеозаписи и иные носители информации, а также материальные объекты, которые в соответствии с уголовно - процессуальным законодательством могут быть признаны вещественными доказательствами.

В иных случаях составляется приложение к рапорту, в котором может содержаться описание индивидуальных признаков материалов, документов, а также иных объектов.

На сотрудников оперативных подразделений так же возлагается большая ответственность по сохранности электронных носителей информации.

При осуществлении такого ОРМ, как прослушивание телефонных переговоров при передаче фонограммы к ней прилагается стенограмма на бумажном носителе.

Так же законом не ограничивается такое право, как создание копий с электронных носителей, в том числе с переносов наиболее важных разговоров, переписок на единый электронный носитель, что позволит сотрудникам правоохранительных органов обратить свое внимание на конкретный нужный момент. В этом случае оригиналы документов, материалов и так далее будут храниться в органе, осуществляющем оперативно-розыскную деятельность, если они не были истребованы в суде либо следователем, дознавателем.

Разъясняя указанные положения, Верховный суд РФ в своем Постановлении № 8 от 31 октября 1995 г. «О некоторых вопросах применения

¹ Приказ МВД России N 776, Минобороны России N 703, ФСБ России N 509, ФСО России N 507, ФТС России N 1820, СВР России N 42, ФСИН России N 535, ФСКН России N 398, СК России N 68 от 27.09.2013 «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд» (Зарегистрировано в Минюсте России 05.12.2013 N 30544)// Российская газета. - N 282. – 2013.

судами Конституции РФ при осуществлении правосудия»¹ указал, что только при получении разрешения суда на изъятие электронной информации результаты оперативно-розыскной деятельности могут быть использованы в качестве доказательств. Такими результатами являются информация, полученная в ходе прослушивания телефонных переговоров, изъятие почтовых, телеграфных и иных сообщений и отправлений (п. 14).²

Так, под результатами ОРД могут пониматься результаты одного или нескольких ОРМ, форма которых соответствует требованиям действующего законодательства (они должны быть оформлены на электронном, бумажном либо ином носителе), которые представляют собой достоверные данные, а также изъятые в ходе таких ОРМ документы, предметы или вещества. При этом результаты ОРД составляют основу содержания оперативно-служебных документов (под содержанием понимается информация, которая впоследствии будет иметь доказательственное значение). Таким образом, результаты ОРД – это не фактические данные (то есть по сути – доказательства), а только информация о фактах, то есть источниках сведений, которые впоследствии могут быть проверены процессуальным способом³.

В соответствии с вышеуказанными положениями УПК РФ, ФЗ «Об ОРД» и приведенным судебным комментарием результаты оперативно-розыскной деятельности представляются в уголовный процесс на основании ст. 11 ФЗ «Об ОРД» в соответствующем порядке. Впоследствии данные результаты принимаются следователем, дознавателем, органом дознания и не должны противоречить ст.86 УПК РФ. Данная статья регламентирует собирание доказательств в ходе уголовного судопроизводства посредством производства

¹ Постановление Пленума Верховного Суда РФ от 16.04.2013 N 9 "О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 31 октября 1995 года № 8 «О некоторых вопросах применения судами Конституции Российской Федерации при осуществлении правосудия»// Бюллетень Верховного Суда РФ. – № 6. – 2013.

² Кучин О. С. Электронные носители информации в криминалистике: монография. М., 2017. - С.99.

³ Нагиленко Б.Я. О понятии результата оперативно-розыскной деятельности // Оперативник (сыщик). – 2016. – № 4. – С. 21–26; Теория оперативно-розыскной деятельности: Учебник / Под ред. К.К.Горяинова, В.С.Овчинского, Г.К.Синилова. – С. 556–557.

следственных и иных процессуальных действий, т. е. приобщаются к материалам уголовного дела для дальнейшей проверки и оценки.

Таким образом, следователю на основании вышеуказанной инструкции дается право на возврат переданных ему результатов ОРД обратно сотрудникам оперативных подразделений, если они не отвечают соответствующим требованиям данной Инструкции (п.п.18-20). В дальнейшем руководствуясь общим порядком доказывания в уголовном судопроизводстве результаты оперативно-розыскной деятельности обследуются на основании ст. 87 УПК РФ путем сравнения их с другими доказательствами, имеющимися в уголовном деле, установления их источников, получения иных доказательств, которые подтверждают или опровергают результаты ОРД.

Подводя итог вышесказанному, сформулируем следующие выводы:

1. Необходимо уточнение в ч. 1 п. 2 ст. 164.1 УПК РФ: на производство, какого следственного действия получено судебное решение, а именно внесение дополнения в перечень полномочий суда и изложить указанную норму в следующей редакции:

«Статья 29. Полномочия суда

2. Только суд, в том числе в ходе досудебного производства, правомочен принимать решения:

14) о производстве изъятия электронных носителей информации».

2. В целях обеспечения непосредственного исследования следователем, дознавателем результатов оперативно-розыскной деятельности, представленной в виде электронных носителей информации предлагаем дополнить ст.89 УПК РФ частью второй и изложить ее в следующей редакции:

«Статья 89. Использование в доказывании результатов оперативно-розыскной деятельности

1. В процессе доказывания запрещается использование результатов оперативно-розыскной деятельности, если они не отвечают требованиям, предъявляемым к доказательствам настоящим Кодексом.

2. Результаты оперативно-розыскной деятельности, представленные в виде электронных носителей информации, осматриваются, признаются вещественными доказательствами, и приобщаются к уголовному делу в порядке, предусмотренном частью второй статьи 81 настоящего Кодекса».

§2. Процессуальные и организационные аспекты производства по уголовному делу в электронном виде

Важной мерой, связанной с внедрением информационных технологий в уголовный процесс, стало принятие Федерального закона от 23.06.2016 № 220-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части применения электронных документов в деятельности органов судебной власти», которым в УПК РФ введена ст. 474.1 «Порядок использования электронных документов в уголовном судопроизводстве». Положения указанного федерального закона прямо указывают на то, что гражданам предоставляется возможность подавать ходатайства, жалобы, представления в судебные органы Российской Федерации в электронном формате с заверенной цифровой подписью. Аналогично есть возможность направить судебные решения с их копиями участникам уголовного судопроизводства с использованием информационно-телекоммуникационной сети Интернет.

Исходя из этого, можно сказать, что законодателем уже делаются небольшие шаги к введению электронного документооборота во всей системе правоохранительных органов. Указанная технология поможет добиться перехода от бумажного судопроизводства в электронный формат, который в большей степени сократит сроки и упростит производство по уголовному делу.

Многие научные деятели, юристы, практические работники правоохранительных органов, следователи, дознаватели, сотрудники оперативных подразделений не раз высказывались о возможности ведения

уголовного дела в электронном формате, а также целесообразности фиксации результатов следственных, процессуальных, оперативно-розыскных мероприятий при помощи электронных средств.

Так, 2020 год для всего мира стал кризисным, и в первую очередь это связано с распространением болезни по всему миру Covid-19. Эти новости не покидают Интернет уже несколько месяцев, и сразу вспоминается 2002 год, когда была эпидемия атипичной пневмонии. В настоящее время люди вынуждены изолироваться дома. Большинство предприятий, организаций переходят на удаленную работу. Заседания советов Министров, обращения президента В.В.Путина, совещания в Министерстве внутренних дел России проходят в онлайн-режиме. Это еще больше подталкивает на мысль о том, что необходимо в структуре правоохранительных органов внедрить систему электронного документооборота, в том числе электронного уголовного дела.

В уголовно-процессуальном законодательстве нет четко указанных норм, касающихся возможности обращения граждан с заявлениями, обращениями жалобами, ходатайствами в электронной форме. На сегодня этот вопрос особенно актуален. Нормы УПК РФ дают четкое определение того, что заявление о преступлении может быть сделано в устном или письменном виде. В Приказе МВД России от 29.08.2014 г. № 736 «Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях»¹ говорится о том, что заявление о преступлении может быть направлено в правоохранительные органы в электронном виде. Однако впоследствии его необходимо распечатать на бумажный носитель и работать как с письменными заявлениями о

¹ Приказ МВД России «Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях» от 29.08.2014 г. № 736 // Справочно-правовая система «ГАРАНТ»

преступлении. Также недостаточно ясным остается вопрос о том, может ли быть подано заявление о преступлении частного обвинения в электронном формате. Прежде всего это связано с невозможностью пострадавших лиц воспользоваться таким средством подачи заявления, так как они не имеют электронной цифровой подписи. Часть 2 ст. 20 УПК РФ не позволяет реализовать право на подачу заявления в форме электронного документа и через представителя (адвоката) как, возможно, имеющего электронную подпись.

В связи с этим, необходимо дать гражданам возможность самим изъявлять желание, в какой форме они могут писать заявление о преступлении.

На основании вышеизложенного, считаем целесообразным дополнить ч.1 ст.141 Уголовно-процессуального кодекса положением о том, что заявление о преступлении может быть сделано в устном, письменном или электронном виде. Но так же необходимо не забывать о сроках и порядке рассмотрения заявления о преступлении в электронном виде.

Электронная система уголовного судопроизводства представляет собой преобразование информации из бумажного носителя в электронный формат. Файлы по уголовным делам могут передаваться между сотрудниками различных подразделений и служб в электронном виде, что значительно ускорит работу сотрудников органов внутренних дел.

На переход на электронный документооборот настаивает и А.Ф. Абдулвалиев, считающий, что модернизация уголовного судопроизводства должна заключаться в отказе от бумажных процессуальных документов и переходе на ведение уголовного дела в электронной форме. По мнению этого автора, переход на электронную форму производства по уголовному

делу должен, в первую очередь, упростить собирание доказательств и составление процессуальных документов¹.

Кроме того, в ходе анкетирования сотрудников следственных органов и органов дознания, было выявлено, что 62% считают перспективным производство предварительного расследования по уголовному делу в электронном виде. 24% опрошенных утверждают, что необходимо сохранить существующую «бумажную» модель уголовного судопроизводства. И лишь 14 % опрошенных видят возможность производства по уголовному делу, как в электронной форме, так и в «бумажной». Также было выявлено, что 86% опрошиваемых считают целесообразным внедрение в уголовно-процессуальную деятельность ОВД электронного документооборота в ходе взаимодействия с судом и иными контрольно-надзорными органами вне системы подразделений ОВД (См. Приложение 1,2).

В связи с этим считаем необходимым внести в Уголовно-процессуальный кодекс РФ новую норму, закрепляющую положения о производстве предварительного расследования в электронном виде.

Таким образом, это позволит обеспечить быстрый доступ к уголовным делам на стадии досудебного производства. В-первую очередь такое новшество улучшит работу таким подразделениям и службам, как уголовный розыск, прокуратура, судебные органы. Также указанным участникам уголовного судопроизводства будет дана возможность вносить различные изменения на каждом этапе расследования. Система управления уголовными делами в электронном виде улучшает координацию и контроль на стадии досудебного расследования. Такие документы, как доказательства, в том числе электронные (больше не будет необходимости записывать на CD-диски, что значительно улучшит работу оперативных подразделений), протоколы допросов, запросы в различные органы и другие документы

¹ Абдулвалиев А.Ф. Предпосылки и перспективы внедрения электронной формы уголовного дела в деятельность судебных органов – URL: http://e-notabene.ru/lr/article_345.html (дата обращения 12.04.2020). – С.58

станут доступными в сию минуту в онлайн режиме, что также сэкономит время и бюджетные деньги.

Отмечено, что цифровизация стадий уголовного и административного производства позволит исключить факты утери дел, фальсификации материалов, сократить бумажную волокиту, сроки расследования (рассмотрения), усилить аналитику и контроль за ходом расследования в онлайн - режиме.

Очевидно, что для успешного внедрения электронной формы уголовного дела в судебно-следственную деятельность потребуется ввести электронный документооборот на всех стадиях уголовного судопроизводства. Для этого понадобится детальная регламентация всех процессуальных действий (заявление о преступлении, производство следственных действий, проведение судебного заседания, составление приговора) при помощи электронных технических средств.

В идеале система, которая в большей степени будет представлять из себя уголовное дело, должна взаимодействовать и с другими базами данных и регистрами. Такие системы позволят реально анализировать работу сотрудников оперативных подразделений, а также органов дознания и следствия.

Вопрос об идентификации личности участника уголовного судопроизводства будет решаться посредством технологии использования электронной цифровой подписи и биометрической идентификации. Правовой основой для ее применения служит ст. 14.1 Федерального закона «Об информации, информационных технологиях и о защите информации», согласно которой государственные органы, банки и иные организации в случаях, определенных федеральными законами, после проведения идентификации при личном присутствии гражданина Российской Федерации, с его согласия, на безвозмездной основе размещают в электронной форме сведения, необходимые для регистрации гражданина в единой системе идентификации и аутентификации, и биометрические

персональные данные гражданина - в единой информационной системе персональных данных.

Исходя из этого, предлагаем ввести в уголовное судопроизводство внедрение системы заверения документов электронной цифровой подписью, а также использования идентификации, и аутентификации для установления личности участника уголовного судопроизводства.

Если в Российской Федерации из бюджета выделяют средства на создание указанного проекта, то это будет прорыв во всей системе уголовного судопроизводства. Большинство стран мира уже активно переходит на электронные уголовные дела, однако уровень развития у всех разный. Как было указано ранее, в указанном направлении двигаются такие страны, как США, Япония, Германия.

В 2005 году правительство Бельгии приняло решение о создании проекта электронного уголовного дела под рабочим названием «Phenix». Электронное уголовное дело не только ограничивается электронным документооборотом, но и взаимодействием с судами, прокуратурой, адвокатом, которые так же в свою очередь могут вносить дополнения либо изменения в электронное уголовное дело. Для того, чтобы данная система еще лучше функционировала у граждан вопрос с идентификацией и аутентификацией решается с помощью электронного паспорта. В Саудовской Аравии по большинству уголовных дел принимается решение в течение двух дней, а всего несколько лет назад бумажная система уголовного судопроизводства отнимала большое количество времени, и расследование уголовных дел затягивалось не только на несколько недель, но и месяцев. В 2011 году в Грузии властями было принято решение о переходе на электронный формат уголовного дела. Также такие страны, как Южная Корея, Сингапур, Эстония активно продвигаются в направлении цифровизации уголовных дел¹.

¹ Zuev S.V. Electronic criminal case: for and against - URL: <http://ec.europa.eu/idabc/servlets/Doc3443.pdf?id=32321> (дата обращения: 12.04.2020)

Но большой прорыв в указанном направлении сделала Республика Казахстан, в которой в 2011-2012 годах был запущен пилотный проект «Е-уголовное дело». Нельзя говорить о том, что Республика Казахстан отказалась от ведения уголовного дела в традиционной форме на бумажных носителях. Следователь либо дознаватель на свое усмотрение принимает решение о том, в какой форме вести расследование уголовных дел, о чем выносится соответствующее постановление «О ведении уголовного дела в электронной форме». Документы, которые ранее были созданы на бумажном носителе, сканируются в электронный формат в виде PDF документа. Все собранные материалы по уголовному делу передаются в орган прокуратуры либо в суд, заверенные электронной цифровой подписью, вместе с электронным уголовным делом.

С ноября 2016 г. в Азербайджанской Республике запущен модуль «Электронное уголовное дело». Применение автоматизированной информационной системы «Уголовное преследование: Е-дело» стало обязательным для сотрудников прокуратуры Республики Молдовы с 1 июля 2017 г. Следственным комитетом Республики Армения в практической деятельности используются системы «Электронное следствие» и «Оцифровка уголовных дел». В настоящее время Следственным комитетом Республики Беларусь изучаются зарубежный опыт ведения досудебного производства в электронном виде и возможность его применения в белорусском уголовном процессе¹.

Если говорить о Российской Федерации, то большое количество научных деятелей, юристов, академиков выступают за идею создания электронного уголовного дела, однако на законодательном уровне и в практике никаких продвижений на сегодняшний день нет.

Нельзя не согласиться с мнением Ю.Н. Соколова, он отмечает, что: «электронное уголовное дело должно представлять собой электронное

¹ О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года [Электронный ресурс]: указ Президента РФ от 7 мая 2018 г. № 204. Доступ из информационно-правового портала «Гарант».

устройство со сложным внутренним строением файлов, адаптированным к действующим информационным системам, содержащим персональные данные участников уголовного судопроизводства, оснащенное специальным программно-аппаратным обеспечением, которое должно быть сертифицировано в установленном законом порядке». Кроме того, Ю.Н. Соколов отмечает, что названное электронное устройство должно обладать определенной спецификой и удовлетворять всем требованиям относимости, допустимости, достоверности, а в совокупности и достаточности, предъявляемым уголовно-процессуальным законом к источникам содержащейся в нем уголовно-процессуальной информации, позволять исследовать и оценивать данную информацию в судебном разбирательстве¹.

В связи с этим, предлагаем ввести в Уголовно-процессуальный кодекс новую статью, посвященную производству по уголовным делам в электронном виде и изложить ее в следующей редакции:

«Статья 161.1. Досудебное производство по уголовному делу в электронном виде

1. Должностное лицо органа предварительного расследования получает доступ к ведению уголовного дела в электронном формате – «Электронное уголовное дело», получая код доступа к авторизации. Так же есть возможность прохождения идентификации по отпечатку пальца. Лицо, осуществляющее производство по уголовному делу, предварительно проходит процедуру регистрации биометрических параметров на устройство хранения цифровых анкетных данных.

2. Решение о выборе формата (электронный или бумажный) производства по уголовному делу принимается по своему усмотрению следователем или дознавателем, которому поручено осуществление предварительного расследования, при принятии его в свое производство.

¹ Соколов Ю.Н. Допустимость рассмотрения материалов уголовного дела в электронной форме // Информационное право. 2017. № 1. - С.26.

После вынесения постановления о принятии дела к своему производству в электронном формате, посредством электронного документооборота в течение 24 часов уведомляется прокурор.

3. В случае выбора электронного формата ведения уголовного дела, заполняется соответствующая электронная форма. Дальнейшее производство по уголовному делу в бумажном формате не допускается.

4. О выборе формата производство по уголовному делу в течении 24 часов следователем или дознавателем уведомляются все заинтересованные участники уголовного судопроизводства.

5. Документы материалов уголовного дела, созданные ранее на бумажном носителе, после принятия решения о производстве по уголовному делу в электронном формате вкладываются в электронное уголовное дело в виде PDF-документов незамедлительно, но не позднее двадцати четырех часов после вынесения постановления о ведении электронного судопроизводства».

Подводя итог вышесказанному, предлагаем внести следующие изменения в законодательство:

1. Считаем целесообразным дополнить ч.1 ст.141 Уголовно-процессуального кодекса положением о том, что Заявление о преступлении может быть сделано в устном, письменном или электронном виде и изложить в следующей редакции:

«Статья 141. Заявление о преступлении

1. Заявление о преступлении может быть сделано в устном, письменном или электронном виде».

2. Предлагаем внедрить в уголовное судопроизводство систему заверения документов электронной цифровой подписью, а также использования идентификации, и аутентификации для установления личности участника уголовного судопроизводства.

3. Предлагаем ввести в Уголовно-процессуальный кодекс новую статью, посвященную производству по уголовным делам в электронном виде и изложить ее в следующей редакции:

«Статья 161.1. Досудебное производство по уголовному делу в электронном виде

1. Должностное лицо органа предварительного расследования получает доступ к ведению уголовного дела в электронном формате – «Электронное уголовное дело», получая код доступа к авторизации. Так же есть возможность прохождения идентификации по отпечатку пальца. Лицо, осуществляющее производство по уголовному делу, предварительно проходит процедуру регистрации биометрических параметров на устройство хранения цифровых анкетных данных.

2. Решение о выборе формата (электронный или бумажный) производства по уголовному делу принимается по своему усмотрению следователем или дознавателем, которому поручено осуществление предварительного расследования, при принятии его в свое производство.

После вынесения постановления о принятии дела к своему производству в электронном формате, посредством электронного документооборота в течение 24 часов уведомляется прокурор.

3. В случае выбора электронного формата ведения уголовного дела, заполняется соответствующая электронная форма. Дальнейшее производство по уголовному делу в бумажном формате не допускается.

4. О выборе формата производство по уголовному делу в течении 24 часов следователем или дознавателем уведомляются все заинтересованные участники уголовного судопроизводства.

5. Документы материалов уголовного дела, созданные ранее на бумажном носителе, после принятия решения о производстве по уголовному делу в электронном формате вкладываются в электронное уголовное дело в виде PDF-документов незамедлительно, но не позднее двадцати четырех часов после вынесения постановления о ведении электронного судопроизводства».

ЗАКЛЮЧЕНИЕ

Для достижения целей уголовного судопроизводства распространение правового режима ЭНИ не только на съемные носители информации (например, карты памяти, флеш-накопители, съемные жесткие диски, оптические диски и др.), но и на сами персональные компьютеры и серверы, а также иные микропроцессорные устройства, конструктивно предназначенные для постоянного или временного хранения компьютерной информации, является обоснованным, что позволяет избежать терминологической путаницы. Вместе с тем распространение данного правового режима на иную микропроцессорную технику, указанную, в частности, профессором Б. В. Веховым, т. е. конструктивно не предназначенную для хранения компьютерной информации, является необоснованным.

В завершении настоящего исследования сформулируем следующие выводы:

1. Необходимо процессуальное закрепление в Уголовно-процессуальный кодекс определение «информационные технологии». Поэтому предлагаем дополнить пунктом 63 статью 5 Уголовно-процессуального кодекса РФ «Основные понятия, используемые в настоящем Кодексе» следующего содержания:

«Информационные технологии в уголовном процессе - совокупность приемов, средств, методов обнаружения, фиксации, собирания, обработки, передачи сотрудниками правоохранительных органов оперативно значимой информации о событиях или действиях, которые впоследствии помогут установить наличие или отсутствие обстоятельств, подлежащих доказыванию, а также иных обстоятельств, имеющих значение для расследования конкретного уголовного дела».

2. Основными направлениями использования информационных технологий в ходе расследования уголовных дел, являются:

- структурирование информации, касающейся хода расследования уголовного дела, а именно, распределение по времени, месту, объекту преступного посягательства, а также подозреваемых лицах. Это поможет сохранить логическую цепочку расследования серийных и многоэпизодных преступлений;
- объективная оценка полученной информации и последующий ее анализ в целях выбора наиболее эффективной тактики расследования конкретного уголовного дела.

3. Появление термина «электронный носитель информации» в УПК РФ следует рассматривать как некий промежуточный шаг на пути к возможному появлению в российском процессуальном праве термина «электронные доказательства».

4. Предлагаем дополнить пунктом 64 статью 5 Уголовно-процессуального кодекса РФ «Основные понятия, используемые в настоящем Кодексе» следующего содержания:

«электронное доказательство – это сведения, содержащиеся на электронных носителях информации или в телекоммуникационной сети «Интернет», имеющие значение для уголовного дела и собранные в порядке предусмотренным настоящим Кодексом».

Исходя из этого, считаем целесообразным добавить в статью 74 часть 2 пунктом 4.1 Уголовно-процессуального кодекса РФ «Доказательства» новым видом доказательств – «электронное доказательство» и изложить ее в следующей редакции:

«1. Доказательствами по уголовному делу являются любые сведения, на основе которых суд, прокурор, следователь, дознаватель в порядке, определенном настоящим Кодексом, устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела.

2. В качестве доказательств допускаются:

1) показания подозреваемого, обвиняемого;

- 2) показания потерпевшего, свидетеля;
- 3) заключение и показания эксперта;
- 3.1) заключение и показания специалиста;
- 4) вещественные доказательства;
- 4.1) электронные доказательства».

5. Предлагаем дополнить пунктом 65 статью 5 Уголовно-процессуального кодекса РФ «Основные понятия, используемые в настоящем Кодексе» следующего содержания:

«Электронный носитель информации – это устройство, конструктивно предназначенное для постоянного или временного хранения информации в виде, пригодном для использования в электронных вычислительных машинах, а также для ее передачи по информационно-телекоммуникационным сетям или обработки в информационных системах».

6. В связи с тем, что нормативное определение электронных носителей не содержит конкретного перечня устройств, которые следует относить к указанному выше понятию, предлагаем внести перечень устройств, которые могут быть использованы в рамках уголовного дела, в Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации» статьей 2.1. следующего содержания: «К электронным носителям информации могут быть отнесены:

- компьютерные системы – компьютер, ноутбук, нэтбук, айпад, планшет, жесткий диск;
- оптические устройства - лазерный диск, компакт-диск, мини-диски, Blu-ray, HD-DVD;
- флеш-накопители и SSD-диски;
- SMART устройства – смартфон, смарт-телевизор, умные часы, фитнес-трекер, смарт-брелки;
- иные устройства, содержащие электронную информацию».

7. В таких странах, как США, Великобритания, Германия, Швеция, Франция, широко распространено использование видеоконференц-связи в

процессе расследования преступлений. Также в Италии, Бельгии, Латвии, Франции и Украине сотрудники правоохранительных органов в процессе своей служебной деятельности используют видеоконференц-связь с целью обеспечения безопасности свидетелей, потерпевших и обвиняемых. Несомненно, перенять Россией данный опыт у зарубежных стран было бы целесообразно, так как в настоящий момент цифровые технологии все больше поглощают современную жизнь общества. Использование видеоконференц-связи необходимо не только на стадии судебных заседаний, но и сотрудниками органов дознания, следствия, уголовного розыска на стадии предварительного расследования уголовных дел.

8. В США законодательно закреплён исчерпывающий перечень электронных доказательств, которые подлежат оценке их относимости, достоверности и достаточности. В связи с чем, считаем необходимым внести в перечень доказательств УПК и электронные доказательства.

9. Разработанный в США Закон «Об облачности», который направлен на получение электронной информации из Облака, находящегося в единой информационной телекоммуникационной сети «Интернет» может оказать положительное влияние и на российское законодательство. Нельзя забывать о том, что информация содержится не только на электронных носителях информации, но также в сети «Интернет». Так же необходимо и российскому законодателю не упускать из вида тот момент, что в настоящее время большая доля преступлений совершается в информационно-телекоммуникационной сети Интернет.

10. Изучив опыт США, было бы возможным на законодательном уровне в России предпринять попытки к созданию инструкции для правоохранительных органов по правильному изъятию электронных носителей информации, чтобы в дальнейшем использовать полученные сведения в качестве доказательств по расследуемым уголовным делам.

11. Достаточно интересной для России является Британская онлайн-Система цифровых дел. Указанная модель позволяет участникам уголовного

судопроизводства осуществлять загрузку и доступ к оперативной информации, хранящейся на одном портале. Сотрудники полиции в Британии оснащены всеми необходимыми инструментами для изъятия электронных носителей информации на месте преступления, а также принимать заявления от граждан в электронном виде и загружать всю необходимую информацию, касающуюся расследования уголовных дел, при помощи мобильных устройств в единый электронный портал.

12. Положительной чертой Германии, которую может позаимствовать Российская Федерация, является система электронного судопроизводства, которая позволяет передавать данные в считанные секунды, а также осуществляется быстрое взаимодействие между следователями, судами и прокуратурой. Принцип работы электронного уголовного дела Германии заключается в том, что все поступающие в правоохранительные органы материалы и документы, касающиеся расследования уголовных дел, хранятся централизованно в едином электронном архиве.

13. В Японии создана отдельная отрасль права, как цифровая криминалистика. Сотрудники правоохранительных органов изучают ее положения и нормы с целью обучения правильному изъятию электронных носителей информации на месте совершения преступления. Исходя из этого, мы делаем вывод о том, что при изъятии электронных носителей информации необходимо придерживаться следующих правил: электронные данные не должны быть изменены; должны быть созданы криминалистически обоснованные дубликаты оригинала исходной информации; экспертиза электронных носителей информации должна проводиться компетентными лицами.

14. Считаем целесообразным дополнить ч.1 ст.141 Уголовно-процессуального кодекса положением о том, что заявление о преступлении может быть сделано в устном, письменном или электронном виде и изложить в следующей редакции:

«Статья 141. Заявление о преступлении

1. Заявление о преступлении может быть сделано в устном, письменном или электронном виде».

15. Предлагаем внедрить в уголовное судопроизводство систему заверения документов электронной цифровой подписью, а также использования идентификации, и аутентификации для установления личности участника уголовного судопроизводства.

16. Предлагаем ввести в Уголовно-процессуальный кодекс новую статью, посвященную производству по уголовным делам в электронном виде и изложить ее в следующей редакции:

«Статья 161.1. Досудебное производство по уголовному делу в электронном виде

1. Должностное лицо органа предварительного расследования получает доступ к ведению уголовного дела в электронном формате – «Электронное уголовное дело», получая код доступа к авторизации. Так же есть возможность прохождения идентификации по отпечатку пальца. Лицо, осуществляющее производство по уголовному делу, предварительно проходит процедуру регистрации биометрических параметров на устройство хранения цифровых анкетных данных.

2. Решение о выборе формата (электронный или бумажный) производства по уголовному делу принимается по своему усмотрению следователем или дознавателем, которому поручено осуществление предварительного расследования, при принятии его в свое производство.

После вынесения постановления о принятии дела к своему производству в электронном формате, посредством электронного документооборота в течение 24 часов уведомляется прокурор.

3. В случае выбора электронного формата ведения уголовного дела, заполняется соответствующая электронная форма. Дальнейшее производство по уголовному делу в бумажном формате не допускается.

4. О выборе формата производство по уголовному делу в течении 24 часов следователем или дознавателем уведомляются все заинтересованные участники уголовного судопроизводства.

5. Документы материалов уголовного дела, созданные ранее на бумажном носителе, после принятия решения о производстве по уголовному делу в электронном формате вкладываются в электронное уголовное дело в виде PDF-документов незамедлительно, но не позднее двадцати четырех часов после вынесения постановления о ведении электронного судопроизводства».

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Законы, нормативные правовые акты и иные официальные документы

1. Конституция (Основной Закон) Российской Федерации – России : принята всенародным голосованием 12 декабря 1993 г. (в ред. от 05.02. 2014. № 2 –ФКЗ)// Рос. газета. – 1993. – 25 дек.; Собрание законодательства РФ. – 2014. - № 6. – Ст. 548
2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63: Федеральный закон: принят Гос. Думой 24 мая 1996 г.: по состоянию на 07 апреля 2020 г. – Собрание законодательства РФ. 1996. № 25. Ст. 2954.
3. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ: Федеральный закон: принят Гос. Думой 22 ноября 2001 г.: по состоянию на 24 апреля 2020 г. – Собрание законодательства РФ. 2001. № 52 (ч. I). Ст. 4921.
4. О национальной платежной системе: Федеральный закон от 27.06.2011 N 161-ФЗ (с изм. и доп., вступ. в силу с 27.12.2019). // Собрание законодательства РФ. 2011. № 27. Ст. 3872.
5. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ (с изм. и доп., вступ. в силу с 03.04.2020) // Собрание законодательства РФ, 31.07.2006, N 31 (1 ч.), ст. 3448
6. Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 № 144-ФЗ (с изм. и доп., вступ. в силу с 02.08.2019) // Собрание законодательства РФ. – 1995. - N 33. - Ст. 3349.
7. О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации: федер. закон от 28 июля 2012 г. № 143-ФЗ // Собрание законодательства РФ. 2012. № 31. Ст. 4332.

8. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: указ Президента РФ от 9 мая 2017 г. № 203 // СЗ РФ. 2017. № 20. Ст. 2901.

9. Об утверждении программы «Цифровая экономика Российской Федерации»: распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р. // Доступ из справ.-правовой системы «КонсультантПлюс».

10. Приказ МВД России N 776, Минобороны России N 703, ФСБ России N 509, ФСО России N 507, ФТС России N 1820, СВР России N 42, ФСИН России N 535, ФСКН России N 398, СК России N 68 от 27.09.2013 «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд» (Зарегистрировано в Минюсте России 05.12.2013 N 30544) // Российская газета. - N 282. – 2013.

11. Приказ МВД России «Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях» от 29.08.2014 г. № 736 // Справочно-правовая система «ГАРАНТ»

12. Приказ Минтруда России от 01.11.2016 N 598н «Об утверждении профессионального стандарта Специалист по безопасности компьютерных систем и сетей» (Зарегистрировано в Минюсте России 28.11.2016 N 44464) // Доступ из справ.-правовой системы «ГАРАНТ».

13. ГОСТ 2.051-2006 Единая система конструкторской документации. Электронные документы. Общие положения. [Электронный ресурс]. Режим доступа: <http://www.gostbaza.ru/?gost=4288> (дата обращения: 12.03.2020).

14. Постановление Пленума Верховного Суда РФ от 16.04.2013 № 9 «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 31 октября 1995 года № 8 «О некоторых вопросах применения судами Конституции Российской Федерации при осуществлении правосудия»// Бюллетень Верховного Суда РФ. № 6. 2013.

Монографии, учебники, учебные пособия

15. Белкин, А. Р. Теория доказывания в уголовном судопроизводстве. В 2 ч. Часть 1: учеб. пособие для вузов. / А. Р. Белкин. – 2-е изд., испр и доп. – Москва: Юрайт, 2018. – 235 с.

18. Голованова Н.А., Гравина А.А., Зайцев О.А. Уголовно-юрисдикционная деятельность в условиях цифровизации: монография // институт законодательства и сравнительного правоведения при Правительстве Российской Федерации. "ИЗиСП", "КОНТРАКТ". – 2019 г. – 130 с.

24. Зазулин А.И. Правовые и методологические основы использования цифровой информации в доказывании по уголовному делу: дисс. ... канд. юр. наук: 12.00.09 / Уральский государственный юридический университет. – Екб., 2018 – 250 с.

25. Медведева М.О. Уголовно-процессуальная форма информационных технологий: современное состояния и основные направления развития: дисс. ... канд. юр. наук: 12.00.09 / Моск.университет МВД РФ им В.Я.Киотя. – М., 2018. – 250 с.

Статьи, научные публикации

26. Бойчук, А. В. Изъятие электронных носителей информации в уголовном судопроизводстве Российской Федерации / А. В. Бойчук; Байкальский государственный университет // Проблемы становления гражданского общества: сборник статей VI Международной научной студенческой конференции. – 2018. – С.236-245.

16. Булыжкин, А. В. К вопросу о состоянии правового регулирования и правоприменения порядка изъятия электронных носителей информации: учеб. пособие для вузов // Современное уголовно-процессуальное право – уроки истории проблемы дальнейшего реформирования. – 2019. – Т. 1. – № 1 (1). – С.158-163.

17. Васюков, В. Ф. Особенности изъятия электронных носителей информации при производстве следственных действий: новеллы законодательства и проблемы правоприменения // Криминалистика: вчера, сегодня, завтра. – 2019. – № 2 (10). – С.30-38.

19. Горкина, Е. В. О некоторых проблемах изъятия электронной информации и ее носителей учеб. пособие. // Научный альманах. – 2019. – С.329-339.

27. Горбанева, В. С. К вопросу об электронных доказательствах в уголовном судопроизводстве России / В. С. Горбанева ; СГУ им. Н. Г. Чернышевского // Актуальные проблемы социально-гуманитарных наук и образования: сущность, концепции, перспективы: материалы VII Международной научной конференции. – 2019. – С.865-877.

28. Григорьев, В. Н. Об электронных носителях информации в уголовном судопроизводстве / В. Н. Григорьев, О. А. Максимов ; Нижегородский государственный университет им Н. И. Лобачевского // Вестник нижегородского университета им. Н. И. Лобачевского. – 2019. – № 3. – С.116-123.

29. Григорьев, В. Н. Понятие электронных носителей информации в уголовном судопроизводстве / В. Н. Григорьев, О. А. Максимов ; Научно-исследовательский институт ФСИН России // Вестник Уфимского юридического института МВД России. – 2019. – № 2 (84). – С.95-103.

30. Григорьева, М. А. Информация, полученная из сети Интернет, как доказательства в уголовном судопроизводстве / М. А. Григорьева ; Сибирский федеральный университет // Инновационные тенденции развития российской науки : материалы X Международной научно-практической конференции молодых ученых, посвященной Году экологии и 65-летию Красноярского ГАУ. – 2017. – С.89-95.

31. Гришин, А. И. Электронная информация как средство доказывания в уголовном судопроизводстве / А. Н. Гришин ; СГУ им. Н. Г. Чернышевского // Взаимодействие власти, бизнеса и общества в развитии цифровой экономики :

материалы XI Международной научно-практической конференции. – 2018. – С.91- 96.

32. Губарева, Е. К. Информация, содержащаяся на электронном носителе, как вид доказательства по уголовному делу / Е. К. Губарева; Самарский Государственный Экономический университет // Татищевские чтения: актуальные проблемы науки и практики: материалы XVI Международной научно-практической конференции. В 2-х томах. Том. 1. – 2019. – С.150-154.

20. Дёмин, К. Е. Об методических основах получения криминалистически значимой информации, содержащейся в электронных носителях данных // Вестник московского университета МВД России. – 2018. – № 4. – С.53-60.

21. Дёмин, К. Е. О тактике получения криминалистически значимой информации, содержащейся в электронных документах и электронных носителя данных // Обеспечение прав и законных интересов граждан в деятельности органов дознания и представительного следствия. – 2018. – С.187-190 с.

22. Добровлянина, О. В. Некоторые аспекты о процессуальном изъятии (копировании) электронных носителей информации // Пермский юридический альманах. – 2019. – № 2. – С.1159-1170.

33. Евдокименко, А. М. Особенности изъятия электронных носителей информации / А. М. Евдокименко, М. О. Янгаева ; Барнаульский юридический институт МВД Российской Федерации // Криминалистика: теория и практика : материалы VII Международной научно-практической конференции. – 2019. – С.176-188.

34. Зайцев, О. А. Использование электронной информации в качестве доказательств по уголовному делу / О. А. Зайцев // Актуальные вопросы производства предварительного следствия: теория и практика: сборник научных трудов Всероссийской научно-практической конференции. – 2019. – С. 200-205.

23. Зазулин, А. И. Получение следователем информации, содержащейся в сообщениях, передаваемых посредством электронной почты и мессенджеров: проблемы процессуального регулирования // Российский следователь. – 2018. – № 5. – С.23-28.

35. Уткин В.В. Цифровые технологии в институциональной реформе уголовного процесса.// Журнал «Труды Академии управления МВД России», № 4, октябрь-декабрь 2018 г., С.87-93.

Эмпирические материалы

36. Состояние преступности 2019 года. [Электронный ресурс]. Режим доступа: <http://www.gostbaza.ru/?gost=4288> (дата обращения: 12.03.2020).

ПРИЛОЖЕНИЯ

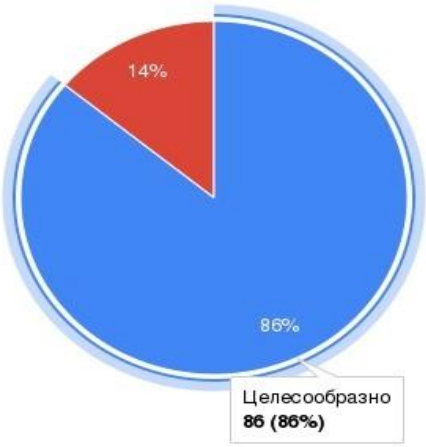
Приложение №1

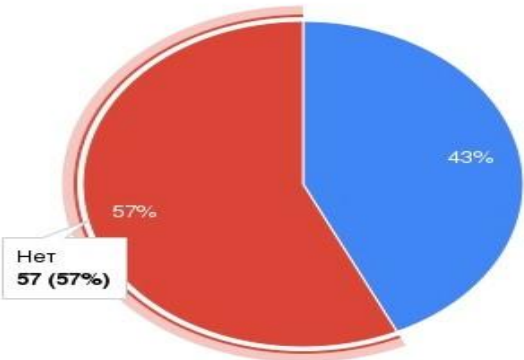
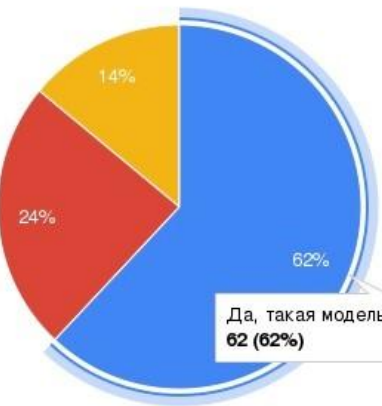
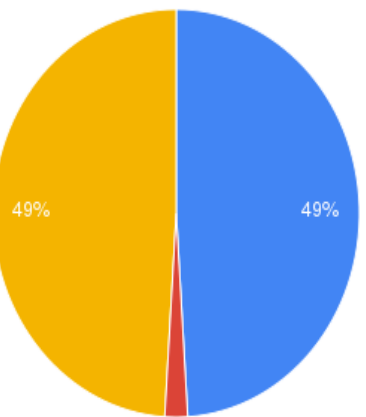
**Перечень вопросов для анкетирования сотрудников следственных органов
и органов дознания по вопросам исследования проблем внедрения
информационных технологий в российский уголовный процесс.**

п/п	Вопросы	Варианты ответов
1	Насколько целесообразно на Ваш взгляд будет внедрение в уголовно-процессуальную деятельность ОВД электронного документооборота в ходе взаимодействия с судом и иными контрольно-надзорными органами вне системы подразделений ОВД?	Целесообразно
		Нецелесообразно
		Затрудняюсь ответить
2	Сталкивались ли вы с необходимостью производства изъятия электронных носителей информации?	Да
		Нет
		Иное
3	Как вы считаете, возможно ли производство предварительного расследования по уголовному делу в электронном виде?	Да такая модель перспективна
		Нет, необходимо сохранить существующую «бумажную» модель уголовного судопроизводства
		Иное

4	Целесообразно ли, по Вашему мнению, обязательное участие специалиста при производстве осмотра и выемки электронных носителей информации?	Да участие специалиста является необходимым и важным условием
		Нет, проведение таких следственных действий возможно без привлечения специалиста
		Привлечение специалиста необходимо, но по усмотрению следователя, дознавателя
		Иное

**Результаты анкетирования сотрудников следственных органов и органов
дознания по вопросам исследования проблем внедрения информационных
технологий в российский уголовный процесс**

/п	Вопросы	Варианты ответов
1	Насколько целесообразно на Ваш взгляд будет внедрение в уголовно- процессуальную деятельность ОВД электронного документооборота в ходе взаимодействия с судом и иными контрольно- надзорными органами вне системы подразделений ОВД?	 Целесообразно 86 (86%) Целесообразно 86% 14% Целесообразно Нецелесообразно

2	Сталкивались ли вы с необходимостью производства изъятия электронных носителей информации?	 ● Да ● Нет
3	Как вы считаете, возможно ли производство предварительного расследования по уголовному делу в электронном виде?	 ● Да, такая модель перспективна ● Нет, необходимо сохранить существующую «бумажную» модель уголовного судопроизводства ● Иное
4	Целесообразно ли, по Вашему мнению, обязательное участие специалиста при производстве осмотра и выемки электронных носителей информации?	 ● Да, участие специалиста является необходимым и важным условием ● Нет, проведение таких следственных действий возможно без привлечения специалиста ● Привлечение специалиста необходимо, но по усмотрению следователя, дознавателя

Проект Федерального закона «О внесении изменений в статьи 5, 74, 141 Уголовно-процессуального кодекса Российской Федерации, а также дополнении Уголовно-процессуального кодекса Российской Федерации статьей 161.1»

Внести в Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 №174-ФЗ, принятый Государственной Думой Федерального Собрания Российской Федерации 22.11.2001 в редакции от 24.04.2020 (Собрание законодательства РФ от 24.12.2001. - №52 (ч. I) – Ст. 4921) следующие изменения:

1) Дополнить статью 5 пунктами 63-65 следующего содержания:

«63) Информационные технологии в уголовном процессе - совокупность приемов, средств, методов обнаружения, фиксации, собирания, обработки, передачи сотрудниками правоохранительных органов оперативно значимой информации о событиях или действиях, которые впоследствии помогут установить наличие или отсутствие обстоятельств, подлежащих доказыванию, а также иных обстоятельств, имеющих значение для расследования конкретного уголовного дела;

64) электронное доказательство – это сведения, содержащиеся на электронных носителях информации или в телекоммуникационной сети «Интернет», имеющие значение для уголовного дела и собранные в порядке предусмотренным настоящим Кодексом»;

65) Электронный носитель информации – это устройство, конструктивно предназначенное для постоянного или временного хранения информации в виде, пригодном для использования в электронных вычислительных машинах, а также для ее передачи по информационно-телекоммуникационным сетям или обработки в информационных системах»

2) Изложить статью 74 в следующей редакции:

«Статья 74. Доказательства

«1. Доказательствами по уголовному делу являются любые сведения, на основе которых суд, прокурор, следователь, дознаватель в порядке, определенном настоящим Кодексом, устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела.

2. В качестве доказательств допускаются:

- 1) показания подозреваемого, обвиняемого;
- 2) показания потерпевшего, свидетеля;
- 3) заключение и показания эксперта;
- 3.1) заключение и показания специалиста;
- 4) вещественные доказательства;
- 4.1) электронные доказательства».
- 5) протоколы следственных и судебных действий;
- 6) иные документы».

3) Изложить ч.1 ст. 141 в следующей редакции:

«1. Заявление о преступлении может быть сделано в устном, письменном или электронном виде».

4) Дополнить главу 21 статьей 161.1 следующего содержания:

«Статья 161.1. Досудебное производство по уголовному делу в электронном виде

1. Должностное лицо органа предварительного расследования получает доступ к ведению уголовного дела в электронном формате – «Электронное уголовное дело», получая код доступа к авторизации. Так же есть возможность прохождения идентификации по отпечатку пальца. Лицо, осуществляющее производство по уголовному делу, предварительно проходит процедуру регистрации биометрических параметров на устройство хранения цифровых анкетных данных.

2. Решение о выборе формата (электронный или бумажный) производства по уголовному делу принимается по своему усмотрению следователем или

дознавателем, которому поручено осуществление предварительного расследования, при принятии его в свое производство.

После вынесения постановления о принятии дела к своему производству в электронном формате, посредством электронного документооборота в течение 24 часов уведомляется прокурор.

3. В случае выбора электронного формата ведения уголовного дела, заполняется соответствующая электронная форма. Дальнейшее производство по уголовному делу в бумажном формате не допускается.

4. О выборе формата производство по уголовному делу в течении 24 часов следователем или дознавателем уведомляются все заинтересованные участники уголовного судопроизводства.

5. Документы материалов уголовного дела, созданные ранее на бумажном носителе, после принятия решения о производстве по уголовному делу в электронном формате вкладываются в электронное уголовное дело в виде PDF-документов незамедлительно, но не позднее двадцати четырех часов после вынесения постановления о ведении электронного судопроизводства».

Президент
Российской Федерации

Кафедра уголовного процесса

УТВЕРЖДАЮ

Начальник кафедры уголовного
процесса Казанского юридиче-
ского института МВД России
полковник полиции

 Д.Р.Марданов
«17» июня 2019 года

ПЛАН-ГРАФИК
выполнения выпускной квалификационной работы

Тема: Уголовно-процессуальные аспекты использования электронных носителей информации в уголовном судопроизводстве

Курсант (слушатель): Веселова Анна Олеговна
(фамилия, имя, отчество)

Учебная группа № 051

Специальность Правоохранительная деятельность

Форма обучения Очная Год набора 2015

№ п/п	Характер работы. Главы, параграфы и их содержание	Примерный объем выполнения (в %)	Срок выполнения	Отметка руководителя о выполнении
1.	Введение	5%	Июль- август 2019 г.	
2.	Глава 1. Электронная информация в уголовном судопроизводстве как источник доказательств: понятие и сущность §1. Правовая регламентация применения электронной информации и электронных носителей информации в уголовно-процессуальном законодательстве РФ §2. Зарубежный опыт использования электронной информации в уголовном судопроизводстве	55%	Сентябрь - декабрь 2019г.	

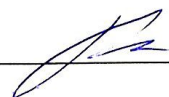
№ п/п	Характер работы. Главы, параграфы и их содержание	Примерный объем выполнения (в %)	Срок выполнения	Отметка руководителя о выполнении
	производстве в качестве до- казательства			
3.	Глава 2. Уголовно- процессуальные и организаци- онные аспекты обнаружения, изъятия и использования элек- тронной информации при про- изводстве по уголовному делу §1. Уголовно-процессуальная форма и способы получения информации, содержащейся в электронных носителях и элек- тронных сообщениях §2. Процессуальные и орга- низационные аспекты произ- водства по уголовному делу в электронном виде	85%	Январь – февраль 2020 г..	
4.	Заключение	95%	Январь – февраль 2020 г.	
5.	Список использованных ис- точников	100%	Январь – февраль 2020 г.	
6.	Подготовка, обобщение и апробация результатов научно- исследовательской работы по теме ВКР (анкетирование, те- зисы, выступление, публика- ция в сборниках и т.п.)		Сентябрь 2019 г. – май 2020 г.	

Подпись выпускника


 А.О.Веселова
 «17» июля 2019 г.

Согласовано

Руководитель



**Отзыв о работе обучающейся 051 учебной группы очной формы
обучения, 2015 года набора по специальности 40.05.02 -
«Правоохранительная деятельность» Веселовой Анны Олеговны
на тему: «Уголовно-процессуальные аспекты использования
электронных носителей информации в уголовном судопроизводстве»**

Выполненная слушателем выпускная квалификационная работа, посвящена весьма актуальной на сегодняшний день теме. Современные информационные технологии все интенсивнее проникают в деятельность государственных органов. Использование в повседневной деятельности информационных ресурсов позволяет государству систематизировать и анализировать поступающую информацию, предоставлять услуги населению и т.д. Не является исключением из правил и уголовно-процессуальная сфера деятельности государства. Так, за последние годы в УПК РФ было внесено значительное количество изменений закрепляющих процессуальный порядок использования информационных технологий при производстве по уголовному делу. Например, предусмотрен порядок вызова участников процесса на судебное заседание путем направления СМС-уведомления, также регламентирован порядок участия подсудимого в судебном заседании посредством видео-конференц связи и т.д. Кроме того, законодатель ввел в УПК понятие «электронного носителя информации» в качестве специального предмета обыска или выемки, а также предусмотрел процессуальный порядок его изъятия. Вместе с тем, данная дефиниция носит сугубо технологический характер, правовые границы которого не ограничены. В связи этим возникает необходимость в осмыслении данного понятия и формулировании рекомендаций по совершенствованию его использования в процессуальном законодательстве.

Представленная работа состоит из двух глав, состоящих из четырех параграфов. Структура работы обусловлена необходимостью определить общетеоретическое и правовое значение понятия «электронный носитель информации», «компьютерная информация». Автор, используя различные нормативные правовые акты и научную литературу, обоснованно делает вывод о различной трактовке данных понятий не только на доктринальном, но и на нормативном уровне. Далее автором, приводятся аргументы о наличии доказательственного значения электронных носителей информации и необходимости их использования при производстве по уголовному делу. Во второй главе автор исследования приводит основные процессуальные способы сбора электронной доказательственной информации, а также особенности использования специальных познаний при ее получении. В заключении автор формулирует обоснованные предложения по совершенствованию законодательного определения понятия электронные носители информации, и процессуального порядка их получения при производстве по уголовному делу.

На всем протяжении выполнения выпускной квалификационной работы слушатель Веселова А.О. добросовестно и дисциплинировано

выполняла задания научного руководителя, провела собственное эмпирическое исследование в форме опроса практических сотрудников ОВД, изучала новейшую российскую и зарубежную литературу, посвященную теме работы. Существенным результатом исследования, проведенного слушателем, является проект Федерального закона «О внесении изменений в УПК РФ», который был включен в работу в качестве приложения.

В ходе своего исследования автором использовались различные источники, в том числе научные публикации посвященные теме использования современных информационно-телекоммуникационных технологий в уголовном процессе, проанализирован значительный массив нормативно-правовых актов, закрепляющих понятие и правовые основы использования электронных носителей информации.

В целом, исследование автора работы, проведено всесторонне и основано на действующем законодательстве и существующей уголовно-процессуальной доктрине. Выпускная квалификационная работа выполнена аккуратно, в научном стиле изложения и заслуживает высокой оценки.

Руководитель:

Старший преподаватель
кафедры уголовного процесса
кандидат юридических наук
капитан полиции

«25» мая 2020 г.



Т.И. Гарипов

С ей заявл ознакомлен

А.В. Вассенова

РЕЦЕНЗИЯ

на выпускную квалификационную работу

слушателя 051 учебной группы очной формы обучения, 2015 года набора, по специальности 40.05.02 «Правоохранительная деятельность»

Веселовой Анны Олеговны

на тему: «Уголовно-процессуальные аспекты использования электронных носителей информации в уголовном судопроизводстве»

Актуальность и новизна темы. Представленная для рецензирования выпускная квалификационная работа выполнена на актуальную для современного состояния общества тему. Современные информационные технологии все интенсивнее проникают в деятельность государственных органов. Использование в повседневной деятельности информационных ресурсов позволяет государству систематизировать и анализировать поступающую информацию, предоставлять услуги населению и т.д. Не является исключением из правил и уголовно-процессуальная сфера деятельности государства. Так, за последние годы в УПК РФ было внесено значительное количество изменений закрепляющих процессуальный порядок использования информационных технологий при производстве по уголовному делу.

Оценка плана и структуры работы.

Цели и задачи работы соответствуют ее названию. План работы составлен логично, что позволило автору последовательно изложить исследуемый материал. Структура работы обусловлена целью исследования и задачами, которые решались для ее достижения. Работа состоит из введения, двух глав, объединяющих четыре параграфа, заключения, списка использованной литературы и приложений. Исследуемая проблематика по частям работы изложена равномерно.

Полнота изложения вопросов темы.

Во введении дипломной работы автор обосновывается актуальность исследуемой темы, характеризуется ее теоретическая разработанность, указаны объект и предмет исследования, обозначены цели и задачи, описаны методология и научная новизна исследования, а также обосновывается практическая значимость данной работы.

В первой главе автор рассматривает правовую регламентацию применения электронной информации и электронных носителей информации в уголовно-процессуальном законодательстве РФ, а также изучает зарубежный опыт использования электронной информации в уголовном судопроизводстве в качестве доказательства.

Во второй главе автор рассматривает уголовно-процессуальную форму и способы получения информации, содержащейся в электронных носителях и электронных сообщениях, а также возможность осуществления производства по уголовному делу в электронном виде.

В заключении сформулированы выводы и предложения по рассмотренной теме исследования.

Степень научности, глубина теоретического анализа проблемы.

Автор выпускной квалификационной работы правильно в работе расставляет акценты, анализирует значительный массив нормативно-правовых актов, закрепляющих понятие и правовые основы использования электронных носителей информации, а также предусматривает возможность осуществления производства по уголовному делу в электронном виде.

Степень организованности и самостоятельности при выполнении работы.

При выполнении дипломной работы автор использовал достаточное количество нормативных правовых актов, учебных пособий, монографий и диссертаций, анализируя уголовно-процессуальные аспекты использования электронных носителей информации в уголовном судопроизводстве.

В работе присутствуют выводы и заключения, к которым автор пришел самостоятельно, изучая заявленную тему.

Практическая направленность работы. На основе изученного материала в процессе выполнения выпускной квалификационной работы, автор делает самостоятельные выводы и заключения.

Полнота использования нормативных актов и других литературных источников. Автор при написании работы использовал достаточное количество литературы, нормативную правовую базу.

Степень решения слушателем поставленных задач. Слушатель в достаточной степени решил поставленные перед ним задачи и достиг цели исследования.

Оформление выводов и заключения. Выводы и заключения, сделанные автором, соответствуют логике изложения материала, а также целям и задачам, поставленным при выполнении работы.

Заключение о соответствии работы предъявляемым требованиям и предложения об оценке. Представленная на рецензирование выпускная квалификационная работа соответствует предъявляемым требованиям и может быть допущена к защите с рекомендованной положительной оценкой.

Рецензент:

Начальник ОУР

ОП №16 «Япеева»

УМВД России по г.Казани

подполковник полиции

«3» июля 2020 г.

С рецензией ознакомлена

«3» июля 2020г.



И.Н.Газизов

А.О.Веселова



АНТИПЛАГИАТ
ТВОРИТЕ СОБСТВЕННЫМ УМОМ



Казанский юридический
институт МВД России

СПРАВКА о результатах проверки текстового документа на наличие заимствований

Проверка выполнена в системе
Антиплагиат.ВУЗ

Автор работы **Веселова Анна Олеговна**

Подразделение 051 уч. гр.

Тип работы Не указано

Название работы диплом Веселова

Название файла диплом Веселова.docx

Процент заимствования **27.13 %**

Процент самоцитирования **0.00 %**

Процент цитирования **23.60 %**

Процент оригинальности **49.27 %**

Дата проверки **11:32:35 26 июня 2020г.**

Модули поиска
Модуль поиска ИПС "Адилет"; Модуль выделения библиографических записей; Сводная коллекция ЭБС; Коллекция РГБ; Цитирование; Модуль поиска переводных заимствований; Модуль поиска переводных заимствований по elibrary (EnRu); Модуль поиска переводных заимствований по интернет (EnRu); Коллекция eLIBRARY.RU; Коллекция ГАРАНТ; Модуль поиска Интернет; Модуль поиска "КЮИ МВД РФ"; Коллекция Медицина; Сводная коллекция вузов МВД; Модуль поиска перефразирований eLIBRARY.RU; Модуль поиска перефразирований Интернет; Коллекция Патенты; Модуль поиска общепотребительных выражений; Кольцо вузов

Работу проверил каф. Уг. процесса

ФИО проверяющего

Дата подписи

26.06.2020

Подпись проверяющего

Чтобы убедиться
в подлинности справки,
используйте QR-код, который
содержит ссылку на отчет.



Ответ на вопрос, является ли обнаруженное заимствование
корректным, система оставляет на усмотрение проверяющего.
Предоставленная информация не подлежит использованию
в коммерческих целях.