АКАДЕМИЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ ПРИ ГЕНЕРАЛЬНОЙ ПРОКУРАТУРЕ РЕСПУБЛИКИ КАЗАХСТАН

АБЗЕЛОВ АРНУР АБДУАХЫПОВИЧ

ЦИФРОВЫЕ ДОКАЗАТЕЛЬСТВА И ПРОБЛЕМЫ ДОКАЗЫВАНИЯ В УГОЛОВНОМ ПРОЦЕССЕ

Диссертация
на соискание академической степени магистра юридических наук
по специальность «6М030100 Юриспруденция»

Научный руководитель:
Доцент кафедры общих юридических дисциплин, Амерханов Р.А., кандидат юридических наук, юрист 1-го класса

_____

Қосшы, 2020

Түйіндеме. Бұл жұмыс белгілеу мен аббревиатурадан, презентациядан, екі бөлімнен, қорытындыдан және пайдаланылған әдебиеттер тізімінен тұрады. Сандық дәлелдемелерді іздеумен және тексерумен байланысты мәселелер. Сандық (компьютерлік) дәлелдемелер және сандық (компьютерлік) ақпарат терминдері, сондай-ақ құқықтық және ұйымдастырушылық мәселелерді шешу ұсынылады.

Резюме. Диссертационная работа состоит из обозначении и сокращении, введения, двух разделов, пяти подразделов, заключения и списка использованной литературы. В работе отражены проблемы обозначения цифровых (компютерных) доказательств, сбора, оценки и проверки цифровых информации, об обязательном привлечении IT специалиста для изъятия, копирования и проверки цифровых доказательств. Предложены термины цифровые (компьютерные) доказательства и цифовая (компьютерная) информация, а также решение пролебем правового и организационного характера.

Summary. This work consists of designation and abbreviation, presentation, two sections, conclusion and list of references. Problems associated with the search and verification of digital evidence. The terms digital (computer) evidence and digital (computer) information are proposed, as well as a solution to legal and organizational issues.

С О Д Е Р Ж А Н И Е

Обозначения и сокращения 4

Введение 5

1. Понятие и виды цифровых доказательств в уголовном процессе

1.1. Понятие цифровых доказательств в уголовном процессе 11

1.2. Разграничение цифровой информации от вещественных доказательств и иных документов 25

1.3 Классификация цифровых информации как самостоятельного вида доказательств в уголовном процессе 36

2. Собирание, проверка и оценка цифровой информации как самостоятельного вида доказательств в уголовном процессе

2.1. Собирание цифровой информации на досудебной стадии 47

2.2. Исследование (проверка) цифровой информации в уголовном процессе 65

2.3. Оценка цифровой информации в уголовном процессе 76

Заключение 94

Список используемой литературы 97

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

РК или Казахстан	Республика Казахстан
РФ или Россия	Российская Федерация
Белоруссия	Республика Белоруссия
Украина	Республика Украина
СССР	Союз Советских Социалистических Республик
СНГ	Содружество независимых государств
США	Соединенные Штаты Америки
Госорганы	государственные органы
ВС	Верховный Суд
ЦОН	Центы обслуживания населения
ОРМ	Оперативно-розыскные мероприятия
ЗРК	Закон Республики Казахстан
УПК	Уголовно-процессуальный кодекс
УК	Уголовный кодекс
ГК	Гражданский кодекс
ФЗ	Федеральный закон
ст.	Статья
ч.	Часть
п.	Пункт
и т.д.	и так далее
в т.ч.	в том числе
т.е.	то есть
т.к.	так как
г.	Год
С.	Страница
физлиц	физические лица
НТС	научно-технических средств
СМИ	средства массовой информации
ЭВМ	электронно-вычислительные машины
ОЗУ	оперативное запоминающее устройство
ПО	программное обеспечение
ГОСТ	государственный стандарт, который формулирует требования государства к качеству продукции, работ и услуг, имеющих межотраслевое значение
СЭВ	Совет Экономической Взаимопомощи
ДТП	дорожно-транспортные происшествия
АКП	автоматическая коробка передач
ЛЭП	Линия электронной передачи
ЭТС	Электрических транспортных средств
ЭБУ или ЭКУ	Электронный блок управления
ОУП	орган уголовного преследования

ВВЕДЕНИЕ

Актуальность темы исследования. Еще 20-ть лет назад никто не поверил бы, что в РК практически в каждом доме будет персональный компьютер либо ноутбук с доступом к Интернету, возможность переговоров в режиме «онлайн» через различные средства связи и видеть лицо собеседников находящихся в разных частях света.

Во всем мире, в т.ч. РК повышается уровень цифровой грамотности общества, люди развивают бизнес, пользуясь «электронными деньгами», «электронными кошельками», расплачиваясь, за предоставленные им услуги и товары уже не только пластиковыми банковскими картами, а через мобильные банковские и иные приложения. Появились те, кто вшивает под кожу чипы, со своими персональными данными, банковскими счетами и т.д.

Билеты на самолет, поезда, вызов такси, бронирование ресторанов и гостинец все можно также заказать и оплатить по разным техническим средствам, таких как ноутбук, нетбук, персональный компьютер, смартфон.

Информационно-коммуникационные технологии уже используется не только военными, правоохранительными и разведывательными органами, но и в повседневной жизни: органах представительной, законодательной и судебной власти; медицине и здравоохранении; образовании и науке, бизнес.

В целях оказания различных услуг первоначально созданы ЦОНы, с принципами одного окна, куда обратившись, получаешь услугу от любого госоргана или учреждения, сейчас нет необходимости ходить и собирать различные справки и документы для получения пособия, пенсии, документа удостоверяющего личность или правом управлять автомобилем и т.д.

На данный момент большинство услуг предоставляемых ЦОНами, можно получить «онлайн» не выходя из дома, достаточно лишь через имеющиеся технические средства зайти на портал «Электронного Правительства», выбрать и заказать нужную тебе услугу.

Проникновение во все сферы общества информационных и телекоммуникационных технологий уже не прихоть, а нужда требуемая временем, служащее одним из условий для перехода к цифровому обществу.

Возможно, не так все гладко в развитии информационных и телекоммуникационных технологий в РК, как это показало введенное Указом Президента от 15.03.2020 г. с середины марта по конец апреля 2020 года в стране чрезвычайного положения, в результате разыгравшейся во всем мире пандемии болезни «коронавируса». Мы увидели слабые стороны развития Цифрового Казахстана, отсутствие Интернета в отдельных регионах, когда преподавателям и учащимся для обеспечения дистанционного обучения приходилось выходить из домов, выезжать на более возвышенные местности, а также сбой (зависание или невозможность входа в систему) в «Электронном Правительстве».

Теперь все минусы, выявленные в этот период, нужно превратить в плюс, после анализа всех минусов нужно начать исправлять и совершенствовать, т.к. надо помнить, что если такие сбой произошли в результате слабости технической стороны и плохого финансирования, то, что будет, при специальных атаках на системы госорганов.

Нужно помнить, что информационные технологии и прогресс стимулировали использование научных открытий в криминальных целях хищения имущества физических и юридических лиц, их персональных данных и секретов. Причем злоумышленникам не важно, каким образом обогащаться и чье имущество похищать (государственное или частное). Данное обстоятельство представляет серьезную угрозу для экономики, т.к. возникают возможности проникновение криминала в компьютерные системы госорганов, банков, иных организаций и технические устройства физлиц.

Законодатель предусмотрел уголовную ответственность за совершение преступлений, с помощью различных технологий имеющих функции как у компьютера. Несмотря на то, что есть отдельная глава 7 УК РК «Уголовные правонарушения в сфере информатизации и связи», она не может полностью охватить преступные деяния, т.к. отдельные нормы «сидят» в других главах кодекса, к ним можно отнести мошенничество, кражу, экстремизм и т.д.

Если действия криминала еще можно как то квалифицировать, то иногда выявить их местонахождение, собрать достаточных доказательств о совершении ими уголовных правонарушении задача не из легких. При расследовании преступлений с использованием технических средств, имеют значения следы их совершения, которые после процессуального закрепления приобретают доказательственные значение. По этой причине, приобретает актуальность использование в качестве доказательств цифровой или компьютерной информаций и ее обозначение как цифровых доказательств. Однако, как бы, не было тяжело выявить или собрать цифровые доказательства, ОУП нужно обеспечить процессуальный порядок обнаружения, закрепления, изъятия, сохранения и исследования информации, в целях последующего использованиях их в качестве доказательств по уголовному делу.

Вопрос выяснения роли цифровой (компьютерной) информации в уголовном процессе, ее классификация, понимание значения цифровых доказательств, требует научного и практического решения. Нужно помнить, что ошибки, допускаемые при досудебном уголовном процессе с цифровой информацией, влечет ее утрату, следовательно, влечет утрату доказательств.

Исследование по нашему мнению приведет, к более эффективному проведению досудебных расследований правонарушений, совершенных с использованием современных технических устройств, что служит одним их приоритетных направлений, т.к. важной целью науки является возможность предвидения. Стоит отметить, что прогноз развития видов доказательств позволит ускорить процесс их практического применения.

Степень научной разработанности темы исследования. Количество научных исследований, посвященных вопросам применения цифровых (электронных) доказательств в уголовном процессе РК очень мал. Однако, вопрос киберпреступлении и применения цифровых доказательств интересен для многих практиков и научных деятелей, особенно среди молодых ученых. В юридических журналах и сборниках конференции не много, но появляются научные труды, в особенности интересны публикации Д.П. Утепова.

Всесторонним изучением же института компьютерных или цифровых доказательств в России занималось и занимается, большое количество практических и научных работников. К ним, можно отнести: Н.А.Зигура, Т.В.Аверьянова, Ю.Н.Батурин, А.В.Варданян, Б.В.Вехов, А.В.Вершинин, А.Г.Волеводз, Ю.В.Гаврилин, Н.А.Иванов, Д.Б.Игнатьева, В.В.Крылов, Л.Б.Краснова, В.А.Копылов, С.П.Кушниренко, Т.Э.Кукарникова, И.Н.Лукьянова, Н.Н.Лыткин, В.А.Мещеряков, В.А.Милашев, Э.М.Мурадьян, Е.В.Никитин, Е.П.Панфилова, Н.С.Полевой, Е.Р.Российская, А.В.Рыбин, С.И.Семилетов, А.В.Ткачев, А.А.Фатьянов, А.И.Усов, А.Н.Яковлев, Н.П.Цареву.

Цели и задачи исследования.

Целью магистерского диссертационного исследования является анализ понятия, свойств, видов, механизма формирования цифровых доказательств с помощью различных процессуальных действий. Нужно это для разработки предложений по совершенствованию норм уголовно-процессуального законодательства и правоприменительной практики по исследуемой тематике.

В целях достижения цели предлагаем решить следующие задачи:

- проследить эволюцию понятия цифровых доказательств на практике, в науке и законодательстве различных стран мира, в особенности ее использования в процессе доказывания с целью выявления преемственности процессуальной формы;

- выработать свое понятие цифровым доказательствам (ее материальных носителей) как нового вида (формы) доказательств, отвечающее требованиям, предъявляемым к доказательствам в судопроизводстве;

- исследовать и выявить природу доказательств, в т.ч. цифровых доказательств и других вещественных доказательств, сформулировать критерии их разграничения;

- проанализировать имеющиеся классификации доказательств, иных документов, электронных документов, машинных документов, аудио, фото-видео документов и на этой основе определить основания для классификации цифровых доказательств;

- проанализировать состояние правовых норм, регулирующих процесс сбора (выявления, получения и процессуального закрепления), проверки и оценки цифровых доказательств как разновидности вида доказательств и практику их применения для разработки предложений по совершенствованию процессуального законодательства по рассматриваемым нами вопросам.

Объектом магистерского диссертационного исследования выступает понятие цифровое доказательство, ее свойства, механизм формирования, способ внедрения в уголовный процесс как разновидностей доказательств и уголовно-процессуальные правоотношения, возникающие в процессе собирания, проверки и оценки цифровых доказательств.

Предметом магистерского диссертационного исследования является уголовно-процессуальное законодательство, регламентирующее понятие, признаки, виды доказательств, порядок их сбора, изъятия, приобщения к делу, проверки и оценки, при разрешении уголовного дела, а также практика применения этих норм, совокупность научных положений, характеризующих закономерности формирования цифровых доказательств.

Методологическую основу исследования составили всеобщий метод (диалектические метод научного познания), общие и частные научные методы: метод анализа и синтеза, системно-структурный, исторический, логический, сравнительно-правовой, социологический, статистический.

Теоретическая и нормативная основа исследования. В магистерской диссертации использованы труды по философии, теории познания, психологии, теории права, уголовному праву, гражданско-процессуальному праву, уголовно-процессуальному праву, криминалистике и судебной экспертизе, оперативно-розыскной деятельности.

Нормативной базой исследования стали: Конституция и иные правовые акты РК, нормы международного права, правовые акты зарубежных стран, регулирующие взаимоотношения в уголовном процессе.

Эмпирическую базу исследования образовали постановления Пленума ВС СССР и ВС РК. Автором изучена судебно-следственная практика РК и РФ, где в доказывании вины подсудимых применялись цифровые (электронные) доказательства, выявлены проблемы их доказывания.

Научная новизна исследования определяется целью, задачами и особенностями подхода к цифровой (компьютерной) информации в качестве самостоятельного вида доказательств. Нами сделана попытка исследовать цифровую информацию как самостоятельное доказательство в уголовном процессе. Предлагается внедрить новые понятия цифровых доказательств, цифровой (компьютерной) информации в уголовно-процессуальное законодательство и практические рекомендации о необходимости осмотра и изъятия цифровых информации специалистом.

О научной новизне свидетельствуют положения диссертационного исследования, выносимые на защиту:

- В целях единого толкования пониятии «цифровые (электронные) доказательства» и «цифровая (компьютерная) информация», предлагаем сформулированные нами данные дефиниции, дополнить п. 59) и п.60) ст.7 УПК РК, изложив их в следующей редакции:

а) п.59: цифровые (электронные) доказательства - сведения, полученные в соответствии с требованиями настоящего Кодекса, из показаний

участников уголовного процесса и иных лиц участвующих в нем, запечатленных на видео или аудио носителях, а также любые иные сведения, полученные путем считывания с электронных устройств, имеющее значение для правильного разрешения уголовного дела;

б) п.60: цифровая (компьютерная) информация - сведения, в электронно-цифровом формате, создаваемые различными техническими средствами и устройствами, программами фиксации, обработки и передачи информации.

- В связи, с целесообразностью выделения «цифровой (компьютерной) информации» в отдельный вид доказательства, предлагаем дополнить ч.3 ст. 111 УПК РК, изложив ее в следующей редакции: «Фактические данные, имеющие значение для правильного разрешения уголовного дела, устанавливаются: показаниями подозреваемого, обвиняемого, потерпевшего, свидетеля, свидетеля имеющего право на защиту, эксперта, специалиста; заключением эксперта, специалиста; вещественными доказательствами; протоколами процессуальных действий; цифровой (компьютерной) информацией и иными документами»;
- Достоверно установлено, что существует проблема сбора цифровых информации и их возможная утрата при изъятии, в виду отсутствия соответствующих специалистов. По этой причине, в целях выделения «цифровой (компьютерной) информации» в отдельный вид доказательства и сбора данного вида доказательств надлежащим образом, предлагаем дополнить главу 11 Доказательства УПК РК ст.120-1 «Цифровая (компьютерная) информация», изложив ее в следующей редакции:

Статья 120-1 «Цифровая (компьютерная) информация».

1. Цифровая (компьютерная) информация используются в качестве доказательств, если имеет значение для разрешения уголовного дела.
2. При обнаружении цифровой (компьютерной) информации имеющей значения для дела, ОУП принимают меры для их осмотра, выемки или копирования на электронный материальный носитель в целях сохранения и использования в качестве доказательств, о чем составляется протокол.
3. Осмотр, выемка и изъятие цифровой (компьютерной) информации производится с участием специалиста и понятых, с обязательной видео фиксацией происходящих событии, при этом выемка и копирование компьютерной информации осуществляется по правилам главы 31 настоящего Кодекса.
4. Изъятая цифровая (компьютерная) информация, вместе с протоколом приобщается к материалам уголовного дела и хранится до окончательного разрешения уголовного дела.

Теоретическая значимость исследования состоит в комплексном исследовании цифровой (компьютерной) информации в качестве самостоятельного вида доказательств в уголовном процессе РК, на основе научных положений уголовно-процессуального права и теории познания. Положения магистерской пополнят потенциал юридической науки.

Практическая значимость исследования состоит в том, что содержащиеся в ней положения, выводы и рекомендации могут быть использованы: 1) при совершенствовании уголовно-процессуального законодательства РК. В частности, нами предложены и сформированы новые нормы в УПК; 2) в практических рекомендациях правоохранительным и специальным органам; 3) при подготовке учебной и научной литературы, а также в учебном процессе. Практическое значение результатов магистерской работы выражается в возможности использовать в дальнейшем исследовании вопроса применения и доказывания цифровой (компьютерной) информации.

Апробация результатов исследования. Основные положения и выводы диссертации обсуждены на кафедре специальных юридических дисциплин Института послевузовского образования Академии правоохранительных органов при Генеральной прокуратуре РК; доложены на международных научно-практических конференциях: «Современные проблемы гуманитарных и социальных наук» Нур-Султан, 6.12.2019 г.; «Актуальные проблемы правотворчества и правоприменительной деятельности в РК», Костанай, 24.04.2020 г., которые в последующем опубликованы в печатных сборниках этих конференции.

Структура магистерской работы разработана с учетом цели и задач исследования. Диссертация состоит из обозначений и сокращений, введения, двух разделов, объединяющие шесть подразделов, заключения, списка использованной литературы.

1. Понятие и виды цифровых доказательств в уголовном процессе

1.1. Понятие цифровых доказательств в уголовном процессе

Прогресс открыл много возможностей для человека в различных сферах деятельности, он в настоящее время «научился летать», преодолевать большие расстояния за очень короткий срок, контролировать на расстоянии, что происходит дома и на работе, общаться, находясь в различных частях света, визуально видя друг друга и четко слыша. Помимо полезных функций для человечества, передовыми технологиями пользуются и криминальные элементы. Появились «новые» преступления, способствующие похищать денежные средства, находящиеся в банках, или информацию, имеющуюся на электронных носителях государственных учреждений, физических и юридических лиц. По этой причине, возникла нужда, в обладании новыми познаниями сотрудниками ОУП в целях выявления, изъятия, закрепления и оценки доказательств с различных технических носителей, таких как компьютер, ноутбук, нетбук, смартфон, фотоаппарат и т.д. Появились новые термины, такие как цифровое или электронное доказательство, электронный документ, электронно-цифровая подпись, электронные деньги и т.д. К сожалению, появление новых терминов не всегда раскрывает их, зачастую каждый толкует по своему, что влечет подмену понятия и не правильное восприятия обсуждаемых вещей.

Вот и сейчас, в уголовно-процессуальном законодательстве и теоретической науке РК отсутствуют понятия «цифровое доказательство» или «электронное доказательство», которые часто используются в научных трудах национальных и зарубежных ученых, практиков, а также в различных СМИ. К примеру, молодой казахстанский ученый Д. Утепов пишет «о сложности сбора и фиксации цифровых доказательств» [1], но, к нашему огорчению, в содержании не раскрывает самого понятия «цифровое доказательство». Он привязывает к термину «цифровое доказательство» другое понятие, как «электронная информация», оговаривая, что последнее «не может восприниматься человеком непосредственно визуально, аудиально и тактильно. Воспринимать ее можно только посредством технических аппаратов и предназначенных для этого специальных программ» [1], а в выводах отраженных в статье, выходец из прокурорской среды использует термин «компьютерная информация».

В противовес отраженной выше идее высказывается Московский адвокат С. Горбачев, отразив, что «Цифровые (электронные) доказательства - это новый вид доказательств, применяемый в арбитражном или ином процессе сравнительно не давно, и по своему внутреннему содержанию принимающий различную форму (электронного документа, аудио-видео запись какого-либо события). По этой причине, у

Суда и сторон, возникают вопросы, связанные с оценкой цифровых доказательств» [2].

Судья Алматинского районного суда №2 города Астаны А. Амингалиев на международном учебном семинаре на тему: «Получение и использование электронных доказательств, при расследовании и рассмотрении уголовных дел» сообщил, что «современный мир диктует свои условия, и ряд определенных технических средств, стал нужным инструментом в процессе доказывания вины или невиновности. В уголовно-процессуальном законодательстве нашей республики нет понятия «электронное доказательство», но в связи с развитием технологий традиционных способов раскрытия преступления оказывается недостаточно, они попросту не срабатывают. Поэтому такие преступления, как терроризм, убийство по найму, взяточничество, вымогательство, незаконное изготовление, приобретение, перевозка, пересылка наркотических средств, чисто следственным путем зачастую раскрыть не удается и требуется использование НТС. В последние годы видео- и фотосъемка стали основанием для соответствующего реагирования правоохранительных органов на нарушение общественной безопасности, начиная с административных нарушений и заканчивая особо тяжкими преступлениями. Примером служит акт самосожжения на городской площади в Таразе. На основании видеозаписи определенные лица привлечены к ответственности за неоказание помощи [3].

По мнению В.А. и Л.Ю. Новицких «как правило, аналогом цифрового доказательства именуют электронный документ, видео- и аудио информацию в цифровой форме, передаваемую суду на компакт дисках и флеш-картах» [4].

Существуют другие публикаций в научных изданиях, а также в СМИ, в т.ч. в Интернете, которые разделяют мнения вышеуказанных авторов, позиции которых не схожи, но оставить их без внимания нельзя и нужно разобраться какую позицию стоит выбрать или вообще выработать свою. В связи с этим, попытаемся разобраться, что означают термины «цифровое» и «электронное» доказательство, означают ли они одно и то же, либо это совсем разные вещи.

Доказательствами по уголовному делу являются законно полученные фактические данные, на основе которых в определенном УПК РК порядке, ОУП и/или суд устанавливают наличие либо отсутствие деяния, предусмотренного УК РК, совершение или не совершение этого деяния лицом, его виновность либо невиновность, а также иные обстоятельства, имеющие значение для правильного разрешения дела. В свою очередь, фактические данные, имеющие значение для правильного разрешения уголовного дела устанавливаются: показаниями подозреваемого, обвиняемого, потерпевшего, свидетеля, свидетеля имеющего право на защиту, эксперта, специалиста; заключением эксперта, специалиста;

вещественными доказательствами; протоколами процессуальных действий и иными документами (ст.111 УПК РК) [5]. Возникает вопрос, какие фактические данные могут быть цифровыми и/или электронными доказательствами, возможно ли отнести зафиксированные на аудио или видео показания лиц либо заключение экспертов к рассматриваемым нами видам доказательств.

Казалось бы, ст. 115, 116 и 117 УПК РК отражают, что показания допрашиваемых лиц никак нельзя отразить «цифровым» и/или «электронным» доказательством. Из имеющихся в главе 15 УПК РК «Доказательства», только ст.120 «Документы» кажутся, что имеют отношение к рассматриваемым нами видам доказательств. Так, ч.3. ст.120 УПК РК отражает, что «Документы могут содержать сведения, зафиксированные в письменной и иной форме. К документам относятся, в т.ч. объяснения, акты инвентаризаций, ревизий, справки, акты налоговых проверок, заключения органов налоговой службы, а также материалы, содержащие компьютерную информацию, фото- и киносъемки, звуко- и видеозаписи, полученные, истребованные или представленные в порядке, предусмотренном ст. 122 УПК» [5].

Наверное, по этой причине, А.П. Вершинин утверждает, что «электронные документы необходимо рассматривать в качестве письменных доказательств»[6], т.к законодательство РФ и РК частично схоже.

Вместе с тем, п.15 ст.7 УПК и пп.12 ст.1 ЗРК «Об электронном документе и электронной цифровой подписи» раскрывает понятие электронного документа как документа, в котором информация представлена в электронно-цифровой форме и удостоверена посредством электронной цифровой подписи [5, 7].

По этой причине, понятие электронный документ и цифровые и/или электронные доказательства по нашему мнению немного не сходятся.

С.Т. Фаткулин отметил, что «Электронный документ как источник доказательств в уголовном процессе можно определить как форму электронно-цифрового отображения информации, зафиксированную на материальном носителе, содержащую сведения о фактах, входящих в предмет доказывания по делу, имеющую установленные реквизиты, полученную с соблюдением требований уголовно-процессуального законодательства и предназначенную для хранения и дальнейшего использования.» [8]. Поэтому, мы более склонны к мнению С.Т. Фаткулина, чем к выводам вышеуказанных правовых актов РК, в связи с этим, считаем нужным доработать отраженные нами термины, а также закрепить в уголовно-процессуальном законодательстве понятия электронные или цифровые доказательства. При этом, нужно отметить, что в правовых актах РК и Международных правовых актах, ратифицированных нашим государством, понятие «электронных» или «цифровых» доказательств

отсутствует, что затрудняет правоприменительную практику и дает возможность различного рода научным дискуссиям.

В апреле 2014 г. в УК РК впервые включаются преступления в области компьютерной информации, появляется новая глава 7-1 «Преступления против безопасности информационных технологий». В июле того же года принимается УК в новой редакции, где присутствует глава 7 «Уголовные правонарушения в сфере информатизации и связи». На данный момент приняты разные изменения и дополнения в этой главе, появляются новые составы уголовных правонарушений, однако, практика расследования и рассмотрения уголовных дел этой категории еще только формируется.

Вместе с тем, значение компьютерной (цифровой) криминалистической информации для выявления и предупреждения преступлений трудно переоценить. В СССР одним из первых вопросов об использовании компьютерной информации (электронных документов), как доказательства в рамках уголовных дел, предложено В.К. Лисиченко, в докторской диссертации «Криминалистическое исследование документов (правовые и методологические проблемы)». Им сделан вывод, что «широкое внедрение вычислительной техники в сферу хозяйства и управления «создает объективные основания для того, чтобы сведения о фактах и практической деятельности людей, закрепленные знаками искусственных языковых систем (машинных языков), рассматривались в общенаучном и правовом смысле, как самостоятельная разновидность документов» [9]. К сожалению, таких фундаментальных работ в настоящее время в Казахстане нет.

Регулирование места и значения цифровой информации в уголовном судопроизводстве и криминалистике актуально и требуют незамедлительного решения. В целях создания правовой основы более широкого применения в судопроизводстве цифровой (компьютерной) информации, нужно определить границы данного понятия и его правовой режим. В науке и правовых актах для обозначения компьютерной информации используются различные термины: «цифровая информация», «бинарный след», «документ, подготовленный с помощью электронно-вычислительной техники», «электронные ресурсы», «электронные доказательства», «цифровые доказательства», «электронный документ», «электронная информация», «электронный билет», «электронная почта», «электронная площадка», «машинный документ», «виртуальный документ», «электронное сообщение», «компьютерно-технический след», «компьютерная информация», «электронное средство платежа» и т.д. В нашей диссертации некоторые эти термины будут использованы, в целях анализа цифровых (электронных) доказательств. Думаем, что многие правоприминители и люди науки согласятся, что становиться очевидным, применение законодателем в правовых актах вышеперечисленных терминов нуждается во всестороннем научно-правовом анализе. Итогом

чего должны стать предложения по совершенствованию правовых актов РК в данной сфере, ибо правоприминитель не всегда адекватно воспринимает до конца не продуманные и научно необоснованные новеллы в законах.

Также в стороне от научного поиска оптимальных правовых решений проблем, не может оставаться наука уголовно-процессуального права от исследования вопросов, связанных с цифровой реальностью. При этом, в рассматриваемой нами науке уголовно-процессуального права одним из основных правовых институтов без сомнения является доказательственное право. Вносимые изменения и дополнения в УПК РК, появляющиеся публикации по данному вопросу, ставят перед наукой целесообразность трансформации норм доказательственного права ввиду появления и широкого распространения на практике новых источников доказательственной информации, имеющих электронную (цифровую) природу. Дискуссии разворачиваются вокруг таких понятий, как «электронные доказательства», «цифровые доказательства», «электронное доказывание», «компьютерная информация». Спектр мнений довольно широк, что показывает о сложности и многоаспектности рассматриваемых явлений новой реальности.

Н.А. Зигура разработала свое понятие «компьютерная информация» - как сведения, представленные в электронно-цифровой форме на материальном носителе, создаваемые посредством использования аппаратных и программных средств фиксации, обработки и передачи информации, а также набор команд (программ), предназначенных для использования в электронно-вычислительной машине, системе ЭВМ или управления ими, на основе которых суд, руководитель следственного органа, следователь, дознаватель устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела, полученные с соблюдением процессуального порядка их собирания и приобщенные к уголовному делу специальным постановлением» [10].

Другого раскрытия термина «компьютерная информация» в научной литературе нами не обнаружено, несмотря на его широкое применение среди специалистов разных областей знаний. По сути данное Н.А. Зигура понятие в своем роде частично раскрывает термин «цифровое доказательство», но оно очень сложное для восприятия и требует доработки, в целях единообразного понимания исследуемого нами объекта. Хотелось обратить внимание, что определение предложено ею в 2010 г., но поскольку технический прогресс не стоит на месте, можно сказать о возможном старении понятия за 10 лет, например термин ЭВМ уже практически не используется.

Возможно, сведения о «компьютерной информации» есть в закрытых источниках, но, к нашему сожалению, их мы не можем исследовать и осветить. Почему нами выбран термин «цифровые доказательства», потому

как в науке оно используется очень активно, но в правовых актах используется и/или раскрываются отдельные его части. К примеру, ст. 272 УК РФ [11], дает следующее определение - компьютерная информация это информация на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, а в ч. 8 ст. 166 УПК РФ используется термин «носитель компьютерной информации» [12].

В уголовном законодательстве РК не раскрывается понятие компьютерная информация, хотя как нами же отмечено, в нем существует целая глава «Уголовные правонарушения в сфере информатизации и связи» [13], а в УПК раскрывается термин «электронный документ», в ст.120 УПК упоминается о материалах, содержащих цифровую информацию, фото- и киносъемки, звуко- и видеозаписи.

Между тем, в п.«б» ст. 1 Соглашения «О сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации» компьютерная информация была определена «как информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи» [14]. По этой причине, правоприминитель в Казахстане может смело ссылаться на эту норму, используя в предмете доказывания в уголовном, административном и гражданском процессе.

Другим из вопросов вызывающим широкую полемику, связано с целесообразностью и обоснованностью отражения в правовых актах нового вида доказательства - «электронного» или «цифрового» доказательства. Несмотря на распространенное в СМИ, научной литературе и практике употребление термина «цифрового либо электронного доказательства», находятся специалисты, отрицательно высказывающиеся в выделении такого вида доказательства и закрепления его в УПК.

Р.И. Оконенко в диссертационном исследовании об электронных доказательствах, сделал вывод, что «в настоящее время преждевременно говорить о понятии «электронного доказательства» как о состоявшейся категории позитивного права. Появление в УПК РФ термина «электронный носитель информации» следует рассматривать как промежуточный шаг на пути к возможному появлению в процессуальном праве, термина «электронные доказательства» [15]. По его же мнению, электронные доказательства не являются особым видом доказательств.

Возможно для научной среды России и развития ее законодательства появление терминов «электронное» либо «цифровое» доказательство преждевременно, но говорить об этом в научной среде Казахстана или решать вопрос о внедрении в правовые акты должны ученые из нашей страны, т.к. наши правовые системы развиваются самостоятельно.

С. В. Зуева и другие авторы коллективной монографии «Основы теории электронных доказательств», соглашаясь, с автором англоязычной статьи в сети Интернет считают, что электронным доказательством является

любая электронное хранимая информация (ESI), которая может быть использована в качестве доказательства в судебном процессе; к такому виду доказательств относятся любые документы, электронные письма или другие файлы, хранящиеся в электронном виде, а также электронные свидетельства, включающие записи, хранящиеся сетевыми или интернет-провайдерами. В этой же работе утверждается, что электронная информация может быть представлена в виде одного из традиционных доказательств - вещественного доказательства или иного документа [16]. Немного схоже с мнением Р.И. Оконенко, с незначительными своими выводами и особенностями, позиция П.С. Пастухова, который полагает, что «в УПК РФ не следует вводить новый вид доказательства («электронное доказательство») или новый источник («электронный носитель информации»), нужно лишь уточнить понятие «доказательство». Отразив о возможности сведении принимать вид электронной информации, которую, «вполне способны восприниматься в одном из традиционных видов доказательств - вещественном или ином документе» [17].

Проникнув мыслью П.С. Пастухова можно понять, что оно далеко не ново для науки, поскольку на территории бывшего СССР вопрос о целесообразности правового регулирования использования электронного документа и новых технологий отдельными авторами поднимался еще в 70-х годах XX века. Они, отражая на особый вид правовой природы документов, полученных с использованием техники, рассматривали их, как «особую разновидность письменных доказательств». В результате сопоставления «машинных»- и «бумажных» документов, с учетом, действия на них единого правового режима, они считали достаточным внести незначительные изменения в правовые акты, таких как признание за машинными документами силы «обычного» письменного доказательства [18].

К сожалению, мы не можем привести примеры позиции казахстанских авторов по рассматриваемому вопросу, т.к. для нашей страны, несмотря на использования всех ранее отраженных терминов, отсутствуют научные работы по уточнению и использованию терминов «электронное доказательство», «цифровое доказательство», «компьютерная информация» и т.д. Возможно, для нас это лучший из способов разработать новую доктрину в науке Казахстана, к которой будут прислушиваться не только национальные ученные, но и зарубежные ученные, соглашаясь или ставя противовес свою точку зрения, тем самым еще больше развивая дискуссию вокруг изучаемого нами вопроса. Нельзя забывать, что ссылка на научные источники Российских ученных, развивает сравнительно-правовой анализ законодательства и предусматривает исторически анализ права, т.к. всего каких-то 30 лет назад мы имели одну единую правовую систему права.

Так, в СССР первым правовым актом, регулирующим вопросы использования документов, подготовленных с помощью компьютерной техники, в судебных разбирательствах были Инструктивные указания

Государственного арбитража СССР от 29.06.1979 г. № И-1-4 (далее - Указания). Они не предусматривали возможность использования в арбитражном процессе непосредственно самих электронных документов, а лишь регулировали правовое положение их бумажных копий. Обращаем внимание, что согласно Указаниям стороны могли представлять арбитражу любой экземпляр документа, подготовленного с помощью электронно-вычислительной техники. Если же для разрешения спора требовался подлинник документа, арбитражу нужно было представить первый экземпляр. Поскольку разъяснений по этому поводу не остались, нет ясности, как стороны доказывали, что предоставляют первый экземпляр копии, но осмелимся предположить, что во избежание неясностей, изначально при распечатке электронные документы нумеровались как того требует документация с грифом «секретно» в государственных учреждениях. В 1984 г. разработан и внедрен ГОСТ 6.10.4-84 «Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники» [19]. В них установлены требования к составу и содержанию реквизитов, придающих юридическую силу документам на машинном носителе, создаваемым первыми компьютерами, а также порядок внесения изменений в эти документы. В то время еще не шел вопрос о сетевом обмене информации, основной целью, ГОСТ преследовал печать на машинах различного рода отчетов, статистических сводок, обобщавшихся в основном вышестоящими и контролирующими организациями. К этому времени каждое министерство и/или крупное предприятие имело свои вычислительные центры, работавшие на стационарных электронно-вычислительных машинах серии «ЕС», созданных на условиях кооперации со странами Восточной Европы, входившими в СЭВ. Естественно, что таким официальным отчетам и статистическим сведениям было нужно придать юридическую силу, равную обычным бумажным документам. Дублирование информации путем параллельного направления распечаток, сопровождалось неоправданными затратами. По этой причине разработчики ГОСТ применили способ формирования некоторого перечня обязательных реквизитов, нужных для отражения в текстах, представленных в электронной форме, либо в ином доступном ЭВМ коде (телеграфном коде на перфоленте). Информация направлялась сопроводительным письмом, оформленный как обычный исполнительно-распорядительный документ, что придавало электронным документам юридическую силу, как выполненную на бумажном носителе. В этот же период в оборот пришел термин «машинограмма», т.е. распечатка документа в доступной для восприятия человеком форме, признаваемой копией документа, помимо обязательных реквизитов, содержащий штамп (печать) организации, преобразовавшей документ в данную форму, удостоверительную надпись и соответствующие подписи.

Как мы видим, электронный документ оформлялся как обычный бумажный документ.

А.Н. Яковлев отмечает, что «адекватная реакция законодателя на изменения методов и способов сбора, накопления, хранения, поиска и обработки информации, связанные с применением средств вычислительной техники, коснулась формирования правового статуса документа распечатанного на бумаге, подготовленного на электронно-вычислительной технике и самих документах хранящихся на машинных носителях информации» [20].

Позднее нашла признание точка зрения, согласно которой проблема использования «электронных документов» должна получить комплексное регулирование [21].

9.07.1982 г. Пленум ВС СССР принял постановлении № 7 «О судебном решении», в котором закреплялось, что в обоснование решения суд в случае необходимости вправе сослаться и на письменные доказательства в виде документов, полученных с помощью электронно-вычислительной техники. Такие документы принимаются в качестве доказательств, при условии их надлежащего оформления в соответствии с установленным порядком [22]. Как мы видим, отраженное постановление прямо предусматривало, что «электронные документы» отнесены к письменным доказательствам. Пленум ВС СССР в постановлении «О строгом соблюдении процессуального законодательства при осуществлении правосудия по гражданским делам» дал более широкое разъяснение: «В случае необходимости судом могут быть приняты в качестве письменных доказательств документы, полученные с помощью электронно-вычислительной техники. Такие материалы оцениваются в совокупности с другими доказательствами» [23].

На сегодня под компьютерной информацией подразумевается не просто текст, отпечатанный на компьютере, когда ЭВМ использовалась как аналог печатной машинки, а гораздо более разнообразная цифровая информация. В них входят данные, создаваемые автоматически, без участия человека, использование телекоммуникационных средств, для сетевого обмена сведениями. Первоначально в Казахстане сетевой обмен информацией в государственных учреждениях использовался через электронную почту, затем созданы – Единая система электронного документооборота (ЕСЭДО), Информационная система электронного документообарота органов прокуратуры (ИС Қадағалау). Переписка между физическими, юридическими лицами и госорганами может производиться без бумажного документа оборота, через «Электронное Правительство» (egov.kz), откуда можно обращается практически по всем вопросам во все госорганы. Отслеживать ход судебных рассмотрений по гражданским и уголовным делам, а также по делам об административном судопроизводстве можно через судебный кабинет (office.sud.kz), а уже окончательное исполнение, кроме наказаний уголовного правового характера можно в

«Автоматизированной информационной системе органов исполнительного производства Министерства юстиции РК (aisoip.adilet.gov.kz).

Теперь нет нужды приобретать печатный вариант правовых актов РК, т.к. они публикуются в Информационно-правовой системе нормативных правовых актов РК «Әділет».

Современные технология применяются в Казахстане во всех видах судопроизводства, протоколы судебного заседания производятся в форме аудио-видео фиксации, которые приобщаются к материалам гражданских и уголовных дел, а также к делам об административном судопроизводстве.

Считается, что протокол один из основных процессуальных документов, требование к его бумажному носителю высокое, в части полноты и правильному отражению в нем информации.

Н.А. Зигура в своем диссертационном исследовании полагает, что «видеозапись обеспечивает наиболее информативные протоколы судебных заседаний, только она способна в полной мере отразить все события в судебном зале, включая психологическое состояние присутствующих, их поведение в определяющие моменты судебного разбирательства [10]. С этим можно согласиться, если видео протокол зафиксировал абсолютно все события, происходящие в период судебного заседания, без помех в эфире и искажения изображении. По этому, нужно, чтобы техника, воспроизводящая аудио-видео запись работала отлажено, секретарь судебного заседания отслеживал за этим. Но, к сожалению, любой технике свойственно ломаться, вследствие чего протокол судебного заседания как доказательство может быть утеряно в последующем и позволить апеллировать стороны на нарушения, допущенные в ходе проведения предварительного слушания, главного судебного разбирательства, на досудебной стадии процессуальные действия, проведенные следственным судьей.

Несомненно, использование рабочих технических средств, способствует открытости и ускоряет процесс судопроизводства, повышает количества законных принимаемых судебных актов. На сегодня можно смело отметить, что практически все суды оснащены нужной техникой, Интернетом, что позволяет взаимодействовать между участниками, находящимися в зале суда, с другими удаленными участниками уголовного, гражданского и административного процесса. Функционирование этой системы обеспечивает оборудование в зале суда видео конференцсвязи, взаимосвязанной с системой звукозаписи и озвучивания зала, судебных заседании.

Нужно обратить внимание, что применяя возможности технических средств оснащенных в судах РК можно обеспечить меры безопасности лиц участвующих в уголовном процессе, опосающихся за жизнь и здоровье. Применение технических средств предоставляет возможность контакта на судебном процессе без визуального наблюдения или изменения голоса, как того допускают нормы главы 12 УПК РК.

В начале 2018 г. в УПК РК внесены изменения и дополнения, внедрены такие понятия как: «Единый реестр досудебных расследований», «модуль «Электронное уголовное дело», «электронное уголовное дело», «электронная цифровая подпись», «медиа-файлы», «планшет подписи» и т.д. [24].

Приказом Генерального прокурора РК от 3.01.2018 г. №2, утверждена Инструкция о ведении уголовного судопроизводства в электронном формате, которая регламентирует порядок проведения досудебного расследования в электронном формате.

В РК при развитии информационного общества бумажный документооборот уменьшается, предоставляя возможность электронного взаимодействия без прямого контакта между людьми, что в свою очередь снижает коррупционные факторы. Документы создаются на основе жестких детерминированных алгоритмов программ, люди перестают формировать документы, ограничиваясь разработкой правил формирования и преобразования электронного документа. Прогресс, будь то научный, технический, технологический протекает очень быстро, от этого сознание большинства масс людей не успевает воспринимать происходящие изменения. Нет сомнений, что у большинства людей доминирует поверхностный подход к «электронному взаимодействию» и «электронному документу», т.к. они немного отступают от бумажного информационного взаимодействия. По этой причине, попробуем раскрыть понятия «электронное взаимодействие», «электронное доказательства», «цифровое доказательства» и по мере возникновения новых терминов касательно нашей темы и их содержание.

Как мы уже ранеем отметили, в правовых актах РК дефиниции указанных выше терминов не раскрываются, но есть отдельные разъясняющие моменты. К примеру, в Правилах оптимизации и автоматизации государственных услуг, отражена цель упрощения и ускорение процесса, оказания государственных услуг, оказываемых госорганами, в т.ч. путем взаимодействия услугополучателей с должностными лицами госорганов по принципу «одного окна» с использованием информационно-коммуникационных технологий без личной явки услугополучателя в госорганы [25]. Несмотря на то, что указанная цель не раскрывает понятие электронное взаимодействие, оно объясняет принцип взаимодействия госорганов с их услугополучателем путем передачи информации через технические электронные устройства, в каком-то роде объясняя, как проходит процесс обмена информацией.

В ЗРК «О почте» раскрыты понятия «гибридное отправление», «электронный абонентский почтовый ящик» и «электронное письмо». Термины, указанные в этом ЗРК в своем содержании отражают возможность передачи данных от адресата к адресату, отражая, что электронные почтовые ящики регистрируются в официальных

организациях почтовой связи, указывая, что mail.ru или gmail не подходят к их требованиям.

Под гибридным отправлением – электронного письма (сообщения), понимается принятое оператором почты к пересылке и доставляемое адресату в виде письма (почтовой карточки), либо письмо (почтовая карточка), принятое оператором почты к пересылке и доставляемое адресату в форме электронного письма (сообщения) на электронную почту или электронный абонентский почтовый ящик.

В свою очередь, электронный абонентский почтовый ящик – это доменное имя пользователя услуг оператора почты, создаваемое в информационной системе Национального оператора почты или оператора почты для приема и доставки электронных писем (сообщений) и документов.

Тогда как, электронное письмо (сообщение) – это информация, пересылаемая в электронной форме с использованием сети телекоммуникаций, интернета или электронных носителей [26].

В России данный термин звучит немного иначе. Согласно п.10 ст.2 ФЗ «Об информации, информационных технологиях и о защите информации»: электронное сообщение - это информация, переданная или полученная пользователем информационно-телекоммуникационной сети [27].

И.Н. Лукьянова, утверждает, что понятие электронного сообщения, очевидно, включает в себя термин электронного документа, т.к. документом признается информация (сообщение), оформленная в соответствии с определенными требованиями [28]. Данная позиция подходит к п.11.1 ст.2 ФЗ РФ «Об информации, информационных технологиях и о защите информации». В нем отражено, что электронный документ это документированная информация, представленная в электронной форме, т.е. в виде, пригодном для восприятия человеком с использованием ЭВМ, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Однако, позиция И.Н. Лукьяновой и вышеуказанного ФЗ, идет немного в разрез с ФЗ РФ «Об электронной подписи» [29], т.к. для признания электронным документом переданных данных через информационно-коммуникационные сети, нужно обязательное удостоверение электронной цифровой подписью, причем, такие требования отражены и в РК [5, 7]. В правовых актах РК есть понятия «электронного документа», «бумажная копия электронного документа», «электронный документооборот», «подлинник электронного документа» [30], то дефиниции к самому слову «документ» отсутствует, что является довольно странным на наш взгляд.

Между тем, п.28-1 ст.3 УК РК раскрывает термин «официальный документ» – документ, созданный физическим или юридическим лицом, оформленный и удостоверенный в порядке, установленном законодательством РК. Полагаем, что это в свою очередь компенсирует

отсутствие в законодательстве РК простого понятия «документ» и уже разграничивает возможность его классификации и признаков [13].

Теперь ясно, что у документа должен быть автор, в виде юридического и физического лица, а также документ должен соответствовать определенным требованиям, а учитывая, что документы бывают разные. К каждому виду документа выдвигаются свои требования в соответствии с действующими законодательными актами РК. К примеру, паспорт гражданина это официальный документ, созданный каким либо юридическим лицом, по заказу государства и отражает в себе все требования, которые предусматривает ЗРК «О документах, удостоверяющих личность».

В Соглашении о свободном доступе и порядке обмена открытой научно-технической информацией государств-участников СНГ и Концепция формирования информационного пространства СНГ отражено, что «документированная информация (документ) – это зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать» [31, 32].

Пункт 4 ст.1 ЗРК «О государственной правовой статистике и специальных учетах» предусматривает другое толкование «документированной информации». Согласно, ей «документированная информация – это сведения о лицах, предметах, фактах, событиях, обстоятельствах и других правовых явлениях и процессах, происходящих в уголовно-правовой, гражданско-правовой, административно-правовой сферах, независимо от формы их представления, зафиксированные в информационном учетном документе» [33].

Анализ правовых актов не дает точно понять, является ли понятие «документированная информация» равнозначным понятием к термину «документ». Судя по правовым актам, у нас есть три формы с разными содержаниями раскрывающие термин «документ».

Если отбросить в сторону дефиницию «официальный документ», т.к. в природе документ может быть и не официальным, то в одном случае документ это материальный объект с зафиксированной на нем информацией, а во втором случае это информация, зафиксированная на материальном носителе. Несмотря на текстуальную близость формулировок, суть их разная.

Нельзя оставлять в стороне термин «официальный документ», т.к. не всегда не официальный документ имеет силу, на нем нет определенных реквизитов, требуемые действующим законодательством РК, т.е. по логике вещей они могут не браться во внимание. К примеру, если лицо, пишет предсмертную записку, а после совершает самоубийство, этот не официальный документ берется во внимание при принятии процессуального решения в виде прекращения уголовного дела.

В.Б. Вехова, отмечает, что «Определение документа - доказательства как материального носителя, содержащего сведения, представляется в корне неправильным. Оно противоречит действующему уголовно-процессуальному законодательству: «доказательствами по уголовному делу являются любые сведения, на основе которых суд, прокурор, следователь, дознаватель в определенном УПК порядке устанавливает наличие или отсутствие обстоятельств, имеющих значение для уголовного дела» [34].

Фактически противоречие в терминологии затрудняет в практике использование отдельных дефиниций. По этой причине, предлагаем свою версию термина «цифрового (электронного) доказательства», которой дополнить п. 59 ст. 7 УПК РК. Раскрывая этот термин, как - сведения, полученные в соответствии с требованиями настоящего Кодекса, из показаний участников уголовного процесса и иных лиц участвующих в нем, запечатленных на видео или аудио носителях, а также любые иные сведения, полученные путем считывания с электронных устройств, имеющее значение для правильного разрешения уголовного дела [35].

Несмотря на то, что многие считают, что вопрос на законодательном уровне понятии «цифровые или электронные доказательства», «цифровые (компьютерная) информация» принимать еще рано, думаем, настало время для их закрепления как самостоятельных доказательств в уголовном процессе.

Нужно детально регламентировать вопросы, связанные с правовым режимом цифровой - компьютерной информации, выделив ее как самостоятельный вид доказательства, расширив список видов доказательств, в ч.2 ст.111 УПК РК, дополнив их цифровой (компьютерной) информацией.

В целях внедрения в уголовный процесс понятии «цифровое доказательство», «цифровой (компьютерной) информации, как самостоятельного вида доказательств», нужно:

- разработать определение «цифровых доказательств» и «цифровой (компьютерной) информации». Нужно отметить, что компьютерная информация, это одна из составных частей «цифровых» и/или электронных доказательств, которая фиксируется на техническом устройстве. При этом, мы уже предложили свою версию «цифрового (электронного) доказательства», теперь же предлагаем раскрыть понятие «цифровой (компьютерной) информации», в п.60 ст.7 УПК РК:

- цифровая (компьютерная) информация - сведения, в электронно-цифровом формате, создаваемые различными техническими средствами и устройствами, программами фиксации, обработки и передачи информации.

Так как, в УПК РК будет раскрыта цифровой (компьютерной) информации, предлагаем свои вариант ч.2 ст.111 УПК РК в следующей редакции: «Фактические данные, имеющие значение для правильного разрешения уголовного дела, устанавливаются: показаниями подозреваемого, обвиняемого, потерпевшего, свидетеля, свидетеля

имеющего право на защиту, эксперта, специалиста; заключением эксперта, специалиста; вещественными доказательствами; протоколами процессуальных действий; цифровой (компьютерной) информацией и иными документами».

Таким образом, точное определение этих терминов позволит на практике и в науке отграничить цифровую информацию от иных документов и вещественных доказательств, что решит процессуальный режим цифровой информации, добываемых ОУП, приобщаемых и предъявляемых сторонами на досудебной и судебной стадии уговорного процесса.

1.2. Разграничение цифровой информации от вещественных доказательств и иных документов

Процесс эволюции вычислительной техники оказался настолько стремительным, что восприятие различия традиционного (бумажного) и электронного документа, созданного с помощью вычислительной техники, вызывает определенные трудности. Молодое поколение уже не может воспринимать, что документ может быть написан (напечатан) на бумаге без использования компьютерных программ, т.е. с использованием обычной шариковой ручки либо печатной машинке, а исправление ошибок нужно будет перепечатывать или переписывать вновь. Такое положение вещей кажется непосильным трудом. Существующая концепция аналогии традиционного и электронного документа мешает полноценно использовать последний вид в качестве цифровых доказательств. В целях выделения цифровых (электронных) доказательств в самостоятельный вид, нужно отграничить цифровую (компьютерную) информацию от иных документов. Для этого нужно учесть совокупность разграничивающих признаков. Познанию сущности доказательств, служит установление механизма их формирования, в т.ч. закономерности следообразования и процессуальные условия их собирания.

Для начала нужно понять, каким образом формируются документы и что к ним относится. В соответствии с ч.3 ст.120 УПК РК документы могут содержать сведения, зафиксированные как в письменной, так и иной форме. УПК к ним относит: объяснения, акты инвентаризаций, ревизий, справки, акты налоговых проверок, заключения органов налоговой службы, а также материалы, содержащие компьютерную информацию, фото- и киносъемки, звуко- и видеозаписи, полученные, истребованные или представленные в порядке, предусмотренном ст.122 УПК [5].

Обратим внимание, что письменные документы, отраженные в УПК это своего рода документы, изготовленные не в процессе процессуальной деятельности, доказательствами они становятся, в случае содержания в них сведении имеющих значение для уголовного дела, изъятые и приобщенные к делу согласно требованиям уголовно-процессуального закона. К ним

относятся печатные и рукописные письменные документы. К примеру, записная книжка, в содержании которой отражены номера телефонов, лиц, скупающих краденые вещи. Доказательствами могут выступать официальные документы (справки, акты и т.д.) и неофициальные (личные письма, записные книжки и т.п.). Документы бывают первоначальными (подлинники) и производными (копии).

УПК РК, гласит, что информация может содержаться не только на бумаге, она фиксируются на фото- и киносъемки, аудио- и видеозаписи и другие носители информации. Причем, позиция ч.2 ст.100 УПК Беларуси, ч.2 ст.84 УПК РФ и ч.2 ст.99 УПК Украины такая же, за исключением того, что Украина отразила о возможности этих доказательств в электронном виде [5, 36, 11, 37]. Наше диссертационное исследование интересует больше именно эта часть документов, ее фиксация и возможность сохранения, изменения, изъятие и т.д. Обязательным требованием к признанию документа в качестве доказательств, служит наличие источника - автор или исполнитель. В особенности если это личные документы, не содержащие подписи и указания автора. В указанном случае должны быть допрошены лица, которые смогут указать на автора, в случае возникновения необходимости должна производиться почерковедческая либо автороведческая экспертиза, а применительно к голосу или иным видам фонограммам - фоноскопическая. Правовое положение этого источника доказательства определяется компетенцией автора документа, ограниченное пределами исполняемых им функций. Официальный характер документы носят, когда исходят от госорганов или иных организаций.

Очень важно выяснить, кто автор электронного документа, при этом, по нашему мнению исходя из требований ч.3 ст.120 УПК РК электронный документ может быть напечатанным, снятым на цифровой фотоаппарат, видеокамеру, мобильный телефон, планшет и т.д., а затем перемещен в компьютер и хранится там, в виде цифровой информации.

Н.А. Полевой в целях выяснения подлинной природы информации и сущности информационных процессов, лежащих в основе познания события преступления, разграничил термины «отражение» и «отображение». Сделал вывод, что «информация может восприниматься познающим субъектом или техническим устройством, она «как бы «отделена» от ее первоисточника - отображения источника объекта познания»; она может «переносится в пространстве, сохранятся во времени, передаваться другому субъекту или техническому устройству, таких как ЭВМ, подвергнута другим операциям, совокупность которых именуется информационными процессами» [38].

Т.В. Аверьянова решая вопрос об отличии термина «информация» в криминалистике от этого понятия в других науках, отражает, что «мы имеем дело с двумя видами (не определенными терминологически) информации. С одной стороны, это объем знаний, хранящийся, транслируемый, обрабатываемый на компьютере. С другой, это информация собственно

«компьютерная, значимая для криминалистики», т.е. материальные и виртуальные следы, отображаемые движущейся в компьютере информацией первого вида. Как мы видим, достаточно понять, что след в компьютере просто приобретает иную форму, чем обыденной жизни» [39].

В.А. Гадасин и В.А. Конявский отражают, что «Кардинальное отличие электронного и аналогового документов заключается в их предназначенности для функционирования в разных средах существования: электронной, среде программных и технических средств вычислительной техники; аналоговой, среде мыслящих объектов, людей. Отличие традиционного и электронного документов в том, что первый предназначен для обработки мыслящими субъектами, т.е. людьми, второй для обработки техническими объектами, аппаратными и программными средствами» [40].

Цифровая информация создается алгоритмом, заданной программы, находящаяся в разных технических устройствах, таких как компьютер, ноутбук, нетбук, смартфон, цифровой фотоаппарат либо видеокамерой и т.д. Сами программы в этих устройствах продукт созданный человеком. Техника сегодня еще не умеет мыслить, она преобразовывает выданное различным способом множество сигналов на основе однозначно заданной последовательности фиксированных операций. Процесс обработки данных осуществляется техническими средствами (программами), можно утверждать, что возникновение и получение (восприятия) информации через «интеллектуальное сознание» человека. При создании цифрового документа на техническом устройстве реализуется априорно заложенная программа формирования электронного документа. Механизм формирования «иного» документа и компьютерной информации не идентичен.

Проблема носителя информации чрезвычайно многопланова и может рассматриваться в различных аспектах: технологическом, историческом, философском, юридическом и тому подобное [41]. В уголовном судопроизводстве документ это материальный носитель информации, на нем один из участников уголовного процесса зафиксировал в установленном порядке сведения об обстоятельствах, имевших значение для дела, в письменной, фото-видео или иной форме в целях их сохранения и последующего использования.

Неотъемлемой характеристикой документа служит способность долговременного хранения и передачи информации во времени и пространстве, а основное функциональное назначение связано с процессом ее фиксации на материальном носителе в целях предъявления на обозрение. В свою очередь, материальные носители информации и способы фиксации могут быть разнообразными, самое важное это способность долговременного хранения информации, а фиксация производилась с соблюдением порядка, соответствующего функциональному назначению каждого документа в отдельности. Это обеспечивает степень защиты документа от возможных подделок путем дополнения или изменения

отдельной ее части, выявляемых при визуальном осмотре и оценки имеющихся ее реквизитов.

Отличие электронного документа заключается в отсутствии жесткой привязки к носителю, т.е. он может находиться на разных электронных носителях. К примеру, на жестком диске компьютера, в виде электромагнитных волн, в период передачи этого файла определенному адресату, но это не мешает ему оставаться аутентичным. Особенности цифровой технологии позволяет быстро и много раз копировать, а затем передавать документ по электронным каналам связи, а также использование одновременно неограниченного числа пользователей.

Иным существенным отличием компьютерной информации служит отсутствие возможности непосредственно и однозначно воспринимать информацию органами чувств человека, как об этом указывал Д. Утепов [1].

Обусловлено это тем, что существующая информация отображается в электронно-цифровой форме, несмотря на то, что она находится на материальном носителе, само наличие цифровой информации, и ее местоположение на этом носителе без соответствующих программ невозможно определить. Люди воспринимают цифровой документ как именованный файл с отдельными известными атрибутами, ее запись находится в определенном известном автору или пользователю виртуальном месте, в системе отдельных программ.

В.А. Гадасин и В.А. Конявский, рассматривая системные основы отличия письменного (аналогового) и электронного документа и ссылаясь на «кардинальное различие физической среды существования документа», утверждают, что традиционный документ есть аналоговое отображение информации, закрепленное на твердом носителе и рассчитанное на непосредственное восприятие субъектом. Человек, обладая знаниями, способен к восприятию, графического представления информации, ее «пониманию» и обработке на основе мышления. Базой восприятия является органически присущий человеку мощнейший аппарат распознавания образов, позволяющий ему отождествлять компоненты документа со сформированными в сознании эталонами. Электронный документ есть цифровое отображение информации, ее носителем служат средства вычислительной техники и информатики. Только объект электронной среды может обрабатывать электронный документ: выполнять априорно заданное детерминированное преобразование входного электронного документа в выходной электронный документ и существует только в электронной (цифровой) среде существования [40].

Более сложно разграничить цифровую (компьютерную) информацию и вещественные доказательства, т.к. ст. 118 УПК РК отражает похожие признаки компьютерной информации. Основным признаком вещественных доказательств, служит их объективная связь с исследуемым событием, в силу которой они и могут являться средствами установления фактических

обстоятельств дела. Такой признак вполне можно отнести к компьютерной информации, поскольку она может служить орудием преступления, таких как: программа, содержащая в себе вредоносный вирус; сохранять на себе следы преступления, в виде попыток несанкционированного доступа; объектом преступления, в виде перевода денежных средств со счетов.

По этой причине, нужно наитии различия, существующие между вещественными доказательствами и цифровой информацией, хотя многие процессуалисты к первым относят только предметы.

По мнению А.А. Эйсман: «вещественное доказательство представляет собой предмет, несущий элементарное отображение (информацию) тех событий, фактов, явлений, в ходе которых этот предмет принимал непосредственное участие, в качестве орудия либо иным средством совершения преступления, объекта преступного посягательства и т.д.» [42, с.144]. Б.Т. Безлепкин отмечает, что «вещественными доказательствами могут быть такие предметы, доступные обычному восприятию, которые используются публично при доказывании в суде, передавая из рук в руки для возможного осмотра [43, с.136].

Некоторые ученые предлагают компьютерную информацию рассматривать в качестве вещественного доказательства, в обоснование, отражая, что «носителем этой информации является предмет, а доказательственное значение имеет ее содержание» [44, с.51]. Нет сомнения, что цифровая (компьютерная) информация не существует вне материального носителя, на ее носителем может быть как предмет (жесткий диск, карта накопитель и т.д.), так и электромагнитное поле (информация, передаваемая по каналам электронной связи), значит указанный подход ошибочный.

Рассматривая доказательственное значение цифровой информации нужно учесть, что им служит не физические свойства материального носителя информации, его состав, внешний вид, как у вещественных доказательств, а само содержание информации. Непонимание физической сути механизма образования, хранения, передачи цифровой информации приводит к смешению содержания понятий цифровой информации и вещественного доказательства. Первое это содержащиеся сведения, второе - это предмет. Информация находится на материальном носителе, по другому, оно не признается доказательством, но внешний вид носителя никак не отражает те сведения, записанных на нем, т.е. имеет значение только информация.

В зависимости от принятия сознания человека в участии отображения на носителе доказательственной информации, доказательства делятся: предметные и личные. Первые это те доказательства, в которых при формировании сознание человека не принимало участие. К ним относятся все вещественные доказательства. Остальные - личные. Есть доказательства, состоящие из двух частей: личной и предметной. К примеру,

обладающие признаками предметного доказательства определенные приложения к протоколам досудебных действий (слепки, видеозапись и т.д.) и заключениям экспертов (обычно фотографии). Остальные - полностью личные.

Предметные доказательства наименьшим образом искажают отобразившиеся на них следы исследуемого события, т.к. появившаяся на предмете информация, как правило, остается не изменой, если на нее не оказывает влияние внешняя среда (поверх видео, записаны другое). В отличие от этого личностное может исказиться, даже не по вине субъекта, т.к. каким бы не был добросовестным человек, доказательства, формируемые его сознанием, что не исключает потерю или искажения отдельных сведений. По сути, личное доказательство, это передача лица, о фактах, ставших известных ему при определенных событиях (свидетель, ставший очевидцем преступления; понятой, участвовавший в изъятии предметов и т.д.).

И. Кертэс разграничивая личные и вещественные (предметные) доказательства рассматривает механизм их формирования, полагая, что: «для вещественных доказательств характерно механическое элементарное отражение фактов, в то время как для других видов доказательств - мысленное, психическое отражение, это отделяет вещественные доказательства от всех других видов доказательств...» [45, с.26]. Между документом и вещественным доказательством отличия видят ученые в теории отражения. Документ, отражающий доказываемый факт механически, т.е. элементарно, то оно служит вещественным доказательством, если же в качестве субъективного восприятия объективного - мира, то оно имеет доказательственное значение документа [44, с.28].

По мнению А.В. Остроушко, «одним из элементов системы следообразования при совершении киберпреступлений, служат нетрадиционные материальные следы преступлений в виде компьютерной информации [46, с.28]. Наиболее полно отражающим специфику следов киберпреступлений, на наш взгляд, служит термин «виртуальный след», введенный впервые В.А. Мещеряковым. Он определил его «как любое изменение состояния автоматизированной информационной системы (образованного ею «кибернетического пространства»), связанное с событием преступления и зафиксированное в виде компьютерной информации (т.е. информации в виде, пригодном для машинной обработки) на материальном носителе, в т.ч. на электромагнитном поле» [47, с.104].

Н.Н. Лыткин предложил науке термин «компьютерно-технический след», отнеся их к материальным следам, представляющих особую форму следов - отображений, зафиксированных на электронных цифровых носителях» [48, с.24].

Л.Б. Краснова полагает, что «традиционные следы представляют собой отображение на одном материальном объекте внешнего строения другого материального объекта, тогда как основными взаимодействующими объектами при образовании виртуальных следов служат программные и информационные элементы компьютерных объектов, не обладающие материальной формой и соответственно, не имеющие внешнего строения». Автор отмечает, что следообразующим объектом выступает определенный алгоритм команд, оно может образоваться в результате действия пользователя при помощи применения программного обеспечения ЭВМ либо же появится без участия пользователя, действиями программного обеспечения в соответствии с алгоритмами его функционирования, заложенными в него разработчиками. В результате такого воздействия изменится состояние автоматизированной системы, в виде различных сбоев в работе системы либо модификации или появлении новой информации. Она также вводит термин «компьютерных объектов» а исследуя их, обращает внимание, что наибольший интерес представляют программные и информационные элементы компьютерных объектов, выступающие в качестве следообразующих и следовоспринимающих объектов [49, с.80].

По мнению Л.Б. Красновой, отличительной особенностью виртуальных следов, это их способность сохраняться в памяти технических устройств и являться изменениями автоматизированной информационной системы. Следообразующим и следовоспринимающим объектом выступают цифровые информации в виде программных и информационных элементов. Интересным является, что программа сама может быть объектом преступного воздействия либо использоваться как предмет совершения правонарушения. В качестве следообразующего объекта выступают программные элементы, а в качестве следовоспринимающего как программные, так и информационные элементы компьютерных объектов[49].

Давайте на примере ст.206 УК РК, рассмотрим распространение вредоносных программ, в этом случае, следообразующими объектами будут: сама программа, которая может попасть в компьютер двумя способами. Как правило, самый распространенный способ попадания вредоносной программы через электронную почту либо через USB-флэш-накопитель, в которой находятся файлы, уже содержащие вирус. В обоих случаях, следа воспринимающими объектами будут файлы вредоносной программы, скопированные с помощью вредоносной программы файлы данных и т.д. При рассмотрении возможности несанкционированного доступа к информациям следа образующим процессом будет процедура регистрации входа в сеть.

В операционных системах Windows существует специальная возможность фиксации действий, производимых на компьютере и для

фиксации действий, предпринимаемых взломщиком, пытавшийся нарушить целостность информационной системы - аудит.

Журнал безопасности Security Log используется в целях отслеживания (аудита) действий пользователей в системе. Есть три основных категории: 1) аудит сеансов работы пользователей; 2) аудит доступа к объектам системы; 3) аудит выполняющихся задач. Они дают основные сведения при наблюдении за действиями пользователей и служат важнейшими категориями в журнале безопасности Windows. Связав сеансы работы пользователя, процесс доступ к объектам, можно точно сказать, чем занимался пользователь, но для этого нужно знать, что и где проверять. В целях отслеживания входа в систему в первую очередь просматривают журналы безопасности на рабочих станциях и простых серверах, где нужно искать события с определенными номерами, т.к. все попытки проникновения в систему отслеживаются среди событий с указанием его номера.

По мнению Ю.К. Орлова, «Информация, содержащаяся в личных доказательствах, предварительно воспринимается сознанием индивида и перерабатывается, поэтому всегда содержит в себе элементы субъективности. Известно, что не бывает одинаковых показаний об одном и том же событии, воспринятых несколькими очевидцам в один момент и в одинаковых условиях, т.к. все они воспринимают и оценивают информация по-разному, которую также каждый по-своему воспроизведет [50, с.72]. Тогда как информация, созданная технической программной, подчиняется правилам, заданным ее автором или пользователем, которая применяемой программой, поэтому элемент субъективизма, в компьютерной информации отсутствует.

Мы полостью согласны с позицией Ю.К Орлова. Он разграничивает документы и вещественные доказательства следующими признаками: 1) информация в документе закодирована и выражена в определенной условной знаковой системе, тогда как в вещественных доказательствах информация не кодируется и содержится в естественном виде; 2) доказательственное значение вещественных доказательств определяется его физическими признаками или местонахождением, а для документа определяется его содержанием [50]. В.Я. Дорохов полагает, что содержание вещественного доказательства составляют лишь те их свойства, воспринимаемые непосредственно должностными лицами ОУП, судом и иными участниками уголовного процесса, свойства же, не поддающиеся непосредственному восприятию, образуют содержание иных доказательств [51, с.112].

Компьютерная информация это цифровое отображение информации на определенном носителе, являющийся средством вычислительной техники. Материальные носители этой информации - материальные объекты, в т.ч. физические поля, в них сведения отображаются в виде цифр, символов, алгоритмов, образов, сигналов, предназначенные для

перенесения информации во времени и пространстве. Информация всегда опосредована физическим носителем, вне которой она не может существовать и восприятие её возможно только посредством различных технических средств, от смартфона до стационарного компьютера.

Научно-технический прогресс в экспертной деятельности и криминалистике предоставил возможность использовать как доказательство микрообъектов, обнаружить их, при осмотре места происшествия нельзя, но также невозможно исключить их наличие. Выявить такие объекты, можно только в лабораторных условиях, используя соответствующее оборудование и криминалистические методики. Ю.К. Орлов, критикует любые возможные дополнения перечня вещественных доказательств иными видами, появившимися благодаря научно-техническому прогрессу в криминалистике и судебной экспертизе, акцентируя тем, что «размер объекта «микрочастиц» не может служить критерием различия вида доказательств... Деление на виды проводится совсем по иным признакам, их роли в событии преступления и производным отсюда доказательственным свойствам. Объект, будь он микро или макро-, в этом отношении никакого принципиального значения не имеет» [50]. М.Б. Вандер: «Под микрочастицами понимаются разные мелкие тела, а также малые количества веществ и материалов, невидимых либо слабовидимые при простом наблюдении». Он определяет микроследы как изменения в материальных объектах, вызванные микрочастицами [52].

По мнению Д.А. Турчина, «микроследами являются все микроскопические вещества, не видимые обычным зрением человека» [53].

Позиция ученых о невозможности восприятия микроследов без применения технических средств обосновано, но надо отметить, что даже в случае их применения, в целях обнаружения микрочастиц требуется химический анализ. В данном случае никакое преобразование либо перекодирования объекта не происходит, как с цифровой информацией. В этом случае, техническое средство перекодирует информацию из одного цифрового вида в другой аналоговый вид, либо наоборот. Компьютер, смартфон ил иное устройство обрабатывает сведения, представленные в цифровой форме. Ввод информаций и ее вывод осуществляется в привычной для пользователя форме, в виде цифр, букв, звуков, изображения и т.д., все это устройство осуществляет самостоятельно, на основе загруженных программ.

Рассматривая второй признак, предложенный Ю.К. Орловым разграничивая документы и вещественные доказательства, применительно к изучаемым нами объектам, следует согласиться с Б.Д. Завидовым и Н.П. Кузнецовым. По их позиции: «содержанием вещественного доказательства служат следы, свойства, признаки, которые непосредственно запечатлелись на предмете, доступны непосредственному восприятию и могут быть обнаружены путем осмотра. Наличие такой информации уже дает

основание считать этот предмет относящимся к делу» [54]. Вещественные доказательства интересуют ОУП исключительно в качестве предметов, их индивидуальных (физических) признаков (или местоположения). Компьютерная же информация используется в процессе доказывания для получения сведений, выраженных в знаковой (цифровой) форме. И если «...вещественное доказательство является непосредственным носителем информации, нужно для установления обстоятельств дела» [55, с.91], то компьютерная информация служит средством фиксации сведений с помощью программных средств.

Такое положение вещей, еще раз показывает, что доказательственное значение цифровой информации отражается в ее содержании, но никак не физическими свойствами носителя этой информации.

«Незаменимость и уникальность» это следующее качество служащее разграничением, его обычно называют процессуалисты [56, с.207]. Основа признака, то, что у любого материального предмета не может быть полностью идентичного двойника. Отличие от документов, вещественные доказательство уникально и незаменимо, все изменения, произошедшие с ним, связано с конкретным преступлением и никак невозможно воспроизвести его заново.

В.А. Камышин, разделяя документы - самостоятельные доказательства от документов - вещественных доказательств, отмечает, что первые, интересуют субъектов уголовного процесса в аспекте мыслей, закрепленных на материальном объекте, которые могут неоднократно воспроизводиться в содержании конкретной разновидности акта [57, с.111].

Если применить к компьютерной информации сведения, записанные на носителе компьютерной информации, могут быть многократно скопированы, но самое главное, чтобы целостность этой информации была сохранена, учитывая то обстоятельство, информация и ее носитель не связаны между собой неразрывно. Физический носитель информации в случае надобности заменяется другим, в т.ч. точно таким же носителем. К примеру, данные отправляются с ноутбука на флэш-карту, с соблюдением полного тождества файла, содержащего цифровую информацию (содержание и реквизитов).

Признак «среды существования» это следующее качество служащее разграничением, которое нам следует рассмотреть. Вещественное доказательство - это часть той среды, где происходило преступление. Оно всегда связано с изменениями в окружающей среде вследствие совершения преступления, поэтому служит средством выявления наличия или отсутствия этих изменений. По своему характеру изменения могут быть самыми различными: перемещение предметов в пространстве; изменения в самом предмете; уничтожение, предмета; создание нового предмета и т.д. Поэтому, вещественные доказательства надо рассматривать как предметы, бывшие частью той среды, в которую преступлением или другим

установленными по делу событиями внесены какие-либо изменения [58, с.11].

Между тем, ученые по-разному раскрывают содержание термина среды существования. Л.Б. Краснова отражает ее «как файловую систему» [49].

Т.Э. Кукарникова более широко трактует его, подразумевая под электронной (цифровой) средой систему объектов (компьютерных средств и систем), взаимодействующих на основе, формальных правил (архитектуры, стандартов, технических параметров устройств, языков программирования и т.д.) обработки, хранения и передачи информации, представленной в цифровой форме. В контексте электронный документ, и есть компьютерная информация, понимается как объект, несущий информацию, имеющую смысловое значение и не существующий вне электронной среды» [59].

«Аналоговая среда существования документа – это среда людей, действующих на основе выработанных обществом формальных и неформальных правил (с одной стороны, это – традиции, с другой стороны, – нормы, правила, установленные законодательством). При этом важно, что правила выработаны в процессе развития общества и являются по отношению к субъекту внешней силой. В электронной среде документ представляет собой последовательность сигналов, импульсов, являющихся элементами этой среды, поэтому электронный документ воспринимается только программно-техническим средством и целиком зависит от него» [60].

Подытоживая разграничение цифровой - компьютерной информации от других документом возможно по следующим четырем признакам:

- механизму образования: цифровая информация создается с помощью алгоритмов, заданных программой, источником доказательства иного документа выступает его автор;

- среде существования: компьютерная информация обрабатывается различными программами, с помощью техники и ее среда обитания электронная, иной документ мыслящими субъектами, т.е. людьми;

- привязке к носителю: компьютерная информация не привязано к материальному носителю, ее, возможно, использовать неоднократно, в отличие от иного документа, который привязан к материальному носителю;

- воспроизведения: цифровую информацию можно воспринимать только с помощью программы в техническом устройстве, ею считываемое, иной документ непосредственно воспринимается органами чувств субъекта.

Разграничить цифровую информацию от вещественных доказательств также возможно по следующим четырем признакам:

- доказательственному значению: цифровую информация это содержание сведений, которые находится на материальном носителе, по иному, оно не может быть доказательством, но внешний вид носителя ни как не отражается на самой информацию, записанной на ней (доказательственное значение имеет информация, не ее носитель).

Вещественное доказательство - это предмет и доказательственное значение определяется физическими свойствами или местоположением предмета;

- механизму образования: цифровой информация формируется на основании алгоритмов, заданных автором-разработчиком и реализуется программой (программа средство отражения фактов), а для вещественных доказательств характерно именно механическое отражение фактов;

- восприятия: цифровая информация передается через техническое устройство, т.е. физический носитель, вне любого устройства она не может существовать, а в вещественных доказательствах информация содержится в естественном, не кодированном виде, преобразование ее с помощью техники в целях восприятия субъектом не нужно;

- среды существования: цифровая информация обитает в электронной среде технических устройств и программ, а вещественные доказательства является частью аналоговой среды.

Подводя итог, в разграничении можно отметить, что существующие различия между цифровой информацией и вещественными доказательствами, а также другими документами, позволяют определить ценность компьютерной информации как отдельного вида доказательств. Она заключается в фиксации информации без ее обработки сознанием субъекта, в той форме, в каком, объективно существует, независимо от субъективного восприятия того, кто ее закрепляет. Такое положение вещей, свидетельствует о ценности компьютерной информации и надобности эффективного использования ее в доказывании.

1.3. Классификация цифровых информации как самостоятельного вида доказательств в уголовном процессе

Всякое научное исследование требует классификации, поэтому использование цифровых информации в уголовном процессе в качестве доказательств, также предопределяет целесообразность её научной классификации. Б.М. Кедров в исследованиях становления и единообразия развития науки, анализируя проблемы классификации, отражает, что «изучение объекта для классификации должно производиться комплексно, на основе логики и теории познания, с использованием всего арсенала понятий и категорий для решения задач познавательного характера, вытекающих из современного уровня научного знания» [61, с.116].

Классификация в теории доказательств состоит в систематизации накопленных научных знаний, предполагает правильное применение терминов, удаляет двусмысленность языка науки. Важным теоретическим и практическим значением классификации служит: помощь глубже осмыслить природу классифицируемых феноменов, систематизировав, верно использовать их при доказывании в уголовном процессе. Поэтому, мы

решили, что классификация цифровой информации, имеет ценность для сбора, проверки и оценки допустимости и относимости доказательств.

Давайте для начала вкратце осветим общую классификацию доказательств, т.к. отдельные аспекты распространяются на компьютерную информацию, которая является в свою очередь «цифровыми доказательствами». Классификация доказательств базируется на объективных различиях: происхождении сведении, структуре и функции. Прямые, косвенные, первоначальные, производные, обвинительные или оправдательные, личные и вещественные доказательства это общепризнанные деления доказательств.

Прямые доказательства, существующие в деле, устанавливают непосредственно факт совершения или не совершения лицом правонарушения, косвенные, через промежуточный факт. При существовании косвенных доказательств, требуется кропотливая работа ОУП или защитника, где значение больше придается логическому аспекту доказывания. Отдельные процессуалисты полагают, что деление доказательств на прямые и косвенные должно осуществляться по отношению к фактам в рамках конструктивных признаков состава преступления [62, с.58, 63, с.32]. Других полагаю, что это касается по отношению к обстоятельствам, указанным в ст. 113 УПК РК, т.е. к главным фактам, обстоятельствам, подлежащих доказыванию. Авторы «Теории доказательств в советском уголовном процессе» отражают, что «прямыми доказательствами нужно считать доказательства, прямо (т.е. одноступенчато) устанавливают предмет доказывания или один из его элементов, указанных в законе» [64, с.261].

Рекомендаций устанавливающие любой из элементов предмета доказывания, подвергается сомнениям Ю.К. Орловым, который полагает, что «при таком подходе нередко создается парадоксальная ситуация, когда при обилии прямых доказательств остается недоказанным главный факт, и никакие цели уголовного процесса не достигнуты» [50, с.67]. По смыслу, получается, что деление доказательств на прямые и косвенные по отношению к любому обстоятельству предмета доказывания закрепленных в ст. 113 УПК РК ведет к широкому определению прямых доказательств и признанию, что подчас ими устанавливаются факты, которые, выступают в качестве косвенных доказательств по отношению к другим обстоятельствам.

По мнению Н.П. Царева, «более правильно деление доказательств на прямые и косвенные в зависимости от их отношения к событию совершения или не совершения лицом, привлекаемым к уголовной ответственности, действии либо бездействии, предусмотренных уголовным законом. Оно упорядочивает процесс доказывания, облегчает мыслительные, логические стороны данного процесса, повышая значения прямых доказательств по делу» [65, с.60]. В данном случае упускается обстоятельство виновности

лица, что служит главным условием привлечения к уголовной ответственности.

В теории и практике доказывания спорным является достаточность косвенных доказательств, в обоснование истины по делу. Используя прямые доказательства, трудность доказывания состоит в признании соответствия их содержания фактам реальной действительности, их достоверности. Косвенные доказательства делают этот процесс сложным, поскольку нужно сначала достигнуть достоверности знания о промежуточных фактах, а затем на их основе делать вывод, связывающий с главным фактом. В связи с этим, одного косвенного доказательства не хватает сделать вывод, они должны быть в совокупности. Образованная совокупность косвенных доказательств, согласованных между собой, дополняют друг друга и влекут к однозначному выводу о виновности либо невиновности лица в уголовном правонарушении.

Как мы уже отметили, по отношению к источнику доказательств есть деление на первоначальные и производные. К первому, относятся полученные доказательства от первоисточника, а производными приобретенные от второго или последующего источника, т.е. не от первоисточника. Применительно к цифровой информации, данные, введенные пользователем или автором программы, являются первоначальными доказательствами. К примеру, к ним можно отнести: отчеты о продажах, бухгалтерские записи и т.д. Компьютерная информация, созданная ЭВМ согласно заложенной программой, служит производными доказательствами. Например: розыск автомашины правонарушителя, по полученным данным из аппаратно-программного комплекса «Сергек», восстановление облика человека по фотографиям многолетней давности; реконструкция дорожно-транспортного происшествия с применением компьютерной программы GPS (ГЛОНАСС) [65, с.271].

По вопросу разделения доказательств полученных от цифровой информации на обвинительные и оправдательные базируются на связи с предметом доказывания. Обвинительные доказательства, это изобличающие субъект в совершении уголовного правонарушения либо выявляющие отягчающие обстоятельства. В свою очередь, оправдательными доказательствами служат обстоятельства частично либо полностью исключающие вину субъекта в совершении правонарушения, а также предоставляющие смягчающие наказание обстоятельства.

Любой вид научной классификации, в т.ч. цифровой информации, немного относительно и строиться по самым разным основаниям. Как доказательств, научно-практическое значение имеет классификация цифровой информации, из учета характера механизма образования, формы существования.

Считается, что в 1991 г. впервые на территории СССР развернутое понятие «электронного документа» и классификацию предложили В.И. Першиковым и В.М. Савинковым в таком варианте:

1. Электронный документ (electronic document) - совокупность данных в памяти ЭВМ, предназначенная для восприятия человеком с помощью соответствующих программных и аппаратных средств;

2. Машинный документ (hard copy) - документ, подготовленный и выданный ЭВМ, при этом, форма документа готовиться заранее либо генерируется программой для ЭВМ;

3. Печатный документ (printed document) - твердая копия машинного документа, полученная на печатающем устройстве ЭВТ [67, с.89].

Классификация, предложенная Першиковым В.И. и Савинковым В.М., не совсем соответствует реалиям нынешнего времени в связи с техническим прогрессам, хотя в отдельных случаях ее возможно применить, поскольку она отчасти раскрывает отдельную информацию о цифровых доказательствах.

Н.А. Иванов утверждает, что «первым, наиболее общим и естественнонаучным основанием для классификации документов, служит, каким из органов чувств субъекта будет изначально восприняты сведения, отраженная на документе. Поэтому, документы он разделяет на две группы. Первая группа, где содержание информации в документе остается неизменно во времени. Вторая группа, к которой относятся документы содержание информации динамичные, т.е. аудио-, кино- и видеодокументы [68, с.54-59].

Кроме того, Н.А. Иванов в качестве следующего основания «отражает способ фиксации и восприятия информации, нанесенной на носители, с учетом этого различая документы, восприятие сведении производимых напрямую человеческим зрением и документы, информация на которых зафиксирована в преобразованном виде. В целях восприятия этой информации нужно обратное преобразование с помощью специальных технических приемов и средств» [68, с.54-59].

Более широкую трактовку оснований квалификации дает В.А. Камышин, в своей оригинальной концепции «свободных» доказательств:

1. Источнику формирования:

- официальные, исходящие от предприятий, учреждений и организаций;
- частные.

2. Способу закрепления:

- письменные (буквенные, цифровые и т.д.);
- графические (схемы, графики, чертежи, эскизы и т.д.);
- технические (фото-, видео, аудио).

3. Уголовно-процессуальной форме:

- процессуальные (объяснение, заявление, протокол явки с повинной и т.д.);

- непроцессуальные (документы, удостоверяющие личность, характеристики, справки и т.д).

4. Назначению:

- удостоверяющие;
- излагающие.

5. Способу получения:

- путем следственных действий;
- составленным органом ведущий уголовный процесс;
- истребованные;
- представленные участниками уголовного процесса либо иными лицами[57].

Как мы видим эта классификация В.А. Камышин, интересна для науки и практики, но к пятой по способу получения, мы бы еще предложили «путем проведения ОРМ, впоследствии легализованных согласно требованиям УПК». Некоторые процессуалисты, возможно, возразят, мотивировав тем, что оно охватывается «представленными участниками уголовного процесса либо иными лицами», но в этом случае, по нашему мнению не всегда возможно соблюдения требовании легализации материалов ОРМ.

А.Н. Яковлев классифицировал документы на машинных магнитных-носителях информации по тем же критериям, что бумажные документы:

3. Юридической природе:

- подлинные;
- поддельные;

2.Признаку дубликатности:

- оригиналы;
- дубликаты
- копии.

Оригинальность определяется по времени даты записи информации на носитель, документ, который имеет более раннюю дату создания и является подлинником, поздняя - дубликатом. Копия же это результат перезаписи оригинала или дубликата с одного носителя, на другой, при которой сохраняется аутентичность содержания документа.

3. Признаку общего происхождения:

- первоначальные;
- производные.

В случае создании нового экземпляра документа в качестве основы берется документ и в текст вносятся изменения, то исходный документ будет первоначальным, а итоговый - производным.

Между тем, А.Н. Яковлев не исключает, что подход к классификации компьютерной информации с технической автоматизированной точки зрения подготовки документов. К примеру, по способу фиксации информации документы воспроизводятся с помощью знаков, графических

изображений, звуков, видео; по способу создания документы: при помощи конкретной программы; а также могут использоваться иные признаки [69, с.61-65].

Т.Э. Кукарникова, классифицирует «электронные документы» по следующим признакам:

1. Форме существования:

- материальный электронный документ - объект, зафиксированный на электронном носителе, несущий в себе сведения, со смысловым значением и существующих только в электронной среде;

- виртуальные - документ, представляющий совокупность информационных объектов, создаваемый во взаимодействии пользователя с электронной информационной системой;

4. Источнику происхождения (создания):

- пользователем;

- компьютерной системой (т.е. электронной средой на основе программ и алгоритмов);

3. Содержанию:

- файлы, содержащие текстовую информацию, графику, анимацию, фото-, аудио- или видео;

- информация, записанная специальными машинными кодами и обозначениями.

4. Степени защищенности:

- открытые;

- закрытые.

5. Материальному носителю:

- устройства внешней памяти, оперативное запоминающее устройство ЭВМ;
- ОЗУ периферийных устройств;
- ОЗУ компьютерных устройств, связи и сетевые устройства[70, с.67-74].

В.Б. Вехов с позиции криминалистики условно подразделяет компьютерную информацию по следующим признакам:

1. Юридическому положению:

- не документированная - данные, команды и сигналы, образующиеся в процессе создания, преобразования, передачи, хранения, воспроизведения, уничтожения информации, не обладающие признаками документа. Однако, если они используются в качестве идентификационных реквизитов сообщения, то играют существенную роль в определении его документальности;

- документированная компьютерная информация (документ) - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

2. Категории доступности:

- общедоступная - компьютерная информация общего пользования, с неограниченным доступом;

- охраняемая законом - компьютерная информация, доступ к которой ограничивается в соответствии с правовыми актами.

3. Форме представления:

- электромагнитный сигнал - средство переноса компьютерной информации в пространстве и во времени с помощью электромагнитных колебаний (волн);

- упорядоченные семантические данные и команды;

- файл - поименованная область записей на машинном носителе информации, где в закодированном виде хранится строго определенная информация с реквизитами, позволяющими ее идентифицировать;

- программа для ЭВМ - это объективная форма представления совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата, а также подготовленные и зафиксированные на физическом носителе материалы, полученные в ходе ее разработки, и порождаемые ею аудиовизуальные отображения [71, с.15-17].

Полагаем, что в особенности заслуживает внимание классификация отраженная В.А. Мещеряковым в криминалистике: «- цифровая звукозапись (аудиозапись); - цифровой фотоснимок (картинка); - цифровая видеозапись; -программа для ЭВМ; - электронный документ» [72]. Классификация отраженная В.А. Мещеряковым отражает суть того, что компьютерная информация создается не только непосредственно на компьютере, как это могут подумать простой обыватель. Создать такую информацию можно с помощью другой техники, как смартфона, цифровой фотоаппарат либо видеокамера и т.д., что в целом генерируют компьютерную информацию.

Проанализированные и приведенные в статье А.Н. Иванова классификации американских ученых правоведов также заслуживают внимания. Они рассматривают классификацию электронных доказательств по происхождению доказательств, к которым относятся данные, внесенные пользователем, а также созданные компьютером в соответствии с заложенной программой. Такая квалификация идентична с одной из квалификации предложенной Т.Э. Кукарниковой. Другую классификацию предложил Крис Рид: по сущности доказательств, выделив шесть видов доказательств, представленных на примерах из судебной практики США: 1)исходные данные (raw data); 2)базы данных (daiabases); 3)коды, нужные для расшифровки электронной информации (codes necessary to interpret computer information); 4)особенности алгоритма программирования или обработки данных; 5)программное обеспечение коммерческого характера (commercial software); 6)компьютерные системы (computer systems) [73].

Классификация, предложенная Крис Рид, скорее правильным будет назвать как основания по механизму формирования содержания доказательств, т.к. в ней, отражается суть цифровых доказательств.

В своей диссертационной работе В.К. Лисиченко полагает, что для криминалистики и уголовного процесса существенное влияние на классификации имеет назначение, место возникновения и источник [74, с.105]. В свою очередь, Ю.К. Орлов не исключает возможность классификации по основаниям, касающихся содержания доказательств (существующие сведения) или к их источнику [75].

Выше отраженные все классификации различных авторов действительно заслуживают внимание, но более подробно в этом направлении по нашему мнению отработала Н.А. Зигура, предложившая свою классификацию компьютерной информации по следующим признакам:

1. Связь с событием преступления:

- компьютерная информация, послужившая орудием преступления (различные вредоносные программы; программы – взломщики и подбора паролей и т.д.);

- компьютерная информация, сохранившая в себе следы преступления. Пример, модификация компьютерной информации. Понимается любые изменения компьютерной информации, в т.ч. перевод такой программы или такой базы данных с одного языка на другой язык, за исключением адаптации, т.е. внесения изменений, осуществляемых исключительно в целях функционирования программы для ЭВМ или базы данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя [76]. Если Н.А. Зигура использовала пример с отражением норм п.9 ч.2 ст.1270 ГК РФ (часть четвертая), то по нашему законодательству можно сравнить это с п.43 ст.2 ЗРК «Об авторском праве и смежных правах» [77];

- компьютерная информация, послужившая объектом преступного посягательства. Предметом преступления в этом случае служит охраняемая правовыми актами (государственная, служебная или иная тайна, персональные данные) компьютерная информация, находящаяся на машинном носителе, в ЭВМ, в ее системе или их сети;

- иная компьютерная информация, устанавливающая наличие либо отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для дела (пример, регистрация входа в локальную сеть в не рабочее время) [10].

Классификации по этому признаку отвечает цели уголовно-процессуального доказывания - установлению обстоятельств, входящих в предмет доказывания. Согласно норме п.1 ч.1 ст.113 УПК РК по уголовному делу подлежит доказыванию событие и предусмотренные уголовным законом признаки состава уголовного правонарушения (время, место, способ и другие обстоятельства его совершения) [5].

Никто не оспорит, что событие уголовного правонарушения и виновность конкретного лица в его совершении, это главные элементы предмета доказывания для ОУП. Досудебное расследование начинается и

продолжается, а затем переходит на стадию судебного разбирательства, пока существуют основание полагать, что совершено уголовное правонарушение и существует субъект его совершивший. В случае не подтверждения указанных фактов, имеющимися доказательствами, уголовное дело либо преследование в отношении конкретного субъекта прекращаются.

2. Происхождению:

- компьютерная информация, созданная автором или внесенная пользователем, т.е. это деятельность человека. Пример: записи личного, делового характера; данные, внесенные в программу для последующей обработки. Ее особенность, это хранение на носителе, а не бумаге;

- компьютерная информация, созданная программами, т.е. результат обработки данных согласно заложенной программой. К примеру, восстановление облика лица по фото, сделанной много лет назад, информация регистрирующих- журналы, лог файлы, т.е. файлы фиксирующие с какого компьютера, в какое время, на какой адрес была передана информация [10]. Такую информацию подразделяют на регистрируемые данные (лог-файлы) и научные данные. «К научным данным возможно отнести результаты полученные с помощью компьютерных программ, разработанных на базе математических моделей процессов, протекающих при разрушении теплотехнических объектов, и позволяющие по последствиям, вызванным аварийной ситуацией на теплотехническом оборудовании (разлет осколков и элементов конструкций, травматизму обслуживающего персонала), выявить возможные причины разрушения оборудования» [78, с.460, 461], программы моделирования и анализа ДТП [79, с.500], программы воссоздания облика человека по фото или останкам.

Вышеуказанное основание классификации приводится большинством числом авторов, занимающихся исследованиями компьютерной информации, поскольку они понимают, что механизм образования такой информации создаваемой пользователем и компьютерной системой различен. Н.А. Зигура утверждает о возможности провести аналогию между механизмом образования компьютерной информации первого вида и личными доказательствами, между компьютерной информации второго вида и вещественными доказательствам. Поскольку созданную пользователем компьютерную информации можно исследовать по аналогии с личными доказательствами, а программой по аналогии с вещественными доказательствами.

3. Типу данных:

- текстовая информация;
- база данных;
- графическая информация;
- анимация;

- мультимедийная;
- программы [10].

Наблюдается очевидность, необходимость классификации по типу данных, т.к. исчерпывается все возможные виды компьютерной информации, что позволяет органам досудебного расследования, суду и защитника не упустить ни одного из этих признаков. Значение этой классификации является отображение и исследование разных типов данных, производимые различными программами. Разными являются подходы и методы изучения этих данных. Пример: при анализе баз данных, нужно учесть потенциал помещенных на хранение данных, эти определяют специфику обзора и учета особенностей информации в уголовном процессе.

4. Типу носителя:

- компьютерная информация на энергозависимом носителе, т.е. на устройстве памяти, предназначенной для хранения данных (программ, переменных и т.д.) только при включенном компьютере. Отключение компьютера, влечет отсутствие энергии, удаляется содержимое памяти, восстановить ее невозможно. Примером служит ОЗУ.

- компьютерная информация на энергонезависимом носителе, т.е. устройстве памяти, предназначенной для хранения данных, основанные на принципах магнитной, оптической или любой другой записи, не зависящей от наличия электропитания. Пример: диски, флэш-накопители и т.д. [10].

Ценность классификации по типу носителя отражается по способу выявления и закрепления компьютерной информации, которые этих носителях разные. В первом случае сведения можно получить только на этапе первичных процессуальных действиях при функционирующем компьютере, как только он выключается, будет утеряна возможность получения каких либо данных. Во втором случае, информация не теряется, т.е. на последующих этапах досудебного и судебного расследования, есть возможность проведения экспертизы. Мы видим, имеется различие и в закреплении информации, которые могут выступить впоследствии доказательством на этих носителях.

5. Степени свободы использования на основании закона:

- общедоступная (открытая), к ним относятся общеизвестные сведения и иная информация, с не ограниченной формой доступа. Общедоступная информация может использоваться субъектами по своему усмотрению при соблюдении правовых актов, устанавливающие ограничения по ее распространению;

- ограниченного доступа, т.е. охраняемая правовыми актами государственные секреты, банковская, коммерческая, служебная и иная тайна. Ограничение к доступу к информации устанавливается правовыми актами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны и безопасности государства[10].

Примером защиты информации ограниченного доступа может служить ЗРК «О персональных данных и их защите», согласно им нельзя распространять определенные сведения о физических лицах, таких как анкетные данные, сведения о месте проживания и наличии имущества [80].

Существуют также другие правовые акты, регулирующие определенные сферы деятельности общественной жизни, такие как ЗРК «О государственных секретах», «О нотариате», «О банках и банковской деятельности в РК» и т.д., которые охраняют тот или иной вид секретов (тайн). Интересным является факт, что информация, находящаяся в открытом доступе также может быть отнесено к охраняемой. К ним относятся принадлежащие обладателю, доступ к которому он ограничивает в силу своего права обладания. Значение классификации по степени свободы использования на основании закона заключается в определенных ограничениях в доступе ко второй группе информации, это в свою очередь дополнительные временные и организационные мероприятия. К примеру, в целях легализации результатов ОРД и их приобщения к уголовному делу, ОУП нужно вынести постановление с соблюдением всех мер безопасности, процессуальной стороны и т.д. Однако, возможно предоставления материалов ОРД с соблюдением режима секретности и только ограниченному кругу лиц.

6. Степени защищенности программными средствами:

- открытая, в этом контексте, является информация, доступная при её открытии;

- скрытая (защищенная), это информация, для ознакомления с которой нужны дополнительные манипуляция: ввод пароля; использование программ дешифрирования; настройка системы для отображения файлов с различными атрибутами и т.д. [10].

Значение этой классификации заключается в ознакомлении с содержанием открытой информации без труда, во втором случае для этого нужно дополнительное время, ее продолжительность, применение специальных программ, дополнительной технически может повлиять на планирование времени досудебного расследования.

Подводя итог, по этому подразделу, можно без сомнения утверждать, что классификация способствует развитию науки, анализу классифицируемых объектов, в нашем случае «цифровой информации», крупицы собранных в теории знании, позволяет на практике осмыслить возможности сбора и применения «цифровых доказательств». Анализ предложенные разными авторами, позволила осмыслить все возможные виды квалификации «компьютерной информации», которая служит основой всех «цифровых доказательств». Осознание этого, по нашему мнению позволит развить нашу диссертационную работу и способствует выработке определенных методов сбора, проверки и оценки на основе полученных знании квалификации компьютерной информации.

Раздел 2. Собирание, проверка и оценка цифровой информации как самостоятельного вида доказательств в уголовном процессе

2.1. Собирание цифровой информации на досудебной стадии

В соответствии с ч. 1 ст. 121 УПК РК доказывание состоит в собирании, исследовании, оценке и использовании доказательств с целью установления обстоятельств, имеющих значение для законного, обоснованного и справедливого разрешения дела. Доказывание производится только по уголовным правонарушениям, по которым начато досудебное расследование в порядке, предусмотренном гл.23 УПК «Начало досудебного расследования» [5].

Интересным явлением служит то, что еще за долго до приобретения Казахстаном независимости и начало разработки, а затем принятия УПК ряд авторов изложили свои мысли по вопросам доказывания. Они утверждают, что «по своему содержанию доказывание слагается из ряда элементов, органически связанных между собой. Классическим и общепризнанным является выделение в процессе доказывания элементов сбора, проверки и оценки доказательств, неразрывно связанных между собой, протекающие в единстве на всех стадиях процесса в установленных процессуальных формах» [81, 82, 83].

По этой причине, можно смело утверждать, что нормы отраженные в УПК основаны на уголовно-процессуальной теории доказательств и частной криминалистической теории доказывания. Кроме того, вникая в процесс доказывания, начинаешь понимать ее сложность в деятельности ОУП. Поскольку обязанность доказывания наличия оснований уголовной ответственности и вины подозреваемого, обвиняемого согласно ч. 2 ст. 121 УПК РК лежит на обвинителе.

Как мы видим, законодатель в РК, так и люди науки, создававшие в СССР доктрину по вопросам доказывания схожи во мнении, отразив три элемента: 1) собирание; 2) проверка; 3) оценка. Поэтому, неслучайно в нашей диссертационной работе, мы решили рассмотреть все три элемента в отельном разделе, рассмотрев каждый элемент в отдельном подразделе.

Содержание первого элемента процесса доказывания в юридической науке раскрывается неоднозначно. А.И. Винберг, Р.С. Белкин определяют его как «совокупность действий по обнаружению, фиксации, изъятию и сохранению различных доказательств» [83, 84].

О.В. Волынская раскрывает «собирание доказательств как единство обнаружения и фиксации фактических данных» [85, с.128]. З.З. Зинатуллин утверждает, что «сбор доказательств это обнаружение, получение и процессуальное закрепление фактических данных в структуре собирания доказательств [86, с.128].

В.М. Тертышник утверждает, что «собирание доказательств заключается в выявлении источников и носителей доказательств, получении и закреплении фактических данных, содержащихся в них [87]. По мнению А.А.Хмырова «объекты окружающей среды с отразившимися на них следами преступления сами по себе еще не являются доказательствами, т.к. они должны быть обнаружены, закреплены и надлежащим образом удостоверены специальными субъектами: ОУП либо судом» [88]. Интересная позиция у А.Шейфер, который первым ввел термин «формирование доказательств» и приравнял его к «собиранию доказательств». «Собирание (формирование) доказательств - это активная целенаправленная деятельность ОУП и суда, состоящая в извлечении из следов, оставленных событием, фактических данных, относящихся к делу, в преобразовании и закреплении этих данных, т.е. в придании им надлежащей процессуальной формы» [89]. Е.А. Доля, вообще полагает: что «Словосочетание «собирание доказательств» искажает существо деятельности, которую ею обозначено, психологически предполагая наличие доказательств в готовом виде. Если исходить из такой посылки, то доказательство остается только собрать, значит, их не собирают, а формируют» [90].

Между тем, по мнению Е.А. Доля «доказательств в уголовно-процессуальном смысле в готовом виде в природе либо в обществе не существует. Нужна практическая деятельность, направленная на включение в процесс доказывания той части объективной и субъективной реальности, в которой отразилось уголовное правонарушение. По мере реализации этой деятельности формируются доказательства являющиеся сведениями о фактах и обстоятельствах, имеющих значение для уголовного дела» [91].

Обратим внимание, что В.А. Семенцов разделяет мнение А.И. Винберг, Р.С. Белкина и З.З. Зинатуллина. Он утверждал, что «сущность формирования доказательств состоит в совершении действий, направленных на обнаружение, получение и последующее процессуальное закрепление любых сведений, в порядке, определенном УПК, на основе которых суд и ОУП устанавливает наличие или отсутствие обстоятельств, имеющих значение для правильного разрешения уголовного дела» [92].

Нужно отметить, что закрепление добытой информации на основании требовании предусмотренных правовыми актами служит заключительным и одним из основных этапов формирования доказательств. Поскольку в случае не надлежащего процессуального оформления собранные доказательства могут быть признаны недопустимыми.

Более того, М.С. Строгович отмечал, что «пока доказательство не рассмотрено и не закреплено процессуально, нельзя утверждать, что оно действительно обнаружено, т.к. еще неизвестно, что именно обнаружено и будет ли служить действительно доказательством то, что обнаружено» [93].

Есть авторы, рассматривающие закрепление не как завершающий момент формирования доказательств, а в качестве самостоятельного элемента в структуре уголовно-процессуального доказывания.

По мнению В.С. Балакшин в структуре уголовно-процессуального доказывания помимо 3-х ранее указанных элементов присутствует «закрепление» и они расположены в следующем порядке: сбор, закрепление, проверка и оценка. Он полагает, что «закрепление доказательств - это не часть собирания доказательств, а самостоятельный элемент доказывания» [94]. Не включает закрепление в «собирание доказательств» и В.П. Колмаков. Он рассуждает о «способах собирания и закрепления доказательств» или наравне с собиранием - об обнаружении доказательств» [95].

По нашему мнению В.А. Семенцова «доказательства формируются в процессе познавательно-удостоверительной деятельности, поэтому процессуальное закрепление в совокупности с обнаружением и получением образуют в единстве первый элемент уголовно-процессуального доказывания - формирование доказательств. Обнаружение относимых к делу данных - означает их восприятие органами досудебного расследования и судом из источников, в формах, предусмотренных УПК, которое он называет «непосредственным чувственным» [92].

Прежде чем, относимые к делу информация может воспринято субъектами доказывания, нужно найти возможный ее источник. В свою очередь способами формирования доказательств, служит процедура определенных методов, предназначенных для обнаружения, получения, фиксации, исследования фактических данных конкретного объекта. Теории доказательств отмечает, что основным содержанием приемов сбора и проверки доказательств, служат познавательные методы, которые позволяют получить нужные сведения и передать ее адресатам доказывания. Наличие формализованных правил, исполнение которых должно удостоверить ход и результаты использования соответствующих познавательных приемов и операций, составляет специфику процессуального способа сбора и проверки доказательств. Учеными предлагается сочетание следующих приемов и операций, предназначенных для получения и передачи доказательственной информации: «а) определение вида сведении, на получение которых направлен этот способ; б) перечень участников; в) описание методов по сбору и проверке доказательств; г) место и время применения методов; д) условия их допустимости; е) последовательность методов; ж) меры обеспечения полноты и достоверности доказательств, исключающие попытки заинтересованных препятствовать их получение либо искажения; з) меры обеспечения всесторонности сбора и проверки доказательств; и) меры предотвращения незаконного вторжения в личную жизнь граждан, обеспечения безопасности и ограждения достоинства лиц, у которых или с

помощью которых должны быть получены сведения; к) специальное детализированное определение методов по закреплению собранных сведений и результатов их проверки, как и сведений, подтверждающих соответствие действий по сбору и проверке доказательств, требованиям закона» [64].

Из этого можно сделать вывод, что каждому самостоятельному виду доказательств, свойственный свой определенный способ формирования, следовательно, в целях формирования компьютерной информации нужна специальная технология, особые методы исследования, изъятия, закрепления, заключающихся в этих видах доказательств. По этой причине, нельзя не согласиться с точкой зрения Т.С. Дектярь: «если ОУП не владеют средствами и методами сбора различных изменений материальной среды (сведений о фактах), то содержащаяся в них информация не сможет фигурировать в уголовном деле». Он указывает на три аспекта этих знаний: 1) «без использования специальных знаний сложно выяснять многие обстоятельства, подлежащие доказыванию»; 2) «использование специальных знаний существенно поднимает уровень достоверности собранных доказательств»; 3) «применение специальных знаний повышает результативность сбора и формирования доказательств, в процессе досудебного расследования» [96].

Нет сомнений, что последние 30-ть лет актуален вопрос криминалистического исследования любых видов технических средств, позволяющий создавать, воспроизводить и передавать «компьютерную информацию» на предмет установления их использования в преступных целях и получения значимой информации для ОУП, в целях использования их в процессе доказывания уголовных правонарушении. Еще в 90-е годы прошлого века В.А. Махов и В.П. Зезянов утверждали: «в целях эффективного выявления, быстрого и полного расследования преступлений, где использована компьютерная техника, требуются новые подходы, основанные на достижения науки и техники, при содействии сведущих лиц» [97, 98]. В начале 2000 годов Е.Р. Российская отмечала: «сложность и многообразие форм электронных документов и создаваемых на их основе машинограмм, в условиях отсутствия достаточно разработанного методологического аппарата, накладывают особые требования к использованию специальных знаний при их исследовании» [99].

Согласно, ч.1 ст.80 УПК РК, специалистом является лицо, обладающее специальными знаниями, нужными для оказания содействия в сборе, исследовании и оценке доказательств путем разъяснения участникам уголовного процесса вопросов, входящих в его компетенцию, а также применения научно-технических средств, который также как и эксперт не должен быть заинтересован в исходе дела [5].

В научной среде бытует мнение, что «в отличие от эксперта, специалист действует не самостоятельно, его деятельность в уголовном

процессе протекает под контролем следователя, он помощником следователя и «заменяет следователя в силу не процессуальной, а научно-технической некомпетентности последнего» [100].

Соглашаться с тем, что фигура специалиста не самостоятельна нельзя.

Специалист приглашается судом или ОУП в целях оказания разного рода научно-технической помощи в проведении процессуального действия. Содержание процессуальных действий заключается в исследовании ОУП и суда, осмотра места происшествия; выявления, изъятия и фиксации в соответствии с требованием УПК различных материальных объектов и следов на них для получения информации, имеющих значение для конкретного уголовного дела, а также событий, содержащих уголовное правонарушение.

Н.А. Иванов полагает, что «привлечение экспертов судебной компьютерно-технической экспертизы в качестве специалистов для обнаружения и изъятия информации с машинных носителей, которые физически не могут быть доставлены в экспертное учреждение (случаи в практике не редкость), является одним их важных направлений деятельности экспертов. Одним из них служит исследование энергозависимой памяти, а именно: проанализировать действия выполняемых программ и процессов, зафиксировать информацию на энергонезависимом носителе» [68]. Роль специалиста незаменима в выявлении внешнего коммуникационного оборудования (свичи, кабели), отражающее возможность подсоединение компьютеров к сети.

Разъяснения специалиста это самостоятельные доказательства, поскольку, как правило, содержат сведения об обстоятельствах, имеющих значение для уголовного дела. Законодатель отметил, что разъяснения бывают в письменном и устном виде. В первом случае это его заключения, во втором это полученные его показания в ходе допроса, которые запротоколированы судом или ОУП. Следственно-судебная практика показывает, что заключение специалиста имеет самостоятельный статус доказательств. К примеру, по делам об уголовных правонарушениях, квалифицируемых ст.198 УК РК «Нарушение авторских и (или) смежных прав», в случае изъятия предположительно контрафактной продукции на DVD и CD дисках. Перед специалистом ставятся такие вопросы: 1) Имеются ли признаки контрафактности, на исследование DVD и CD дисков. Если да, то, какие? 2) Кто обладатель прав на произведения отраженных в DVD и CD дисков на территории РК? 3) Какова стоимость аналогичных лицензионных экземпляров представленной продукции? В зависимости от того какие вопросы еще интересуют ОУП для принятия правильного процессуального решения могут быть поставлены и иные вопросы.

В других случаях, по делам об уголовных правонарушениях, квалифицируемых ст.ст.311, 312, 313 УК РК перед специалистом ставятся вопросы наличия в информационных материалах порнографического

характера, привлечение несовершеннолетних лиц, незаконное распространение произведений, пропагандирующих культ жестокости и насилия, наличие призыва экстремисткой и/или террористической деятельности.

Роль специалиста при изъятии и исследовании «компьютерной информации» незаменима в следующем: 1) содействие в выявлении и изъятии информации; 2) применении технических и программных средств; 3) оказании помощи формировании вопросов эксперту; 4) разъяснении сторонам и суду вопросов, входящих в его профессиональную компетенцию.

При сборе доказательств, в особенности «цифровых» на досудебной стадии нужно применение НТС. В ч.2 ст.126 УПК РК отражен, что «для оказания содействия при использовании НТС органом, ведущим уголовный процесс, может быть привлечен специалист» [5]. В научной литературе идут споры по допустимости доказательств собранных с помощью НТС.

Еще во время СССР появилась первая теория, ее сторонники утверждают, что сбор доказательств допустимо только с помощью НТС, прямо предусмотренных законом, в случае применения иных средств, то оно должно влечь их недопустимость [101]. Другие авторы утверждают, что в законе нельзя предусмотреть исчерпывающий перечень допустимых НТС, т.к. техника совершенствуется, а значит, законы всегда будут отставать. Следовательно, нужно идти по пути разработки лишь общих принципов допустимости НТС в уголовном процессе. Ю.К. Орлов предлагает: «при поиске доказательств допустимо применение разных НТС, разумеется, за исключением опасных для жизни и здоровья и унижающих честь и достоинство человека. Главное это факт обнаружения доказательства, способ не имеет никакого значения. Например, если в лесу обнаружен тайник с оружием, то совершенно неважно, каким образом это сделано - с использованием какой-то техники или путем сплошного прочесывания местности. Доказательство остается доказательством независимо от способа его обнаружения (при условии правильного оформления)» [50].

С позицией второй категорией ученных, в т.ч. и Ю.К. Орлова мы можем согласиться, но с первой никак нельзя. Обратим внимание, что УПК, в СССР, РК и других постсоветских странах не отражают какие НТС можно применять. В них отражается о фото– и киносъемки, звуко– и видеозаписи, а в УПК РК отражено еще о доказательствах содержащихся в компьютерных информациях. Следовательно, в УПК не идет речь о применении самих НТС, хотя в них есть отсылка на ЗРК «Об ОРД», «О контрразведывательной деятельности». В этих правовых актах нет точных сведении об НТС, но применяются такие термины «оперативное снятие информации с устройств, предназначенных для сбора, обработки, передачи и хранения информации», «оперативные аудио- и (или) видеоконтроль лица, места», «оперативное получение информации о соединениях между абонентами и (или) абонентскими устройствами», «специальные технические средства».

Поэтому мы, полностью поддерживая Ю.К. Орлова, полагаем, главная задача при сборе это обнаружение нужной информации и правильная фиксация, т.е. приобщение к материалам досудебного расследования.

Наша позиция подтверждается ст.126 УПК РК, которая гласит, что «НТС в процессе доказывания по уголовному делу могут быть использованы органом, ведущим уголовный процесс, а также экспертом и специалистом при исполнении ими процессуальных обязанностей, предусмотренных УПК».

Однако, «применение НТС признается допустимым, если они: 1) прямо предусмотрены законом или не противоречат его нормам и принципам; 2) научно состоятельны; 3) обеспечивают эффективность производства по уголовному делу; 4) безопасны».

«Использование НТС органом, ведущим уголовный процесс, фиксируется в протоколах соответствующих процессуальных действий и протоколе судебного заседания с указанием его данных, условий и порядка их применения, объектов, к которым эти средства были применены, и результатов их использования»[5]. «Отражение в протоколах применение НТС удостоверяет факт их использования, это обстоятельство позволяет полученную с их помощью информацию, оценить и проверки»[102]. «Игнорирование протоколирования факта применения НТС обесценивает доказательственное значение запечатленных на соответствующих носителях информацию, не позволяя определить их относимость к делу и, соответственно, их допустимость» [103]. Е.А. Доля придает важное, значение для сбора, проверки и оценки доказательств роли о характеристиках НТС, условиях и порядке их применения при производстве ОРМ. Он отмечает, что такие сведения нужны, чтобы при досудебном либо судебном разбирательстве (просмотр видео- кино- либо фотосъемки, прослушивании аудиозаписи представленных ОУП) применить технические устройства, позволяющие воспроизвести запись, съемку без искажений и каких-либо необратимых изменении. Как правило, в практике с такого рода трудностями встречаются работники судов, когда в процессе требуется воспроизвести компьютерную информацию с носителей, представленных участниками процесса. Использование несоответствующей техники и программного обеспечения может привести к повреждению, изменению или утере «компьютерной информации», что в свою очередь может повлечь к потере доказательств в целом. Поэтому при представлении «компьютерной информации» нужно отражать их список и реквизиты, находящиеся внутри носителя и информацию о программах, с помощью чего можно ее воспроизведение [104].

Осуществляя сбор «цифровых доказательств» нужно всегда помнить о типах носителей «компьютерной информации»: энергозависимых и энергонезависимых, а также их особенностях. В частности потери информации с энергозависимых носителей при отключении энергетического

питания и возможности изменении и/или удаления сведении на энергонезависимых носителях в случае установления на нем программ против несанкционированного доступа (использование неправильного пароля). В целях сохранения информации выявленной специалистом с энергозависимого носителя, ее нужно зафиксировать путем копирования на энергонезависимый носитель, все эти действия нужно отразить в протоколе. В указанном случае в одном процессуальном документе фиксируются две группы свойств: 1) составляет содержание протоколов досудебного и судебного разбирательства как самостоятельный вид доказательств (...обнаружен персональный компьютер, находящийся во включенном состоянии ...); 2) содержание в нем цифрой информации.

В другом случае, при выявлении работающего персонального компьютера и надобости описания информации, содержащиеся в его оперативной памяти, можно для полноты процессуальных действий отдельно произвести осмотр «компьютерной информации» и составить отдельный протокол осмотра. Содержание «компьютерной информации» будет выражаться через процессуальную форму - протокол осмотра компьютерной информации, в котором нужно отразить:

- программу, исполняемую или исполненную компьютером на момент проведения или до проведения досудебного процессуального действия;

- результат действия запущенной (исполняемой) программы;

- манипуляции со средствами компьютерной техники, включая описание порядка соединения между собой всех устройств, а также нажатия на клавиши клавиатуры, произведенные в процессе проведения процессуального действия и их результат (например, при операции копирования программ и файлов нужно указать сведения о компьютерной информации и ее реквизиты, список файлов, тип, размещение файлов на носителе, объем, дата и время создания, изменения, открытия);

- системное время на осматриваемом компьютере.

Между тем, трудно судить какой из этих способов фиксации «компьютерной информации» в протокол является правильным, но можно смело утверждать, что применения любого из них не нарушает закон, самое важное это отразить всю имеющуюся в компьютере «цифровую информацию» в протоколе.

Нами изучены приговора, где ОУП расследовали преступления в отношении «хакеров» использовавшие свои знания и с помощью технических устройств (ноутбука, смартфона) и интернета похищали денежные средства юридических и физических лиц. Приведем выдержку из одного приговора:

Протоколом осмотра предметов и документов от 01.09.2015 г., выявлено, что на ноутбуке марки «AppleMacbookPro» серебристого цвета серийный номер C02LX5YRFD56 установлена операционная система MAC OS X 10.10.1, а также с помощью программы Parallels Desktop для Mac

установлены два виртуальных компьютера на базе Windows 7 и Windows XP. На рабочем столе операционной системы MAC OS X имеются скриншоты экранов зараженных компьютеров, выполненные на этом ноутбуке, имена файлов имеют дату и время исполнения скриншотов. На рабочем столе виртуального компьютера на базе Windows XP имеется большое количество разновидностей RAT- программ. RAT- программа - это один из наиболее опасных вредоносных программ, дающая возможность злоумышленнику получить полный доступ и контроль над компьютером. Обнаружены следующие RAT- программы: Darkcomet2014, CyberGate v3.4.2.2, Indetectables Rat v.0.3.1, NanoCore. Также обнаружены программы упаковщики исполняемых файлов. Программы используются при создании вирусов, чтобы зашифровать и видоизменить код вируса для затруднения его обнаружения системами. В системе Windows XP запускалась клиентская часть Darkcomet, т.к. имеется журнал действий пользователя данного ноутбука в папке «C:/Documents and Settings\Admin\Application Data\dclogs». В журнале имеется переписка об упаковке вредоносного ПО за вознаграждение, имеются записи о подготовке текста писем и ссылок с вредоносными ПО для рассылки. Имеется информация об использовании электронных адресов: mail2omarov@gmail.com, knb6kz@gmail.com, karim2masimov@gmail.com, dastarov@mail.ru. В системе Windows XP запускалась клиентская часть неизвестного ПО. В системе Windows XP 01.06.2015 г. запускалась клиентская часть NanoCore RAT. При осмотре почтового ящика mail2omarov@gmail.com обнаружена переписка с адресом NimoruSoftware@gmail.com о приобретении вредоносной программы ПО NanoCore RAT и оплата с помощью платежной системы PayPal, имеется переписка с адресом AtomParkSoftware о приобретении программы для массовой рассылки электронных писем ePochta и оплата с помощью платежной системы PayPal. В переписке с пользователем Дастаровым Б.Е. в одном из писем обнаружен текст письма, использованный при рассылке вредоносного ПО. На зараженном компьютере использовали электронную почту gmc_astana2@mail.ru, nadinura@mail.ru [105].

По мнению Я. Дорохова: «Протокол осмотра предмета нельзя отнести к самостоятельному виду доказательств - протоколам досудебных и судебных действий, имеющих свое содержание и форму с характерными для них особенностями. Его составление предназначено только для фиксации чувственность наглядный вид предмета» [51]. Данный подход применим к «цифровым доказательствам», в частности «компьютерной информации». Протокол осмотра - это элемент формирования, введения в процесс доказывания «компьютерной информации» или процессуальная форма как доказательство, выражающее ее содержание.

Поскольку способами сбора и проверки доказательств, служит система приемов и операций, предназначенных для обнаружения и закрепления информации определенного вида, рассмотрим, какие приемы и операции

нужно использовать для выявления фактических данных в виде «компьютерной информации» при досудебном расследовании. Важными досудебными процессуальными действиями при расследовании преступлений, совершенных с использованием средств технических средств, являются осмотр, обыск и выемка информации, в т.ч. на разных технических устройствах и иных стационарных накопителях.

Перед осмотром места происшествия нужно принять меры, что бы присутствовал специалист с соответствующим техническим устройством, используемый для считывания и хранения изъятой информации. Им может быть переносной ноутбук, электронный планшет или смартфон, в иных случаях может быть достаточно любой из внешних электронных носителей информации. Напомним, что к электронным носителям относятся носители для однократной или многократной записи (обычно цифровой) электрическим способом: оптические (CD-ROM, DVD-ROM, Blu-ray Disc); полупроводниковые (флеш-память, SSD-диски); магнитные (магнитные ленты, дискеты, жёсткие диски). Все технические средства, устройства и специальные программы, позволяющие считывать, копировать, сохранять и производить экспресс-анализ различных компьютерных информаций должны быть заранее подготовлены до произведения процессуального действия.

Прибыв на место происшествия нужно принять меры к сохранности компьютерной информации в подлежащих осмотру технических устройств и внешних электронных носителях, для этого нужно запретить:

- использование и в целом прикасаться к любому техническому средствам, устройствам, кабелям питания и Wi-Fi оборудованию, для этих целей нужно выделить ответственных лиц;
- выключать электроснабжение объекта.

При проведении какого-либо процессуального действия, в т.ч. копирования компьютерной информации обращать внимание понятых на все детали производимые специалистом или другими должностными лицами ОУП и отражать это в протоколе. Осматривая работающий компьютер, с участием специалиста требуется:

- определить тип установленной операционной системы. В случае установления системы семейства Microsoft Windows, следует выяснить серийный номер и имена зарегистрировавших её лиц. Полученную информацию, изображенную на экране дисплея, требуется детально описать, по возможности произвести распечатку, сфотографировать или произвести видеозапись;
- обратить внимание и зафиксировать в протоколе дату и системное время на осматриваемом компьютере, которое расположено в правой нижней части экрана, оно иногда отличаться от реального времени;
- выявить, какие программы, приложения, открыты и функционируют. Если загружена одна из версий операционной системы семейства Microsoft

Windows, это видно на дисплее, открыв Диспетчер задач Windows (Task Manager в англоязычной версии Windows). Диспетчер задач открывается при одновременном нажатии сочетания клавиш Ctrl Alt Del;

- установить, какие процессы запущены. Сведения также доступны из Диспетчера задач. Все появившееся на экране нужно описать в протоколе и по возможности зафиксировать с помощью фото- или видеозаписи. Тип программного обеспечения, загруженного в момент осмотра компьютера, может свидетельствовать о задачах, для которых использовался данный компьютер;

- при наличии технической возможности скопировать информацию, имеющих значении для дела (программы, файлы данных), находящиеся в ОЗУ, т.к. после отключения компьютера она может быть утеряна;

- копируя информацию, требуется показать понятым об отсутствии информации на технических устройств и внешних электронных носителях, куда производится копирование.

- отразить тип и размер, изготовитель электронного носителя, куда производится копирование, программу, позволяющее копировать, список скопированных файлов, их тип, размещение на носителе, объем, дата и время создания, изменения, открытия;

- упаковать электронный носитель (конверт, коробку, полиэтиленовый пакет и т.д.) и опечатать. Информацию можно утерять, если в нее попадет влага, сильное температурное нагревание или переохлаждение, влияние электростатических - магнитных полей;

- по мере нужды и возможности приостановить программы и выяснить, какой результат получен после окончания работы;

- определить наличие в компьютере накопителей информации (жесткие диски, дисководы, стримеры, оптические диски, иные внешние электронные носители), их тип (вид) и количество.

В случае подключения компьютера к локальной сети, требуется:

- выяснить количество подключенных к серверу рабочих станций либо компьютеров, вид связи сети, количество серверов в сети;

- по возможности организовать одновременный осмотр включенных в локальную сеть рабочих станций и компьютеров (по изложенной выше схеме осмотра работающего компьютера). Если возможность отсутствует, можно остановить работу компьютера и производить осмотр в режиме неработающего компьютера. Но, нужно помнить, что даже если по внешним признакам создается впечатление о не работе компьютера, все равно следует избегать каких-либо самостоятельных действий с ним без специалиста.

Изымая технические устройства и электронные носители информации, выявленные при осмотре места происшествия, требуется соблюдать правила безопасности указанные производителями, а также руководствоваться методическими рекомендациями по упаковке и транспортировки:

1) Компьютерная техника изымается только в выключенном состоянии, об этом нужно отразить в протоколе такие действия:

- описание рабочего состояния оборудования и фиксация порядка отключения;

- описание точного местонахождения изымаемых предметов и их расположения относительно друг друга и окружающих предметов, с приложением схем, планов, фото таблицы и видео;

- описание порядка соединения между собой всех устройств с отражением особенностей соединения (цвет, количество, размеры, характерные индивидуальные признаки соединительных проводов, кабелей, шлейфов, разъемов, штекеров и их спецификация);

- наличие или отсутствия компьютерной сети, используемых каналов связи и телекоммуникаций, в таком случае должен быть установлен и зафиксирован тип связи, используемая аппаратура, абонентский номер, позывной либо рабочая частота;

- разъединение с соблюдением всех мер безопасности и опломбирование их технических входов и выходов;

- определение вида упаковки и транспортировки изъятых предметов.

2) Упаковать технические устройства в виде персонального компьютера желательно в коробку, в которой она была приобретена, если, разумеется, она сохранилась.

3) Другие электронные носители цифровой информации, в виде дискет, лазерных дисков, USB накопителей и т.д. нужно упаковать отдельно друг от друга, т.е. каждый в свой конверт, коробку, специальную упаковку, либо завернуты в плотную бумагу, во избежание электромагнитных воздействий. Магнитный носитель информации целесообразно дополнительно обернуть в алюминиевую фольгу.

4) Технические устройства при отсутствии заводской тары упаковываются в ящики (желательно деревянные), где во внутренних перегородках используются прокладки из упругого материала (гофрированного картона, пенопласта, толстого слоя бумаги).

5) Упакованная техника и машинные носители должны быть опечатаны и снабжены удостоверительными надписями.

6) Транспортировка устройств вычислительной техники и машинных носителей информации осуществляется так, чтобы не допустить:

- механического воздействия на аппаратуру;

- влияния атмосферных факторов (дождя, снега и т.д.);

- воздействия электромагнитных излучений;

- влияния слишком высоких и низких температур, помня, что аппаратура, содержащая в себе носители информации, должна храниться в. диапазоне температур от 0 до + 50 градусов.

Все вышеизложенные аспекты желательно согласовать (по совету) со специалистом, во избежание утери изъятой информации. Вообще как видно

из тех действий, которые нужно предпринять для сохранности цифровой информации, с момента начала осмотра, изъятия, упаковке и транспортировке технических устройств и других носителей, показывает, что без специалиста сложно в полном объеме произвести обнаружение и закрепление данных оперативной памяти, правильно обращаться с техникой и энергонезависимыми носителями компьютерной информации. Каким бы не был профессиональный должностное лицо, ОУП, но без соответствующих знаний в технических средствах, все его действия по сбору доказательств может свестись к нулю. Возможно, на сегодня назрела нужда при осмотре компьютерной техники и изъятии их с места осмотра, в законе закрепить обязательное участие специалиста в этой области по аналогии с ч.1 ст.227 УПК РК «Порядок производства эксгумации».

При этом, казалось бы в качестве специалиста можно было бы пригласить эксперта из государственного учреждения или негосударственных организаций, но, это может повлиять на качество проводимых работы, затраты дополнительных бюджетных средств, а также утечку или утрату информации при досудебном расследовании. Поэтому, наравне с законодательной инициативой, во всех правоохранительных и специальных органах организовать специальные подразделения по противодействию с киберпреступностью, которые будут, занимается сбором цифровых доказательств. Фактически такие подразделения уже существуют в системе органов внутренних дел РК и называются «Отделами «К». Тем не менее, полагаем, что такие подразделения должны существовать во всех правоохранительных органах, более того, в образовательном процессе для сотрудников правоохранительных органов будь то послевузовское образовании или повышение квалификации должны передаваться знания в этом направлении, тем более, что в Академии правоохранительных органов при Генеральной прокуратуре РК существует подразделение, которая изучает и обучает в исследуемом нами направлений (Кафедра международного обучения в сфере противодействия глобальным угрозам (Региональный ХАБ).

С.А. Шейфер утверждает, что «объективной фиксацией результатов процессуальных действий служит институт понятых» [106]. Однако, по нашему мнению это не совсем так. Процедура формирования показаний от восприятия до передачи сведений у очевидцев, в данном случае понятых носит психологический характер. На психику человека влияют различные объективные и субъективные обстоятельства, которые отражаются на полноте и достоверности показаний. К примеру, человек спешил на работу, был болен и т.д. Поэтому на ровне с привлечением понятых правильно осуществлять видеосъемку от начала и до конца. В ст.82 УПК РК статус понятого отражен четко, он признан участником уголовного процесса, в главе «Иные лица, участвующие в уголовном процессе». Законодатель утвердил главную удостоверительную функцию понятого, ради, которых

привлекаются к участию в процессуальных действиях. Пункт 2 ч.3 ст.82 УПК РК закрепляет за понятым право участвовать в следственном действии и делать по поводу следственного действия заявления и замечания, подлежащие занесению в протокол. При проведении осмотра, обыска, выемки «компьютерной информации», исполнение требовании УПК обязательно, в части приглашения понятых, было бы еще лучше если бы они обладали хотя бы базовыми знаниями, лица, умеющие обращаться с компьютером, которые понимали бы смысл действий должностных лиц ОУП.

При участии специалиста, понятых, протоколировании и видеозаписи происходящих событии осмотра у сторон при рассмотрении уголовного дела и суда никогда не возникнут сомнения в достоверности и законности полученных при вышеуказанных процессуальных действиях доказательств.

Как отметил, М.Ч. Когамов «Безусловно, основная тяжесть собирания доказательств, приходится на органы, ведущий уголовный процесс, использующие властные полномочия по розыску и добыче информации, ее исследованию, в т.ч. посредством проведения широкого круга процессуальных действий». Нужно согласиться с мнением данного ученного, что «рядом с обвинением правозащитную деятельность ведут защитники и представители потерпевших, занимающие свое место при сборе доказательств» [107]. Предоставление доказательств один из способов обнаружения и получения информации, имеющих значение к делу, - это, как замечает В.Д. Арсеньев, «пассивная форма получения доказательств». Материалы поступают не по инициативе ОУП и суда, а волеизъявлению участников процесса, ими обладающими. Тем самым, реализуется возможность участников процесса влиять на ход досудебного и судебного рассмотрения, вносится вклад в установление истины. Полученная информация обрабатывается органом ведущий, уголовный процесс в части относимости их к делу, и в случае подтверждения приобщается к материалам дела или не подтверждения возвращается лицу, ходатайствовавшему к их приобщению. Опять же при предоставлении электронного носителя «компьютерной информации» требуется специальная техника, которая возможно не имеется у ОУП или суда, в данном случае возникает вопрос привлечение специалиста, а на досудебной стадии процесса еще и понятых, которые удостоверят факт передачи и наличия имеющейся информации на этом носителе [108].

Рассмотрим сбор доказательств, при применении цифровой информаций имеющихся в бортовых компьютерах автомобилей, т.е. электронных систем безопасности и управления транспортного средства при ДТП. Только 9 месяцев 2019 г. совершены 11626 ДТП, повлекших гибель или ранение людей. Из них по видам: автомобильные аварии – 5900, столкновение с пешеходом – 4781, другое ДТП – 945. По типу транспорта: частный – 10911 и общественный – 715. На момент совершения ДТП состояние водителей: трезвое – 9649, в алкогольном опьянении – 517,

наркотическом опьянении – 8, токсикоманическом опьянении – 1, резкое ухудшение здоровья – 16 и по 1423 водителям состояния в статистических данных не указано. Превышавшим и время непрерывного нахождения в пути 12 водителей [109].

Показанная статистика с каждым годом только растет, и каждый факт нарушения правил дорожного движения повлекших гибель или ранение людей, требуют дательного изучения для установления всех фактов ДТП.

ДТП отличаются не только значительной распространенностью и повышенной общественной опасностью, но и сложностью расследования. Одной из причин, обосновывающей сложность расследования является не только качественная оценка происшествия, но и установления конкретных данных, характеризующих скорость и траекторию движения транспортных средств, расположение участников дорожного движения во время происшествия, видимость водителя и другие обстоятельства. При определении механизма ДТП одним из основных элементов является установление объективных параметров движения транспортного средства при ДТП и перед ним. Данные, как правило, можно получить путем опроса участников и свидетелей события. Однако участники ДТП являются заинтересованными лицами и зачастую умышленно искажают реальную картину в своих интересах. На восприятие ДТП его участниками, свидетелями влияет множество как субъективных, так и объективных факторов. Поэтому как мы уже отмечали, полученные таким образом данные не могут быть полными, при которых возможно установление конкретного обстоятельства происшествия ДТП и создание его объективной модели. Одним из перспективных путей решения проблем, связанных с получением объективной доказательственной информации при расследовании ДТП, на наш взгляд, является исследование данных бортовых компьютеров автомобилей. К электронным системам безопасности и управления транспортным средством относятся модули пассивной системы безопасности (SRS), активных систем безопасности (ABS, ASR, ESP и т. д.), систем защиты (антиугон и т. д.), систем обеспечения комфорта, а также электронный блок управления автомобилем, т.е. бортовой компьютер. Как правило, указанные системы обеспечения безопасности транспортного средства взаимосвязаны, соединены с единой сетью и контролируются бортовым компьютером автомобиля, поэтому система устройств, указанная в руководстве по эксплуатации некоторых современных автомобилей, определяется как «мультиплексная сеть».

Во всех автомобилях, оборудованных подушками безопасности, управление ими осуществляется блоками управления Airbag (SRS). Конструкция многих современных блоков включает в себя регистратор данных о событиях Event Data Recorder EDR (другое название Collision Data Recorder, CDR. Управление SRS осуществляется микроконтроллером –

специальной микросхемой со своей постоянной электронной памятью и способной выполнять встроенные в него программы.

Размер информации, закрепленной модулем EDR, зависит от конструкции и комплекта транспортного средства, но содержит по меньшей мере следующие данные: - скорость движения транспортного средства; - частота вращения коленчатого вала; - значение резкого изменения скорости в продольном и поперечном измерениях дельта-V (потеря скорости удара); - состояние педали акселератора и дросселя; - состояние тормозной педали; - цикл зажигания; - статус ремня безопасности водителя, пассажиров; - наличие масс на стульях; - статус срабатывания подушки безопасности, время и этапы развертывания; - АБС, ESP, статус системы контроля давления на шинах; - работа средств наружного освещения; - статус и показатели активных систем безопасности (при их наличии).

Некоторые модули EDR ведут непрерывную запись данных до прекращения записи в результате ДТП, другие активируют запись в определенных случаях, признаваемых модулем, как столкновение (например, внезапное резкое изменение скорости, резкое торможение, срабатывание датчиков удара). При этом информация в модуле памяти хранится до его перепрограммирования (переплетения). Многолетние исследования и испытания, проводимые национальной администрацией безопасности дорожного движения США (NHTSA), подтвердили надежность и высокую точность данных, закрепленных модулями EDR, и эти данные придают большое значение при определении обстоятельств и механизма ДТП.

Кроме того, автомобили, оборудованные автоматической коробкой передач, имеют собственную память в электронном блоке управления АКП, который, кроме первичной информации об автомобиле, его идентификационном номере (VIN), номере коробки передач и заводских параметрах, регистрирует информацию о его сервисной деятельности, движении автомобиля, возникновении неисправностей или нештатной работе отдельных его частей. Сведения о работе тормозной системы транспортного средства, имеющего какое-либо криминалистическое значение, могут быть зарегистрированы в памяти модуля управления системой анти пробуксовкиабс (ABS). Информация о параметрах движения транспортных средств во время ДТП не регистрируется не всеми системами пассивной безопасности (SRS), а только с функцией записи (EDR). Но это не означает, что в случае отсутствия модуля EDR на транспортном средстве электронный блок управления будет абсолютно бесполезен для выяснения обстоятельств, происшествия и доказать по досудебному расследованию. При отсутствии модуля EDR либо аналогичных устройств, работающих по принципу «черного ящика», ЛЭП не осуществляет постоянное закрепление показаний всех датчиков и систем транспортного средства, работающих в исправном, штатном режиме. При получении сигнала датчиков какой-либо

системы о возникновении неисправности он записывается в памяти ЭГУ. Фиксируется код возникшей неисправности, время ее возникновения, данные о возникшем пробеге. Соответственно, анализ информации, содержащейся в памяти ЭГУ: позволяет объективно установить VIN транспортного средства, его техническое состояние до ДТП. Анализ кодов неисправностей, их расшифровка, определение хронологии и последовательности их возникновения в совокупности со следовой картой на месте совершения ДТП и другими доказательствами по делу позволяют полностью определить механизм происшествия, моделировать его. Анализ данных ЭТС позволяет объективно подтвердить факт осведомленности водителя о техническом неисправности транспортного средства в случае возникновения аварийной ситуации по причине неисправности транспортного средства, которую водитель может обнаружить перед или входе эксплуатации. Речь идет о неисправностях, сообщающих водителю ЭБУ с подачей звукового сигнала и освещением соответствующего графического изображения на приборной панели. Важнейшая особенность большинства блоков управления они оснащены энергонезависимой памятью. Соответственно, при повреждении аккумуляторной батареи, отключении автомобиля системой обеспечения безопасности или умышленным водителем, информация, ранее зарегистрированная в ЭКУ, сохраняется в его памяти и может быть удалена только при перепрограммировании модуля. Кроме того, индикаторы неисправностей на приборной панели транспортного средства могут быть отключены после отключения и включения источника питания.

Очевидно, что использование информации, зарегистрированной электронными системами управления комфортностью и безопасностью транспортного средства при расследовании ДТП, позволит более полно, объективно и беспристрастно установить механизм происшествия, роль и влияние водителя транспортного средства на ход его развития. Однако, нельзя не согласиться с мнением сотрудников Центра исследования дорожно-транспортного травматизма США (CenterforInjuryResearch, CfIR) о том, что такие данные требуют своего подтверждения и должны рассматриваться вместе с другими доказательствами, собранными по делу.

Например, при исследовании Центром, установлено, что модуль EDR допускает регистрацию неправильной информации о пассажирах в транспорте. При применении водителем экстренного торможения перед столкновением с препятствиями пассажир подается вперед по инерции. Давление на сиденье ослабляется. Датчики пассажирских сидений не устанавливают вес пассажира или устанавливают меньший и соответственно EDR фиксируют его отсутствие при ДТП или идентифицируют его как ребенка, в результате не срабатывают подушки безопасности.

При определении скорости движения транспортного средства при ДТП нужно учитывать, что скорость определяется от датчика выходного вала коробки передач путем анализа данных EDR. Соответственно, в случае применения водителем тормоза на автомобиле, не оборудованном АБС, колеса блокируются. Поэтому скорость движущегося автомобиля «юзом» будет равна нулю с момента блокировки колес. Поэтому скорость транспортного средства, осуществляющего движение при занавесах и разворотах, не соответствует фактическим показателям и показателям изменения скорости. Показатели скорости транспортного средства, оборудованного АБС, практически точно соответствуют.

Несмотря на указанные недостатки, скорость движения транспортного средства на момент обнаружения водителем опасности при расследовании ДТП имеет первостепенное значение, а сам происшествие немедленно, поэтому при минимальном объеме времени регистрации событий этот показатель скорости фиксируется модулем EDR.

В условиях максимальной компьютеризации автомобиля, оснащения его современными активными средствами безопасности, способными вмешиваться в процесс управления транспортным средством, данные, зарегистрированные в EDR, имеют большое значение не только для установления объективных параметров движения транспортного средства, но и для определения конкретных причин возникновения и влияния электроники на развитие аварийной ситуации.

Анализ следственно-судебной практики установление параметров движения транспортного средства при ДТП в нашей стране путем чтения информации из электронного блока управления или модуля EDR носит эпизодический характер и вызывает множество трудностей. При осмотре места происшествия, как правило, информации о наличии этих устройств, в транспортном средстве отсутствует. Такая информация позволяет диагностировать транспортное средство. В свою очередь, для диагностики указанных бортовых систем и снятия с них зафиксированной информации требуется специальное оборудование, которое отсутствует у следователя. В большинстве криминалистических подразделений нет соответствующего оборудования. Решение проблемы это приглашение специалиста из числа ведущих сотрудников официального сервисного центра, обслуживающих автомобили конкретных марок, на проверку транспортного средства. Но это не всегда положительный результат. Сервисные центры часто ссылаются на отсутствие нужного оборудования и специалистов.

В качестве положительного примера использования помощи специалиста при расследовании ДТП можно привести опыт Чехии, где в соответствии с соглашением полиции с автомобильным концерном «Skoda» по каждому случаю ДТП могут выезжать специалисты концерна на место происшествия с участием данных авто производящих автомобилей, которые получают и раскрывают информацию от различных датчиков и электронного

блока управления. Данные используются для последующего определения механизма ДТП и компьютерного моделирования средств авто ремонта.

Кроме того, оборудование и соответствующее программное обеспечение для снятия и шифрования данных из модулей EDR редко находятся в ведении экспертов, что связано с индивидуализацией модулей EDR каждого производителя, различными форматами записи информации и различиями типов разъединителей диагностических и служебных шин этих модулей. Для получения и обработки данных из модулей EDR могут использоваться соответствующие универсальные комплексы. Например, в комплект фирмы Vetronix входит более 80 видов дата-кабелей, подключаемых для всех видов разъемов диагностических и служебных шин штатных модулей управления подушками безопасности с функцией записи. Аналогичные комплексы разработаны фирмой Bosh. Аппаратно-программный комплекс «BOSH Crash Dataretrieval Tool» обладает всем нужным оборудованием для получения и визуализации информации, содержащейся в электронных системах управления транспортным средством.

Еще одним электронным устройством, фиксирующим существенную информацию для расследования ДТП, является штатные навигационные системы, установленные на многих современных автомобилях.

Штатная навигационная система устанавливается на автомобильном заводе и обычно является частью мультимедийной или головной системы. Основу каждого навигатора составляют: само устройство с установленным приемником GPS (ГЛОНАСС), программное обеспечение и карты для навигатора. С точки зрения возможности получения аргументированной информации важно наличие функции записи треков на многих современных навигаторах (последовательность фиксированных точек координат, отражающих всю пройденную строку). Точки трека содержат информацию о текущих координатах и времени. Некоторые модели также включают описание высоты над уровнем моря. Скорость рассчитывается по данным координат соседних точек и промежуткам времени между ними.

Запись треков на простых моделях навигаторов осуществляется автоматически и пользователь не доступен для редактирования. Трек всегда пишется. При заполнении «новой» памяти циклические данные записываются над старыми данными. Современные и функциональные модели предлагают пользователю несколько режимов записи: Данные OFF-трека не записываются. Этот режим автоматически включается при загрузке трека с компьютера; WRAP-запись постоянного трека. При заполнении памяти новые данные протирают старые данные; FULL-Остановка записи при заполнении памяти. При оставлении свободного места в памяти на экране отображается соответствующее уведомление. Как правило, доступ к информации, содержащейся в памяти штатной навигационной системы, осуществляется подключением соответствующего

оборудования к диагностическому отключению автомобиля. К сожалению, главная проблема, как при использовании данных EDR в доказательстве информации, содержащейся в памяти навигационных систем, – это отсутствие в экспертных подразделениях соответствующего оборудования для получения этой информации и программного обеспечения для ее анализа.

Мы видим «положительный опыт использования информации электронных систем управления, безопасности и комфорта автомобилей стран Европы и северной Америки в целях установления обстоятельств ДТП. Компьютеризация транспортных средств, оснащение их IT-технологиями, способными вмешиваться в процесс управления автомобилем, на наш взгляд, убеждает в развитии технологий использования записей электронных бортовых систем при расследовании уголовных дел связанных с ДТП» [66].

В этой связи, предлагаем дополнить главу 11 Доказательства УПК РК ст.120-1 «Цифровая (компьютерная) информация» в следующей редакции:

Статья 120-1 «Цифровая (компьютерная) информация».

1. Цифровая (компьютерная) информация используются в качестве доказательств, если имеет значение для разрешения уголовного дела.
2. При обнаружении цифровой (компьютерной) информации имеющей значения для дела, ОУП принимают меры для их осмотра, выемки или копирования на электронный материальный носитель в целях сохранения и использования в качестве доказательств, о чем составляется протокол.
3. Осмотр цифровой (компьютерной) информации производится с участием специалиста и понятых, с обязательной видео фиксацией происходящих событии, при этом выемка и копирование компьютерной информации осуществляется по правилам главы 31 настоящего Кодекса.
4. Изъятая цифровая (компьютерная) информация, вместе с протоколом приобщается к материалам уголовного дела и хранится до окончательного разрешения уголовного дела.

Таким образом, проведенные исследования цифровых доказательств, цифровой информации, их механизма образования и носителей наводят на мысль о необходимости ее введении в качестве самостоятельного вида доказательств, что позволит эффективно применять электронно-цифровую информацию в процессе доказывания.

2.2. Исследование (проверка) цифровой информации в уголовном процессе

Проверка доказательств это второй элемент процесса доказывания в уголовном процессе, которые неразрывно связаны между собой, поэтому этот элемент невозможно отделить от собирания и оценки. Ожегов С.И. отмечал, что «проверить» есть «удостоверение в правильности» чего-нибудь

либо «подвергнуть испытанию для выяснения» чего-нибудь[110]. Обратим внимание, что в УПК РК отсутствует этап проверки, как это отражено в ст.87 УПК РФ, этот термин заменен на слово синоним «исследование».

Ожегов С.И. в первом случае отсылает «исследование» на «исследовать», во втором отражает, что это «научный труд. И. по русской истории». В свою очередь, «исследовать, дую, - дуешь, - анный; сов. и несов., кого- что. 1. Подвергнуть (-гать) научному изучению. И. законы природы. 2. Осмотреть (осматривать) для выяснения, изучения чего-н. И. больного». В этом случае, все встает на свои места, исследование о котором идет речь в ст.124 УПК РК, - это мыслительно-логический и иной процесс, осуществляемый для установления достоверности или недостоверности собранной информации, опровержение либо подтверждение определенных фактов и событии.

М.Ч. Когамов отмечает, что «исследование осуществляется практически после каждого случая обнаружения, закрепления и изъятия, т.е. сбора нового доказательств» [107]. В свою очередь, соглашаясь с его мнением, мы полагаем, что исследование начинается с самого начала доказывания и продолжается на протяжении всего досудебного и судебного разбирательства, вплоть до окончания рассмотрения уголовного дела в кассационной инстанции в ВС РК, где ставится окончательная точка. Если только не учитывать право обращаться гражданам в Международные организации, которые отражают о соблюдении либо несоблюдении судами РК международных принципов правосудия, и в случае отражение их несоблюдения, возможно повторное рассмотрение дел в ВС.

Проверке доказательств в различных стадиях досудебного и судебного производства по уголовным делам есть свои особенности. На первоначальном этапе эта процедура по нашему мнению сложная, поскольку имеются лишь отдельные факты, отражающие наличие признаков уголовного правонарушения, и у ОУП нет полной картины произошедших событии. Поиск истины на этом этапе происходит в условиях ограничения ряда принципов уголовного процесса, таких как: гласность, непосредственность, состязательность и равноправие сторон. Как не печально, это признавать, но на результаты деятельности досудебного расследования по исследованию доказательств возможно оказание влияния прокурором, начальником органа дознания или следственного отдела, которые могут быть как положительными для расследования уголовного дела, так и отрицательными.

В процессе проведения процессуальных действии на стадии досудебного расследования у ОУП нет нужды привлекать всех субъектов процесса, что дает возможность должностному лицу, ведущему уголовный процесс направлять ход расследования в удобную ему струю, которое не всегда возможно выявить на стадии предания суду. Хотя при предании суду, возможно, проверить основные обстоятельства. К примеру, потерпевший на

первоначальном этапе указывает прямо на правонарушителя, в последующем отражает о сомнениях, что это он, а за тем и вовсе отрицает о наличии его опознания.

Вместе с тем, в судебном разбирательстве все нестыковки по делу сразу же выявляется, поскольку именно в условиях непосредственности, состязательности, открытости и равноправия сторон создаются благоприятные условия для исследования доказательств. Возможно - это связано, что суд, самостоятельный и независимый субъект уголовного процесса и не связанный с деятельностью уголовного преследования и защиты. В суд поступают доказательства, как от обвинения, так и защиты, что дает возможность сформировать полную картину произошедших событий, выявляются все факты, оказывающие влияние на результаты исследование доказательств. Суд в процессе разбирательства предоставляет всем сторонам участвовать в исследовании доказательств, а также предоставлять их для исследования суду.

«Оглашение показаний полученных в ходе досудебного производства по делу, а также воспроизведение приложенных к протоколу допроса звукозаписи, видеозаписи или киносъемки, их показаний и ссылка на них в приговоре возможны только в случаях, предусмотренных ст.ст. 368 и 372 УПК. Фактические данные, содержащиеся в этих показаниях, могут быть положены в основу выводов суда только после их проверки, всестороннего исследования и подтверждения в главном судебном разбирательстве». «Приговор является законным, если он постановлен законным составом суда с соблюдением правил подсудности, в точном соответствии с требованиями УПК о процедуре судебного разбирательства на основе принципа состязательности и равноправия сторон с обеспечением их доступа к исследованию доказательств на равных основаниях, при условии правильного применения норм права» [111].

Цель доказывания состоит в достоверном выявлении обстоятельств, входящих в предмет доказывания, следовательно, нужно собрать, исследовать и оценить систему доказательств, достаточных для установления каждого элемента предмета доказывания.

По мнению Ю.В. Худяковой «целью проверки доказательств является всестороннее и полное уяснение качеств и свойств самих проверяемых доказательств, а также поиск, накопление и анализ знаний о свойствах, связях и отношениях действий и событий, устанавливаемых данным доказательством с самим доказательством» [44].

Наверно нужно конкретизировать это определение, тем, что под полным осознанием качеств и свойств доказательств, служит исследование их достоверности, т.е. соответствии или несоответствии содержащихся в них сведений фактам и обстоятельствам, имеющим значение для правильного разрешения уголовного дела, а также допустимости доказательств на соответствие их формы закону.

Исследование «компьютерной информации» предполагаем сложным элементом, т.к. в энергонезависимых носителях, т.е. электронных внешних носителях, количество файлов исчисляются десятками тысяч, разные системные файлы, программы и т.д. Информацию можно спрятать, зашифровать и уничтожить, но при исследовании возможно применение различных программ осуществляющие поиск компьютерной информации, которые выявляют и восстанавливают ее. Сейчас множество различных программ восстанавливающие удаленные данные, к ним относятся: «Hetman Partition Recovery », «R-Studio», «Wondershare Data Recovery», «Recuva», «Pandora Recovery», «PC INSPECTOR», «GetDataBack»,

«MiniTool Power Data Recovery», «Recover My Files». Выбирая программы для восстановления данных нужно обратить внимание на характеристики и какие из них, требуется восстановить, при этом, использовать нужно в обязательном порядке ее лицензированную версию, которые как правила приобретаются на платной основе. В любом случае, по нашему мнению этим должен заниматься соответствующий специалист, имеющий знания в области компьютерной информации.

Статья 124 УПК РК конкретно не отражает субъектов исследующих доказательства, но, ими могут быть только органы ведущие уголовный процесс, на досудебной стадии это прокурор, следователь и дознаватель, на судебной только суд, остальные участники процесса как мы отметили, в предыдущем подразделе могут заявлять различного рода ходатайства, связанных с исследованием доказательств. Глава 13 УПК РК предусматривает возможность ходатайствовать перед органом, ведущим уголовный процесс произвести определенное процессуальное действие и в случае несогласие с их решением обжаловать действия (бездействия) и решений госорганов и должностных лиц, осуществляющих производство по уголовному делу.

Исследование доказательств возможно путем сопоставления их с другими сведениями, добытых при досудебном и судебном расследовании, выявления достоверных источников, приобретение любых других доказательств, как подтверждающих, так и опровергающих проверяемое доказательство. Интересным является тот факт, что исследование доказательства практически возможно как при проведении научного исследования, используются познавательные и логические операции как анализ и синтез для установления их полноты, непротиворечивости, логической последовательности изложения сведений. В последующем формы и направления исследования, а также стороны, которые нужно сопоставить с другими строго определенными доказательствами.

Анализ доказательств, представляет их всестороннюю проверку, без привлечения других имеющихся в уголовном деле информации, при работе с «компьютерной информации» нужно визуально воспроизведение и выяснения ее содержания. Ее методы могут быть разнообразными - от

простого визуального воспроизведения до сложнейших инструментальных и аналитических методов, применяемых при производстве экспертизы. К примеру, в первом случае прочтение текста, во втором, восстановление удаленной информации с помощью одной из вышеуказанных программ. Вместе с содержанием компьютерной информации, нужно анализировать ее реквизиты, такие как: тип файла, объем, дата создания, изменения, открытия и т.д. Ю.К. Орлов утверждает, что «проверка доказательств является таковой только в отношении проверяемых доказательств, для проверяющих это сбор» [50]. К примеру, производя экспертизу энергонезависимых носителей цифровой информации, самой техники, в результате этих исследований экспертом проводится поиск новых сведений.

После анализа цифровой информации, доказательство вновь исследуется, но уже как единое целое всех его отдельных частей с учетом установленных признаков и особенностей, такие доказательства можно получить только синтезом.

Анализ и синтез доказательств дает органу, ведущий уголовный процесс обнаружить дальнейшее направление и формы исследования, т.е. те стороны, которые нужно сопоставить с другими строго определенными доказательствами. По С.И. Ожегову сопоставить означает «рассмотреть, обсудить, сравнивая с чем-нибудь для получения какого-нибудь вывода» [110, с.650]. В случае сопоставления доказательств, А.П. Рыжаков отмечает, что «сравнивание информации, содержащихся в различных доказательствах, в целях прийти к выводу об истинности, содержащейся в проверяемом доказательстве информации или же в ее полной либо частичной недостоверности» [112]. Интересную мысль выражает А.В. Смирнова, по его мнению «проверка доказательств имеет место только, когда речь идет о физическом сопоставлении предметов, в случае сопоставления сведений имеет место мыслительного характера, которая уже является оценкой доказательств» [113]. Л.В. Головко согласен с мнением А.В. Смирнова, подчеркивая, что «сопоставление доказательств это ее оценка, в особенности, когда это касается оценки всей совокупности доказательств» [114].

Другие ученые, не исключат сопоставление из элемента исследования, по их мнению, процесс не завершается после его сравнения с той информацией, которыми обладали ОУП на момент, когда исследуемое доказательство собрано. При появлении в деле новой информации, процесс сопоставления повторяется. Применение этого способа исследования доказательств завершается после сопоставления с последним доказательством, полученным по конкретному уголовному делу, позволяющие установить достоверность или же недостоверность, хотя бы в части проверяемой информации [112, 115].

ОУП или суд, на основе сопоставления нескольких доказательств, взаимно согласующих через определенные факты, приходят к тому, что

информация об уголовном правонарушении, которые они несут в себе, действительны. Доказательства могут проверяться в момент их получения (пример: путем уточняющих вопросов специалистам и т.д.) при досудебном и судебном рассмотрении дела по мере поступления дополнительных сведений их исследовании.

В исследовании цифровой информации особым значением служит соответствующее разъяснение специалиста в этой области. Т.В. Аверьянова при рассмотрении заключения и показании специалиста отмечает, что «вопросы, поставленные любой из сторон перед специалистом, должны носить не оценочный, а проверочный характер». К примеру: «достаточно ли представленных материалов, с учетом их качества для всестороннего исследования?», «отвечали ли использованные методы и методики требованиям надежности, достоверности получаемых с их помощью результатов?», «какие методы целесообразно использовать в данном исследовании?» По ее мнению, «сведения, сообщаемые специалистом об обстоятельствах, требующих специальных знаний, - это его консультативная деятельность. Консультации могут касаться как общих положений науки, техники, искусства, ремесла, так и конкретного их приложения к обстоятельствам дела. К примеру: «достаточно ли в материалах дела о ДТП данных для решения вопроса наличия технической возможности водителем избежать аварию. В случае не достаточности, какие дополнительные материалы требуются для решения этого вопроса» [116]. Мы согласны с ее позицией, что допрос эксперта или специалиста возможен только в рамках проведенных ими исследовании, т.е. после дачи соответствующего заключения, по этой причине, законодатель обезопасил их, предусмотрев в ч. 3 ст. 285 УПК РК запрет на допрос до дачи ими заключения.

Консультации специалиста по нашему мнению с начала сбора, изъятия и проведения исследования цифровой информаций необходимо, иначе ОУП не понимающий в этом деле ничего, не будет знать, что искать. Первоначально специалист принимает меры по правильному изъятию информации, после исследует ее, где его знания по вопросам полученных данных облекается в форму заключения, в случае, неясностей орган, ведущий уголовный процесс, вправе допросить специалиста. Так, допрос эксперта и специалиста производится с целью:

1) выяснения связанных с заключением эксперта или специалиста существенных для дела вопросов, не требующих дополнительных исследований;

2) уточнения примененных судебным экспертом или специалистом методов и использованных терминов;

3) получения информации о других фактах и обстоятельствах, не являющихся составной частью заключения, но связанных с участием в досудебном процессе эксперта или специалиста;

4) выяснения квалификации судебного эксперта или специалиста [5].

Пример: на досудебной стадии уголовного процесса производился осмотр интернет-сайта, на нем размещалась цифровая информация, предлагаемая для продажи и распространения. Информация, авторами сайта, предназначалась для получения удаленного доступа к чужому компьютеру и сбору конфиденциальной информации, которая скопирована специалистом на электронный жесткий диск и для установления содержания в ней вредоносных программ, приводящих к удаленному не санкционируемому доступу к чужому компьютеру, проведено исследование и дано заключение. Специалист в заключении подтвердил, что компьютерная информация используется для «взломов» чужих компьютеров и хищения информации. Между тем, специалист при исследовании применял определенные термины, которые не ясны простому обывателю, в связи с чем, орган, ведущий уголовный процесс произвел его допрос в присутствии сторон для надлежащего исследования.

В понятии доказательств нужно выделить две неразрывно связанные стороны - содержание и форму. Под содержанием понимаются сведения, устанавливающие наличие или отсутствие обстоятельств, подлежащих доказыванию. То, в каком виде содержатся эти сведения, будем считать формой. Допустимые формы доказательств перечислены в ч. 2 ст. 111 УПК РК. Эти два элемента неделимы, т.к. не существует информации, вне материального носителя. Несмотря на это, Ю.К. Орлов настаивает на таком разграничении, утверждая, что «форма и содержание проверяются и оцениваются, как правило, порознь, поскольку к ним предъявляются разные требования. Например, относимость - это свойство содержания, а допустимость - свойство формы. В одном и том же источнике могут содержаться сведения о различных фактах, которые оцениваются по-разному. Возможна и обратная ситуация, когда об одном и том же факте содержится информация в различных источниках. Поэтому форма и содержание - обычно подлежат раздельной проверке и оценке. Ученый, справедливо замечает, что несмотря на единство и неразрывную связь формы и содержания, нужно, когда речь идет о доказательствах, выделение той или другой его стороны» [50].

Один из критериев исследования доказательств, служит выявление их источника. Изучая причину происхождения информации, а затем соответствие одних сведений, в последующем доказательств, имеющихся в деле с другими сведениями. Широкое распространение в теории доказывания получило представление о том, что источником доказательства является процессуальная форма, сохраняемые и используемые сведения, полученные органам, ведущим уголовный процесс, из показаний, заключений, вещественные доказательства, протоколы и иные документы (ч. 2 ст. 111 УПК РК). Поэтому авторы делают вывод о невозможности отделения сведений, составляющих содержание доказательства, от источника, т.е. его процессуальной формы. Ученые-процессуалисты,

занимающиеся проблемами доказывания и доказательств, ставят вопрос о неясности термина «источник доказательств» [117].

По этимологическому смыслу «источник - это то, что дает начало чему-нибудь. Откуда исходит что-нибудь» [110]. С.В. Курылев отметил, что «никто не объяснил, почему процессуальная теория должна отступать от этого смысла, называть источником не свидетеля, из которого истекает показание, а само показание, из которого ничего не «истекает». По этой причине, С.В. Курылев «называет источниками доказательств, свидетелей и иных лиц, от которых поступают сведения о фактах, имеющих значение для дела, и материальные предметы, несущие информацию» [118]. В.Я. Дорохов ограничивает круг источников доказательств лишь субъектами: «свидетелями (понятыми), потерпевшими, обвиняемыми, подозреваемыми, экспертами [119]. Похожая позиция об источниках доказательств осветила В.Д. Арсеньевым, который относит к ним лиц, а также документы, место обнаружения и изъятия вещественных доказательств [81].

С.А. Шейфер утверждает на неоправданность раскрытия понятия «источников доказательств» в перечисленных в ч.2 ст.111 УПК РК. Он связал это: 1) с логическими познавательными аспектами доказывания; 2) с неадекватностью понятий «источник» и «форма» доказательств. При этом, предлагая, обозначенные в ч.2 ст.111 УПК РК, отражать не источниками, а видами доказательств [120].

Такую позицию, мы разделяем в нашей диссертации «компьютерную информацию» рассматриваем и предлагаем как новый вид доказательств. Форма «компьютерной информации» будет электронно-цифровая форма на материальных носителях, т.е. информация зафиксирована на электронных цифровых носителях. В целях выявления источника «компьютерной информации» нужно анализировать сам термин «источник доказательств» в уголовном процессе. Как мы видим, определение «источника доказательств» до настоящего времени остается дискуссионным.

Противоположная точка зрения В.Д. Арсеньеву, В.Я. Дорохову, С.В. Курылеву, С.А. Шейферу, гласит, что процессуальным носителем информации, полученной и приобщенной к делу в виде доказательств, либо иной, более принятой в теории уголовного процесса терминологии, источником доказательства выступают не люди и/или предметы, а процессуальные акты. В них зафиксированы сообщенные субъектами или обнаруженные на предметах информация, имеющие значение для дела. Исключение составляют документы, для которых материальный и процессуальный носители информации нередко совпадают. К примеру, приобщенная к уголовному делу бумага, сохранившая на себе информацию.

Убедительна позиция у М. Шалумова: «истина в споре между противниками двух приведенных точек зрения находится, как всегда, посередине. Доказательство и его источник - разные понятия, т.к. в первом случае речь об информации, во втором - о его носителе. С другой стороны,

информация не может существовать отдельно от носителя. Способы и порядок сбора, закрепления и исследование доказательств определяют не содержание и даже не форма, а их юридическое свойство - допустимость, позволяющее оперировать ими в процессе доказывания» [121].

Например, протокол осмотра мог бы подробно и правильно отражать проведение процессуального действия, быть хорошо оформлен, но осмотр произведен с грубым нарушением законом процедуры, без понятых. Поэтому нужно помнить о неразрывной связи между доказательством, его источником и процедурой получения информации из их материального носителя, но никак не о том, что все перечисленное охватывается одним понятием доказательства. Разделение термина «доказательств» и его «источника» имеет теоретическое и практическое значение: 1) Законодатель одним из способов исследования доказательств называет в ст. 124 УПК РК «проверку источников получения доказательств». Значит, для правильного применения этой нормы и обеспечить проверку доказательств, нужно понимать, что же служит их источником; 2) Разделение позволит органам, ведущий уголовный процесс правильно излагать доказательства, положенные в основу обвинения либо приговора, не подменяя содержание формой. Правильно воспринимать выводы, содержащиеся в процессуальных документах, субъектами, знакомящимися с ними.

Исследование доказательств, предполагает выяснения их механизма образования, достоверности источника и их содержания. Б.Д. Завидов, Н.П. Кузнецов отмечают, что «определение доброкачественности источника - это предмет проверки, а не способ. Следовательно, будет правильней говорить о проверке доказательств и их источников. Для определения допустимости доказательства является выяснение доброкачественности источника, а качества источника - для решения вопроса о достоверности полученных из него сведений» [122]. По логике С.А. Шейфера, «источником компьютерной информации служит аппаратные и программные средства. Проверка этого источника заключается, в выяснении исправности оборудования, с которого либо при помощи чего снята компьютерная информация, а также корректно ли работало программное обеспечение.

В юридической науке есть точка зрения, о пересмотре трехзвенной структуры процесса доказывания, из которой предлагают исключить проверку (исследование) доказательств. Л.В. Головко отражает: «...проверка доказательств полностью растворяется в собирании и оценке доказательств - двух подлинных и классических элементах доказательственной деятельности. По этой причине, не является проверка доказательств самостоятельным элементом процесса доказывания, даже теоретически» [123]. Но при этом, он полагает, что нельзя исключать третий элемент доказывания совсем, поскольку, процедура исследования доказательств, при рассмотрении в суде не охватывается собиранием и оценкой доказательств, представляя собой исследование доказательств. Как бы то ни было, мы не

согласны с позицией Л.В. Головко, даже считаем не применимой ее к цифровой информации, и исключать элемент «исследование доказательств» нельзя со стадии досудебного и судебного расследования.

В соответствии с п.9 ч.3 ст.77 Конституции РК «не имеют юридической силы доказательства, полученные незаконным способом. Никто не может быть осужден лишь на основе его собственного признания» [124]. Поэтому, становится понятно, что «допустимость является первоочередным свойством доказывания, вытекающее из требования соблюдать правовые акты субъектами, осуществляющими сбор, закрепление и исследование «источников доказывание».

Законодатель, установив порядок формирования доказательство, преследовал единственную цель, которою служит защита прав и свобод индивида. К сожалению, выполнение ОУП и судом требования закона не означает полностью достоверными доказательствами, поскольку свидетель умышленно может сообщить заведомо ложные показания или заблуждаться в отдельных моментах, надлежащим образом изъятая «компьютерная информация» может быть изначально сфальсифицирована, чтобы направить правосудие по ложному следу. О достоверности полученной информации можно судить только после изучения ее источника, материального носителя. Каким образом можно проверить компьютерную информацию? 1) Механизм возникновения: каким техническим устройством создано; какие программы использовались; 2) Просмотр контента и ее реквизитов; 3) Проверка соответствия доказательств в виде цифровой информации требованиям допустимости. Оно относится к досудебной и судебной стадии. При исследовании нужно получить ответ на вопрос о достоверности информации, находящиеся в проверяемых доказательствах.

По мнению С.А. Шейфер: «Каждое доказательство должно быть проверено и поддаваться проверке» [125]. А.В. Кудрявцева полагает, что «одним из признаков допустимости и достоверности доказательств должна быть проверяемость сведений» [126].

Полагаем, что вышеуказанное мнение по проверке доказательств относится и к исследованию «цифровой информации». Н.А. Зигура предложила соблюдать следующие требования при проверке компьютерной информации: возможность выяснение технического средства, с которой получена или скопирована информация; проверка соответствия типа, модели, фирмы изготовителя материального носителя этой информации с параметрами, указанными в протоколе процессуальных действия, в заключениях специалиста или эксперта; установление программного средства, с помощью чего получена информация. Тут нужно выделить несколько аспектов: 1) какое программное средство использовалось для формирования (создания) информации, например, создание регистрирующих журналов событий происходит посредством работы операционной системы; 2) какое программное средство использовалось для

копирования, если информация скопирована на другой носитель; 3) какой программой надо пользоваться для воспроизведения информации. Отражение в протоколе характеристик программных средств, например, нужно указать тип операционной системы, регистрационный номер; 4) выяснение реквизитов компьютерной информации, таких как тип файла, объем, время создания, время редактирования, время открытия, сведения о пользователе; 5) каким образом обеспечено условие целостности (неизменности) данных. Указать, какие программные средства используются для обеспечения целостности данных в протоколе[10].

Во все времена одним из основных критериев проверки доказательств, служило выявление других дополнительных доказательств, подтверждающих либо опровергающих проверяемое доказательство. Во многих случаях на практике, эта проверка производится проведением процессуальных действий.

При проверке доказательств вопросы о доказанности или недоказанности различных обстоятельств дела непосредственно не рассматриваются, но закладывается основа для их последующего разрешения. Результаты проверки должны отражаться в материалах уголовного дела, как правило, обобщаясь в обвинительном заключении и приговоре. В свою очередь, нельзя ограничиваться только указанием на источники доказательств, требуется расписывать их содержание и результаты, как это сейчас в судебной практике и требует ВС в отдельных ее постановлениях.

Таким образом, исследование цифровой информации требуется с помощью надлежащего технического оснащения и квалифицированного специалиста, который сможет объяснить всем участникам процесса, в особенности органам, ведущий этот процесс о происхождении, содержании и другие данные о рассматриваемой информации.

2.3. Оценка цифровой информации в уголовном процессе

Начнем рассмотрения заключительного элемента процесса доказывания, им является оценка собранных доказательств, заключаемая в выяснении способности объективно удостоверять юридически значимые обстоятельства для дела. Часть 1 ст.125 УПК РК гласит, что «каждое доказательство подлежит оценке с точки зрения относимости, допустимости, достоверности, а все собранные доказательства в совокупности – достаточности для разрешения уголовного дела» [5].

Обратим внимание, что каждый этап процесса доказывания завершается оценкой и изложением вытекающих из нее выводов в соответствующих процессуальных документах. К примеру: оценка доказательств, осуществляемая в процессе сбора, определяет основные направления, в каких нужно выявлять новые доказательства, т.е. оценка

предшествует выявлению новых доказательств. Оценка сведений, сообщаемых допрошенным субъектом, предоставленных при осмотре места происшествия и т.д., предшествует их процессуальному закреплению. В протокол процессуального действия включается информация, переработанная и оцененная органом, ведущим уголовный процесс. По мнению процессуалистов, «оценка доказательств, представляет собой неотъемлемую часть единого процесса доказывания и выделяется исключительно с учебно-методической целью» [85, с.105, 126, 127].

Все элементы доказывания очень сложны, поэтому нельзя говорить, что какой-то элемент легче, а какой-то более сложный. В свою очередь, сложность оценки заключается в том, что на основе совокупности собранных и проверенных доказательств орган, ведущий уголовный процесс, в предусмотренных правовыми актами формах получают новое знание о фактах и обстоятельствах, подлежащих доказыванию по уголовному делу, о части или обо всем уголовном правонарушении, включая вывод о мере наказания.

Если исходить из ч.2 ст.125 УПК РК с учетом публичности начала уголовного процесса, оценка доказательств возложена на суд, ОУП, которые оценивают их по своему внутреннему убеждению, основанному на совокупности рассмотренных доказательств, руководствуясь при этом законом и совестью. Все остальные субъекты уголовного процесса могут принимать активное участие в оценке путем заявления ходатайств о приобщении дополнительных доказательств или недопустимости доказательств, обжалования действий и решений властных субъектов, связанных с оценкой доказательств. При этом, уголовно-процессуальное законодательство РК предусматривает разный порядок и сроки обжалования действий (бездействии) должностных лиц на досудебной и судебной стадиях. Обжалование действий (бездействий) ОУП предусмотрен ст.105 УПК РК, следственного судьи ст.107 УПК РК, а на судебной стадии в порядке главы 48 УПК РК.

Вместе с тем, статья 125 УПК РК упустила из виду такого субъекта оценки как «присяжный заседатель», который согласно абзацу 2 ч.1 ст.25 УПК РК оценивает доказательства по своему внутреннему убеждению, основанному на совокупности рассмотренных доказательств, руководствуясь при этом совестью.

Если сравнивать оценку доказательств, присяжных заседателей и органа, ведущий уголовный процесс, есть отличие, т.к. первые оценивают по внутреннему убеждению, руководствуясь совестью, вторые внутреннему убеждению, руководствуясь в первую очередь законом, а затем совестью. Такое положение вещей, показывает, что для служителей фемиды и ОУП закон играет первостепенную роль, совесть и сентиментальные чувство нравственности уходят на второй план, т.е. есть норма уголовного закона, лицо совершившее нарушение этого закона и

доказательства. Присяжные же заседатели больше оцениваю чувствами и эмоциями. Приведем пример многолетней давности по делу Веры Засулич. В 1877 г. Петербургский градоначальник Ф. Трепов приказал выпороть политического заключенного, члена организации «Земля и воля» А. Боголюбова (Архипа Емельянова) за то, что тот не снял перед ним шапку. Приказ Трепова вызвал широкий общественный резонанс, он нарушал запрет на телесные наказания от 1863 г. Спустя полгода после инцидента В. Засулич пришла на прием к Трепову и дважды выстрелила ему в живот из револьвера. Трепов остался жив, Засучил арестована. Суду Засулич сказала: «Признаю, что стреляла в генерала Трепова, причем могла ли последовать от этого рана или смерть, для меня было безразлично». По законам тех лет Засулич грозило наказание в виде тюремного заключения до 20 лет, но речи ее адвоката и сама обвиняемая снискали симпатии присяжных. 31.03.1878 г. суд присяжных полностью оправдал Засулич. Приговор был опротестован на следующий день, полиция стала разыскивать Засулич, но ей удалось бежать в Швейцарию. Общество в оценках оправдательного приговора Засулич разделилось - одни считали, что суд оправдал терроризм, другие настаивали, что Засулич стреляла в человека, допустившего произвол. «Гражданское общество не может держаться, коль скоро суд, основанный на законе и служащий ему органом, будет оправдывать преступление и возводить его апофеозу», - писали газеты того времени. К слову, Глава Следственного комитета России А. Бастрыкин скептически относится к приговору Засулич. «Деяние В.Засулич однозначно трактовалось как справедливый акт возмездия. Подсудимая и ее юридическая вина вообще выпали из сферы внимания и восприятия людей» [128].

Пример многолетней давности показывает отношение общества к определенным вещам по разному, что самое интересное в нынешнее время ничего не изменилось. Простой обыватель в отличии от должностных лиц с юридическим образованием по другому смотрит на мир, и что кране опасное с негативом на представителей власти.

Процесс и содержание оценки доказательств получило в юридической литературе различное толкование. Содержание процесса оценки учеными процессуалистами определяется не однозначно. Оценка доказательств определяется: как мыслительная деятельность, осуществляемая в логических формах [64, 126], как логический процесс установления наличия и характера связей между доказательствами, определения роли и значения, достаточности и путей использования доказательств для установления истины по уголовному делу [127, с.190], как мыслительная, логическая деятельность, имеющая своей целью определенный вывод, суждение об относимости, допустимости, - достоверности, значении (силе) каждого доказательства и достаточности их совокупности для установления обстоятельств, входящих в предмет доказывания и разрешения уголовного дела [129].

Одни авторы рассматривают оценку как регламентированную законом деятельность субъектов познания, в частности П.Ф. Пашкевич писал: «Оценить доказательства - значит определить, насколько точно установлено каждое из них, в какой взаимосвязи с делом и другими доказательствами оно находится, какой именно факт, имеющий значение для дела, оно устанавливает или опровергает и что означают в совокупности все собранные по делу доказательства» [130]. М.С. Строгович утверждал, что «оценка доказательства является итогом его проверки и состоит в признании существования или несуществования того факта, который этим доказательствам устанавливается» [61]. В.Д. Арсеньев под оценкой доказательств понимает определение силы и значения каждого доказательства в отдельности и всех доказательств в совокупности [108, с.130]. А.И. Трусов считает, что оценить доказательства - значит решить вопрос о достоверности доказательств [62]. По мнению Л.Т. Ульяновой, при оценке доказательств оценивается, прежде всего, их достоверность и значение [131]. По Р.С. Белкину оценка доказательств в судебном исследовании - это логический процесс установления допустимости, относимости доказательств, наличия и характера связей между ними, определения значения и путей использования доказательств, в целях обнаружения истины [82].

Оценка доказательств как любой познавательный процесс, ведет «из незнания к знанию» или «неполного, неточного знания - становится полным и точным». Процесс оценки доказательств, включает определение их относимости, допустимости, достоверности, достаточности сначала для выдвижения версий на досудебной стадии, а затем и достоверных выводов по итогам рассмотрения судом уголовного дела.

Важный аспект в оценке доказательств отметил Ю.К. Орлов, указав, что оценка доказательств, протекает по своим логическим и психологическим законам [50]. Позиция 3.3. Зинатуллина о сущности оценки доказательств, по нашему мнению наиболее верно отражает процессуальную и гносеологическую сторону оценки. По его мнению, оценка доказательств имеет внутреннюю и внешнюю сторону. Внутренняя (логическая) сторона состоит в том, что участники уголовного процесса производят логические операции по их анализу, определяют относимость, допустимость доказательств. Внешняя (правовая) сторона выражается в том, что логические операции по оценке доказательств, производятся в условиях уголовно-процессуальных отношений, оценке подлежат лишь те фактические данные, которые получены в установленном законом порядке, результаты оценки подлежат объективному выражению в процессуальных документах[50].

Изучая проблему дифференцирования предмета оценки доказательств и их проверки, Ю.К.Орлов отразил, что отношение таких элементов процесса доказывания исходит из основного различия этих видов

деятельности - является она исключительно мыслительной или еще и практической. Мы согласны с Ю.К. Орловым, что отдельные свойства доказательств (достоверность, в иных случаях - относимость и допустимость) подлежат и проверке и оценке, остальные (сила, достаточность) - только оценке, т.к. практических никаких проверочных действий в этом случае не нужно. Предметы этих элементов процесса доказывания совпадают лишь частично, являются пересекающимися [50]. На проверочном этапе, такие свойства доказательств как относимость, допустимость и достоверность подлежат проверке, при оценке в отношении них делается вывод. Оценка доказательств, служит нужным условием целеустремленного направления досудебного и судебного разбирательства, применение законных и обоснованных процессуальных решений, правильное применение правовых актов.

Как мы уже отметили, оценка доказательство по внутреннему убеждению, выступает в качестве одного из принципов уголовного процесса согласно ст.25 УПК РК. В ст.17 УПК РФ этот принцип звучит, как свобода оценки доказательств. В ст.19 УПК Беларуси название принципа идентично нашему, но содержание различается. Так ч.1 звучит следующим образом: «Суд, ОУП оценивают доказательства, руководствуясь законом и своим внутренним убеждением, основанным на всестороннем, полном и объективном исследовании всех обстоятельств уголовного дела в их совокупности», а ч.2 звучит так: «Никакие доказательства для органа дознания, следователя, прокурора, суда не имеют заранее установленной силы» [132]. Версия Российского варианта ч.1: «Судья, присяжные заседатели, а также прокурор, следователь, дознаватель оценивают доказательства по своему внутреннему убеждению, основанному на совокупности имеющихся в уголовном деле доказательств, руководствуясь при этом законом и совестью» и ч.2: «Никакие доказательства не имеют заранее установленной силы». Если сравнивать с нормой в УПК РК, то в УПК Беларуси отсутствует, присяжные заседали, есть народные судьи, а также конкретно прописано, что оценкой доказательство занимаются специальные должностные лица. В России и Казахстане, оценку производят суды, ОУП и присяжные заседатели, но в отличие от РК, присяжные в РФ принимают решение на основании совести и закона.

А.В. Кудрявцева правильно акцентирует внимание, что «категории внутреннего убеждения, совести и закона играют роль не принципов, а общих оснований для оценки доказательств» [133], на это указывает ч.1 ст.25 УПК РК [5]. Исследование этих аспектов в нашей магистерской диссертации нужно для определения выяснение общих оснований, применяемых при оценке всех доказательств и в их ряду к компьютерной информации, а также с целью формулирования специальных оснований,

применимых при оценке цифровых доказательств как самостоятельного вида доказательств.

Итак, закон отражает оценку доказательств как три составных компонента, формирование мнения должностного лица, по внутреннему убеждению, основанному на совокупности рассмотренных доказательств, руководствуясь при этом законом и совестью. Внутреннее убеждение как основание для оценки доказательств формируется в результате рассмотрения всех доказательств в совокупности. Ю.К. Орлов утверждает, что «категория внутреннего убеждения введена как альтернатива теории формальной оценки доказательств», т.е.: «Внутреннее убеждение - это прежде всего метод оценки, применяемый «за неимением другого» в тех познавательных процессах, где невозможно получение формализованного вывода» [50]. В свою очередь, авторы теории доказательств в советском уголовном процессе утверждают: «оценка доказательств пока не поддается формализации, в конечном счете, носит содержательный характер, основывается на внутреннем убеждении» [64]. А.И. Трусов полагает возможным формализацию мыслительного процесса при оценке доказательств по уголовным делам, хотя и видит трудности, возникающие на пути [62]. А.А. Давлетов: «Умственная логическая деятельность, составная часть контента оценки доказательств, наверняка не регулируется нормами права. Однако эти нормы влияют на то, чтобы процесс мышления соответствовал целям закона. Полностью свободной от правовых норм данная часть процесса (имеется в виду мыслительная работа должностных лиц) - быть не может» [134].

Внутреннее убеждение формируется на подсознательном уровне, поэтому на это влияет человеческие качества личности субъекта оценки доказательств, его психологические, нравственные установки, мировоззрение и мировосприятие в процессе доказывания. По этой причине, законодатель установил соответствующие требования, к субъектам оценки доказательств, такие как непредубежденность и незаинтересованности в исходе дела. А.В. Кудрявцева обращает внимание на процессуальные гарантии непредубежденности субъектов оценки доказательств. «Гарантиями являются основания для отвода, установленные для должностных лиц, ведущих уголовный процесс в виде запрета совмещать функции участников уголовного процесса, к примеру, не может принять в свое производство уголовное дело лицо (прокурор, судья, следователь), в случае если оно было очевидцем преступления (свидетелем) или защитником обвиняемого [135].

Такое правило строится на психологическом свойстве индивида формировать умозаключение по первому своему впечатлению. Поэтому субъекту оценки доказательств, в особенности судьи должны быть обеспечены новизной восприятия обстоятельствам дела. По сути, субъект оценки доказательств должен быть идеальным: счастливым, здоровым,

обеспеченным, при этом, не он сам, не его родные не подвергаться преступным посягательствам, информация об обстоятельствах рассматриваемых событиях к нему должна поступать только из процессуальных источников. А.В. Кудрявцева полагает, что только этот субъект оценки доказательств может подойти к оценке объективно» [135]. А.В. Победкин рассматривает внутреннее убеждение как метод оценки доказательств и как результат такой оценки: «Внутреннее убеждение как результат оценки доказательств означает уверенность следователя, судей в правильности выводов, к которым они пришли в ходе уголовно-процессуального доказывания» [136]. Вместе с тем, следует согласиться с О.В. Левченко, который считает, что следует различать внутреннее убеждение и убеждённость. Первое связано с рациональной основой деятельности и глубоко укоренившиеся в сознании человека представления морально идеологического плана, мотивирующие его решения и поступки. Второе – субъективное отношение человека к своим поступкам и убеждениям (уверенность в собственной правоте). Оба понятия тесно связаны и при известной сложности дифференциации в ряде работ по исследуемой проблематике, нередко трактуются в едином контексте [137]. Б.Т. Матюшин полагает, что внутреннее убеждение судьи следует трактовать как собственное отношение к своим знаниям, решениям, действиям[138]. А.В. Смирнов указывает: «Убеждение называется внутренним не только оттого, что зреет в сознании оценивающего субъекта (это только предубеждение), - оно внутреннее, главным образом потому, что единственным убежищем, внутри которого сокрыта истина, служит наличная совокупность доказательств» [139]. И.И. Мухин отражает, что «недопустим объективизм, т.е. недооценка значения внутреннего убеждения органа, ведущего уголовный процесс. Лишь адекватное осознание и сочетание объективного и субъективного моментов при оценке доказательств, строгое соблюдение закона, обеспечит истину и обоснованный вывод по делу...» [140]. Ю.В. Кореневский рассматривая внутреннее убеждение как критерий истины в уголовном процессе, утверждает: «В уголовном процессе должностное лицо, ведущий уголовный процесс, в конце концов, приходят к тому, когда на основании собранных и проверенных доказательств создают мысленную картину, образ преступления и остаются наедине со своим представлением. После чего, каждый из них должен решить, правильное его представление или нет, соответствует оно действительности, не ошибся ли он в своих выводах. Никакого объективного критерия здесь нет и быть не может, ибо искомая истина известна нам только в виде наших же представлений, основанных, разумеется (во избежание неправильных толкований) на доказательствах, полученных и проверенных в результате практической деятельности» [141]. А.В. Кудрявцева пишет, что нельзя отождествлять мысленный образ и представления с внутренним убеждением. Правильнее мысленные образы и

представления, их формирование включать в понятие оценки доказательств, ее внутренней стороны как процесса мышления. Представления как отражение в сознании субъекта оценки, обстоятельств уголовного дела и фактических данных, с помощью них эти обстоятельства устанавливаются, служат составной частью внутреннего убеждения [135].

Исходя из всех суждений, можно предположить, что внутреннее убеждение - это метод (способ) оценки доказательств.

Следующим компонентом, для оценки доказательств, служит совесть. Применение в УПК РК оценочных этических категорий: совесть (ст. 25), честно (ст.646), беспристрастность (ст. 8, 23, 24), несправедливость (ст. 438, 494), позволяет наполнять нормы закона моральным содержанием, это влияет на нравственное сознание участников уголовного процесса. Нравственное понимание должностным лицом, ведущих уголовный процесс целей и задач создает психологическую основу выбора ими таких основанных на установлениях процессуального закона форм поведения, исходящие из понимания сущности и значения общечеловеческих ценностей, справедливость и гуманность, положительно воспринимаемое обществом. Однако, не стоит останавливаться подробно на этом, поскольку оно не входит в предмет диссертационного исследования.

Уголовно-процессуальный закон закрепляет закон как третий компонент оценки доказательств, на ровне с внутренним убеждением и совестью. Компонент в виде закона подразумевает правила и принципы, закрепленные в законе, применяемые при оценке доказательств. К ним относятся правила доказывания, основанные на принципах уголовного процесса: презумпции невиновности, законности способов собирания проверки и оценки доказательств. К примеру, требование, закрепленное в ч. 2 ст. 25 УПК РК: «Никакие доказательства не имеют заранее установленной силы», норма выражает свободную оценку доказательств.

Статья 77 Конституции Казахстана формирует принципы правосудия, отражает принцип презумпции невиновности и устанавливает правила доказывания: «лицо считается невиновным в совершении преступления, пока его виновность не будет признана вступившим в законную силу приговором суда; обвиняемый не обязан доказывать свою невиновность; любые сомнения в виновности лица толкуются в пользу обвиняемого». Принципы правосудия отражают, что способы доказывания должны быть законными, и возложены на ОУП. Положение презумпции невиновности реализуется на практике как толкование сомнений в пользу обвиняемого, справедливо отмечая в литературе, что «одной из форм реализации принципа презумпции невиновности является оправдательный приговор» [142].

Статья 6 Европейской Конвенции по правам человека, п. 9 ч. 3 ст.77 Конституции РК, и ст. 112 УПК РК является общей нормой при оценке качества доказательства, как допустимость. Поскольку оценка

доказательств обычно предшествует принятию важных процессуальных решений (о привлечении лица в качестве обвиняемого; об окончании досудебного расследования и направления дела в суд через прокурора; об окончании досудебного расследования и прекращении уголовного дела). При этом, принятые решения должны быть обоснованные, а также обстоятельствам дела должна быть дана соответствующая правовая оценка. Еще одним аспектом служит, что предметом оценки должны быть не только доказательства и устанавливаемые с их помощью обстоятельства дела, но и соответствие обстоятельств дела норме уголовного права. Поэтому уголовный закон нужно включать в число общих оснований оценки цифровых доказательств.

Оценка относимости, допустимости, достоверности доказательств, производится от начала сбора до принятия окончательного процессуального решения. Тем не менее, нужно помнить, что каждый этап оценки доказательств имеет самостоятельное значение и преобладать на определенном этапе доказывания. Авторы теории доказательств отмечают, что признание доказательства допустимым не предрешает вопроса о достоверности, вывод о допустимости предшествует, но никак не заменяет вывода о достоверности [64]. Вместе с тем, допустимость служит обязательной предпосылкой их достоверности. Приступая к оценке цифровых доказательств, орган, ведущий уголовный процесс, обязан, руководствоваться ч. 1 ст.125 УПК РК, оценить её с точки зрения относимости, допустимости, достоверности и достаточности. Такое положение вещей позволит выделить из общего списка доказательства, неотносимые и недопустимые к использованию доказательства. В первом параграфе главы первой диссертации нами были определены элементы, составляющие компьютерную информацию как цифровых доказательств, именно они подлежат процессу оценки.

Относимость - доказательства, в т.ч. цифровых, выражается в наличии существенной, нужной связи его контента (сведений о фактах) с подлежащими доказыванию обстоятельствами, в силу чего эти сведения могут быть использованы для установления истины и повлечь за собой принятие определенного процессуального решения. Относимость это объективное свойство, органически присущее доказательствам, а не их юридический признак. Требования уголовного и уголовно-процессуального закона играют важную роль в решении вопроса об относимости доказательств, но не нормы права делают доказательство относимым, не они раскрывают суть этого свойства. Оно присуще сведениям о фактах объективно, независимо от воли законодателя, закон лишь опосредует это объективное свойство. Сущность относимости доказательств состоит в их связи с искомыми фактами и обстоятельствами, являющаяся одним из проявлений философского закона всеобщей связи и взаимозависимости явлений природы и общества. Информация о фактах становятся

доказательствами именно потому, что они могут служить основой установления наличия или отсутствия обстоятельств, имеющих значение для правильного разрешения уголовного дела. Но относимость доказательств не гарантирует непременного установления истины, она содержит такую возможность, реализация которой зависит от субъективных качеств должностного лица, ведущего уголовный процесс, от их знаний, моральных качеств, опыта и профессиональной подготовки. При этом, относимость носит объективный характер и не зависит от возможности ОУП воспользоваться информацией, содержащими доказательство или установить истину. Предъявляемое к содержанию доказательства гносеологическое требование состоит в том, что доказательство должно давать характеристику предмета доказывания. В противном случае информация не выполнит сигнальной функции. Поэтому относимым является такое доказательство, чей контент воспроизводит предположительно или достоверно фактическое обстоятельство, имеющее значение для правильного разрешения дела. Относимыми могут признаваться достоверные, недостоверные доказательства, отражающие или противоречащие действительности. В данном случае, относимыми служат доказательства, собранные при проверки различных версии. Их роль заключается в опровержении всех возможных гипотетических объяснении происшедшего и тем самым подтверждают правильность одной единственной версии, т.е. из предположения становится достоверным знанием. Относимыми считаются и доказательства, устанавливающие отсутствие ряда фактов, которые должны были быть при естественном ходе событий в соответствии с данной версией. Так называемые негативными обстоятельствами, противоречащими выдвинутому объяснению хода событий и свидетельствующие о частичной либо полной несостоятельности объяснения.

Вывод, что между искомым фактом и добытым доказательством, действительно, существует объективная связь, как правило, делается на заключительных этапах доказывания. В начале процесса доказывания наличие такой связи зачастую лишь предполагается. Обоснованность этих предположении устанавливает по мере проверки версии на досудебной стадии [54]. Особенность определения относимости цифровых доказательств заключается в возможности при их воспроизведении при использовании технических средств и анализе не только содержания цифровой информации, но и ее реквизитов. Связь цифровой информации с событием либо обстоятельствами уголовного правонарушения можно установить с помощью специалиста и последующей соответствующей экспертизы. Оценка относимости предполагает не просто вывод, что цифровая информация по тем либо иным признакам взаимодействует с предметом доказывания, но раскрывает, как именно она связана, какие обстоятельства устанавливает, какой версии соответствует или противоречит. С точки

зрения относимости оценивается как содержание цифровой информации, так и ее свойства: дата создания, изменения, открытия. К примеру, на практике случались такие события, когда сотрудниками Антикоррупционной службы с поличным при получении взятки задерживался полицейский, но при выяснении обстоятельств, оказывалось, что данное лицо, ранее уволено с органов внутренних дел. Данное обстоятельство отражала на иные составы уголовного правонарушения, таких как «мошенничество», «присвоение полномочий должностного лица», а не коррупционного характера «получения взятки». При проведении процессуальных действий на досудебной стадии, в частности обыска и изъятия компьютеров, а также проведения исследования изъятых объектов, установлено, что приказ об увольнении были изданы (составлены) позже задержания полицейского с взяткой. В связи с этим, органами Антикоррупциионой службы были начаты досудебные расследования по факту пособничества укрытия коррупционных уголовных правонарушении. В этом случае, дата создания, изменения, открытия электронного документа, т.е. свойства цифрового доказательства, послужили информацией относимые к предмету доказывания (доказательствами).

Оценка доказательств с точки зрения их допустимости заключается в оценке законности их получения. Существенными признаками соответствия доказательств, требованию закона должно служить разрешение таких вопросов: кто осуществлял сбор доказательств и наделен ли он соответствующими полномочиями; соблюдены ли правила производства процессуальных действий на досудебной стадии при получении доказательств; соблюдены ли права участников процесса; правильность оформление процессуальных действий и их результаты.

По мнению Г.М. Миньковский «существуют следующие условия допустимости фактической информации, собираемые по делу: а) известность и возможность проверки происхождения; б) компетентность и осведомленность лиц, предоставляющих или/и собирающих сведения; в) соблюдение общих правил доказывания; г) соблюдение правил собирания данных определенного вида, гарантирующих от неполноты и искажений; д) соблюдение правил, гарантирующих полноту и точность фиксации собранной информации; е) отказ от включения в нее догадок и предложений» [142]. С.А.Шейфер не выделяет признак законности источника доказательств как самостоятельного условия допустимости, т.к. по его мнению, «все то, что в теории уголовного процесса называется источниками доказательств или средствами доказывания, есть не что иное, как требуемая законом форма». А.В. Соколов придерживает той же точки зрения, с отличием того, что определяется допустимость как «пригодность доказательства с точки зрения его процессуальной формы» [143]. В юридической литературе есть позиция, что оценка допустимости доказательств, проводится не по внутреннему убеждению, а по закону,

поэтому к ее оценке привлекаются нормативные критерии. Наиболее формализованы признаки, делающие доказательства недопустимыми [144].

Выражение мысли появляются в оценочных процессуальных актах, проявляясь в конкретных процессуальных действиях по сбору, проверке доказательств, т.е. оценка доказательств подвергается в некоторых пределах правовому регулированию, воздействию норм уголовно-процессуального права. Данные нормы устанавливают не порядок мышления или ход рассуждения, а цель и условия оценки доказательств, принципы, внешнее выражение в процессуальных документах результатов этой оценки. По этому поводу, Г.П. Корнеев писал «познание с помощью процессуально неоформленной информации не может иметь доказательственной силы». В результате признания недопустимыми доказательствами определенной части процессуального действия, сформировалась новая концепция, названная по образу «Плоды отравленного дерева». Таким названием окрестили американские юристы доказательства, добытые обвинением в нарушение закона [145]. Действительно если исходить из мысли, любое нарушение процессуального порядка сбора доказательств обязано применяться принцип недопустимости использования его результатов в процессе доказывания. Например, в процессе обыска, выемки и осмотра цифровых доказательств из персонального компьютера правонарушителя, были изъята переписка с информацией отражающей продажу наркотических средств, но в момент проведения процессуальных действии один из понятых оказался невменяемым лицом, хотя по внешнему виду это было невозможно определить. В этом случае, несмотря на имеющиеся доказательства, нарушение порядка привлечения понятых послужит основанием для недопустимости всех процессуальных действии.

По нашему мнению, требования к допустимости цифровых информаций как самостоятельного вида доказательств должны выполнять следующие функции: охранительную, т.е. гарантировать охрану прав и свобод личности в уголовном процессе; регулятивную, т.е. упорядочивать процесс получения и передачи цифровых информаций на основании правовых актов; познавательно-удостоверительную, т.е. обеспечивать достоверность и целостность цифровых информаций при получении либо при надобности ее копирования на иные материальные носители.

Правильным примером оценки цифровых доказательств можно отразить ч. 2 ст. 9 Типового закона об электронной торговле, разработанного Комиссия ООН по праву международной торговли, сокращено ЮНСИТРАЛ. Она предусматривает, что «при оценке доказательственной силы сообщения данных учитываются надежность способа, с помощью которого подготавливалось, хранилось или передавалось это сообщение данных, надежность способа, при помощи чего обеспечивалось целостность

информации, способа, при помощи которого идентифицируется его составитель, и любой другой соответствующий фактор» [146].

По нашему мнению цифровая информация в уголовном процессе должна считать допустимым доказательством при:

1) соблюдений гарантий прав и свобод индивида в уголовном процессе;

2) наличие материального носителя цифровой информации, даже при изъятии на новый материальный носитель с удаленной платформы, в целях их сохранения;

3) соблюдения целостности цифровой информации, т.е. сохранения ее в первозданном виде, без каких либо изменении и дополнении.

4) наличий правильно составленного процессуального документа, с помощью чего, цифровая информация вовлекается в уголовный процесс.

Н.А. Зигура предлагает пятым условием принятие ОУП постановления о признании компьютерной информации в качестве доказательства и приобщении ее носителя к уголовному делу. По нашему мнению наличие законно процессуального документа в виде осмотра, выемки и изъятия цифровой информации на материальном носителе достаточно и не целесообразно нагружать ОУП дополнительными документами, отсутствие которых может повлечь недопустимость доказательств, в связи с несоблюдением процедуры в уголовном процессе [10].

Между тем, если первые три условия допустимости доказательств более или менее понятны, то по четвертому нужно рассмотреть подробней, что подразумевается правильно составленного процессуального документа. По этому поводу Н.А. Зигура полагает, что если это энергозависимый носитель, то составляется протокол осмотра или заключение специалиста. В случае содержания цифровой информации на энергонезависимом носителе, а для исследования нужно время, специальные технические устройства или программа, то это может быть заключение эксперта. При этом, в случае предъявления цифровой информации, составляется протокол ее осмотра [10]. С данным утверждением мы немного не согласны, поскольку полагаем, что для выявления цифровой информации нужно сначала ее обнаружить, это возможно только протоколом осмотра. При этом, неважно будет ли это протокол осмотр определенной местности (офиса, квартиры и т.д.), где она будет обнаружена на материальном носителе (ноутбуке, флэш карте и т.д.) либо после осмотра места происшествия будет составлен дополнительный протокол осмотра цифровой информации на определенном материальном носителе. В случае же предоставления участниками уголовного процесса возможно составление протокола выемки и/или осмотра. Такие же процессуальные документы в виде заключения эксперта и/или специалиста являются дополнительными процессуальными документами, которые подтверждают наличие либо отсутствие изменении и дополнении в

цифровой информации или их отсутствии, а также более подробно разъясняют содержание информации, во избежание признания их не допустимыми.

Информация, которая может быть доказательством, полученная с нарушением уголовно-процессуального закона, в любом случае будет признано недопустимым, что в свою очередь будет способствовать отсутствию юридической силы. Такие доказательства не могут быть положены в основу обвинения, приговора или иного решения (прекращения уголовного дела), а также использоваться в качестве доказывания о виновности или не виновности лица.

В соответствии с ч.2 ст.112 УПК РК - недопустимость использования фактических данных в качестве доказательств, а также возможность их ограниченного использования в уголовном процессе устанавливаются ОУП либо судом по собственной инициативе или по ходатайству стороны. Орган дознания, дознаватель, следователь, прокурор или судья, решая вопрос о недопустимости доказательств, обязаны в каждом случае выяснить, в чем конкретно выразилось допущенное нарушение, и принять мотивированное решение [5]. Как мы видим, в УПК РК данные требования отражены в статье «Фактические данные, не допустимые в качестве доказательств», в России такое положение вещей отражено в ч.3 и ч.4 ст.88 УПК РК. В первом случае «Прокурор, следователь, дознаватель вправе признать доказательство недопустимым по ходатайству подозреваемого, обвиняемого или по собственной инициативе. Доказательство, признанное недопустимым, не подлежит включению в обвинительное заключение, обвинительный акт или обвинительное постановление». Во втором случае: «Суд вправе признать доказательство недопустимым по ходатайству сторон или по собственной инициативе в порядке, установленном ст.234 и 235 УПК РФ [12].

Обратим внимание, на отдельные различия в УПК РК и РФ, в частности первое, что бросается в глаза, это разделение суда от ОУП в правовом акте России, второе это обязанность выяснение в каждом случае, в чем конкретно выразилось допущенное нарушение, и принять мотивированное решение. Однако, схожесть в том, что признать в доказательство недопустимым может прокурор, следователь, дознаватель и суд по собственной инициативе и ходатайству сторон. На практике и в науке активно обсуждается, какие именно нарушения закона служат влекущих недопустимость доказательств. Ю.К. Кореневский и П.А. Лупинская утверждают, что на недопустимость доказательств, влияют нарушения отражающие достоверность информации, при этом, их не возможно устранить либо восполнить процессуальными действиями [148]. В. Миронов «В случае нарушения процессуального порядка сбора и закрепления доказательств не накладывают тень сомнения на их достоверность и последствия несущественны и устранимы, то неразумно отказываться от

доказательственной информации в условиях, ее острого дефицита при расследовании, рассмотрении и разрешении дела» [149].

Вышеуказанные позиции обоснованы, и полагаем, применимы к цифровой информации в случае их недопустимости, если:

1. Сбор и получение цифрой информации проводилось с нарушением прав и свобод человека и гражданина, гарантированных международными правовыми актами, ратифицированных РК и Конституцией РК;

2. В материалах дела отсутствует порядок появления этой информации;

3. Цифровую информацию невозможно воспроизвести, в связи с размагничиванием материального носителя, если проводить параллель (аналогию) с письменными или другими документами это нечитаемый текст.

4. Не соблюдена целостность (неизменность) цифровой информации.

Перечисленные нарушения влекут неустранимые сомнения в достоверности цифровой информации, поэтому ее нельзя использовать в качестве доказательств.

Между тем, предлагаем рассмотреть для сравнения пункт 4 части 3 статьи 87 УПК Украины «Недопустимости доказательств, полученных в результате существенного нарушения прав и свобод человека». Согласно, которой «Недопустимо также доказательства, полученные: при исполнении постановления о разрешении на обыск жилища или иного владения лица, если такое решение вынесено следственным судьей без проведения полной технической фиксации заседания» [37].

Результаты технической фиксаций судебного процесса проводимого следственным судьей, по сути, являются «цифровой информацией». Данная норма отражает, что недопустимым являются все доказательства, если суд при выдаче санкции не провел техническую фиксацию своего процесса. Такое положение вещей в целом затрудняет работу ОУП и даже если отсутствуют нарушения с их стороны при производстве процессуальных действии, то в результате неисправности технических устройств, невнимательности или умышленном действии сотрудников суда может повлечь недопустимость всех доказательств. Пример этот применим и к нашей практической деятельности. Несмотря на отсутствие в УПК РК прямой нормы как в Украине, в настоящее время судебные процессы протоколируются с помощью технических средств, фактически в письменных протоколах ничего не фиксируется. И в случае ходатайства одной из сторон действия следственного судьи могут быть признаны незаконными, в случае утери цифровой информации о проведении судебного слушания, что может повлечь и недопустимым всех последующих процессуальных действии произведенных ОУП проведенных по санкции вышеуказанного суда.

Оценка доказательств с точки зрения их достоверности производится на досудебной стадии, при выдвижении версий или принятии

процессуальных решений. При оценке цифровой информации в качестве доказательства, нужно учитывать специфику механизма ее формирования, разбив ее, на созданных пользователями и/или программой.

В юридической науке формулируются общенаучные требования к научно-техническим средствам при их использования в уголовном процессе. Требования подразумевают их соответствие общенаучной состоятельности с обязательной апробацией в лабораторных условиях, где проверяют соответствие научно-технических средств и выясняют степень их надежности и надежности результатов применения. Общенаучные требования нужно применять к цифровым информациям. Критерием оценки созданных программой доказательств, служит установление, какой программой данные создаются, лицензионная ли программа. В зависимости от сложности цифровой информации, для ее оценки нужно проведение экспертизы. К примеру, для моделирования и анализа ДТП, создаются компьютерные программы с инженерно математическими моделями, они используются в целях воспроизведения и визуализации ДТП, это позволяет всесторонне исследовать и наглядно получить результаты [35].

В свою очередь, оценка достоверности цифровых информаций, подразумевается в следующих выводах:

1) о корректной работе технического устройства и загруженных в нем программ, исследованных и используемых при собирании и проверке цифровой информации;

2) о научной достоверности получения цифровых информаций;

3) об обеспечении целостности цифровых информаций;

4) о достоверности цифровых информаций путем анализа контента и свойств этого объекта, а также при его сопоставлении с иными доказательствами.

Оценка компьютерной информации как доказательств с точки зрения их достоверности ставит две проблемы: доказать правильность этих данных и правильность функционирования программы обработки. Оценка достоверности, как и оценка относимости доказательств, представляет собой длящийся процесс, который завершается лишь в момент формулирования окончательных выводов по делу на основе всей совокупности собранных доказательств. Устанавливая правила оценки доказательств, в ч.1 ст.125 УПК РК называет еще одно свойство, присущее всей их совокупности, - достаточность. Под достаточностью следует понимать возможность на основании имеющихся в распоряжении органа, ведущего уголовный процесс доказательств разрешить все вопросы, входящие в предмет доказывания с учетом, что все неустранимые сомнения толкуются в пользу обвиняемого.

При определении достаточности цифровых информаций в виде доказательств, нет нужды собирать всю имеющуюся на исследуемом носителе информацию. По причине отсутствия опыта должностных лиц, ведущих уголовный процесс, как правило, в постановлении о назначении

перед экспертом ставятся не правильные и не корректные вопросы. И В. Собецкий приводит из своей практики пример: «восстановить и распечатать все стертые файлы». Нужно согласиться с И.В. Собецким, что такая постановка вопроса не просто не исполнима, но и абсурдна, в виду возможности существования в системном блоке многочисленных копии файлов. Первостепенной задачей досудебной и судебной стадии уголовного процесса является установление истины и привлечение к ответственности виновных лиц. Следовательно, сбор цифровых информации, в целом, как и иных доказательств, прекращается после предмета доказывания в пределах, нужного объема информации по расследуемому уголовному делу. Не вся представленные суду цифровые доказательства могут быть признаны допустимыми и относимыми доказательствами. В целях оценки представленных материалов как надлежащих доказательств, требуется их детальная процессуальная оценка. Главная функция суда именно заключатся в проверке представленных цифровых информаций, с определением среди них нужных доказательств, исключив из дела информацию не являющимися доказательствами, недопустимых или не относящихся к делу, и на основании оставшихся допустимых доказательств законно и обоснованно принять процессуальное решение.

Н.А. Зигура сделала попытку определить специальные основания для оценки цифровой информации в качестве вида доказательств, отразив некоторые особенности получения, исследования и оценки. Нужно согласиться с ней, что в целях определения специальных оснований оценки цифровой информации как доказательства отправным отчетом, служит механизм образования. Она выделяет в качестве специальных оснований психологические, гносеологические и юридические основания для оценки.

Психологический элемент непосредственно связан с формированием на данный процесс внутреннего убеждения познающего субъекта, влияние его правового сознания и нравственные установки. В качестве психологических оснований выступает убеждение субъекта оценки доказательств в том, что вне зависимости от тех трудностей, которые могут возникнуть при её оценке, нужно критически подходить к цифровой информации. Происходит это потому, что с оценкой такого вида информации еще не так часто сталкиваются в уголовном процессе.

В качестве гносеологического основания для оценки цифровой информации выступает наличие у субъектов оценки основ специальных знаний, их содержание составляет понимание ими механизма образования и формы существования цифровой информации. Основание связано с переработкой и накоплением информации, характеризует оценку как форму познания, способ приобретения нового знания. Наиболее распространенные виды специальных отраслей знаний, относящиеся к цифровой информации, в той или иной степени должностные лица, ОУП и суда изучают, получая юридическое образование: криминалистика, информатика, правовая

информатика, информационные системы в юридической деятельности, информационные технологии. Но быстрый рост использования новых возможностей современных технологий и недостаточность разработанных методик приводят к возникновению определенных трудностей при гносеологическом аспекте оценки доказательств. В целях формирования гносеологического основания оценки цифровой информации у должностных лиц, нужно: выделить цифровую информацию в самостоятельный вид доказательств, на основании специфического механизма её образования и разграничение данного вида доказательств с иными документами и вещественными доказательствами; закрепление в правовых актах определение понятия цифровой информации как доказательства и материального носителя; описание и закрепление в правовых актах методик ее сбора, проверки и оценки; в связи с развитием технологии продолжить научное исследование в этом направлении.

Безусловно толкованием цифровой информации, для ее оценки могут служить разъяснения специалиста и эксперта, а также их заключения. Цифровая информация обладает свойствами, которые не возможно правильно понять и толковать без применения специальных знаний. В качестве юридического основания для получения, закрепления, проверки и оценки цифровой информации, а также отражающие права тех лиц, чьи интересы затрагивает данный вид информации, выступают положения уголовно-процессуального закона. Оценка цифровой информации как доказательства состоит познании субъектом содержания, ее свойства, составляющие ее ценность и полезность для решения каких-либо задач, стоящих перед ним, путем мысленного сопоставления с определенными ценностными установками. Поэтому для оценки цифровой информации, нужно, преобразовать ее с помощью технических средств, в воспринимаемую для человека форму. Субъектам оценки нужно основываться на научном знании, что способствует пониманию и установлению достоверности факта, для этого достаточно разъяснений специалиста, и обладать некой системой ценностей, сложившейся на опыте. Задача субъектов оценки проследить путь формирования цифровой информации, результата отражения событии уголовного правонарушения либо обстоятельств до появления в деле этой цифровой информации.

Подводя итоги, понимаешь, что оценка цифровой информации - сложный и ответственный процесс для органов, ведущих уголовный процесс, требующая наличие у должностных лиц высокого уровня знаний о цифровой информации. При определении содержания оснований оценки нужно исходить из комплексного образования. 1) Это материальный носитель. Особенность, информация, находящаяся на нем, может быть скопирована без искажения и потерь. 2), Это процессуальный документ, в нем описан сам носитель информации, ее содержание, реквизиты, и способ приобщения к материалам уголовного дела.

ЗАКЛЮЧЕНИЕ

Если войти в Интернет пространство и задать в поисковики, вопрос «цифровизация, коронавирус, пандемия, карантин» можно наитий очень много ссылок, что «Карантин ускорил цифровизацию высшего образования» [150], «Коронавирус ускорил цифровизацию экономики в 10 раз» [151], «Технологии карантина. Ускорила ли пандемия цифровизацию?» [152], «Подозрительность к онлайну сходит на нет»: как карантин повлиял на работу интернет-магазинов» [153] и т.д.

Ускорение цифровизации есть положительный процесс, но, этому есть и отрицательная стороны, которым является развитие преступности. Криминальная среда использует развитие цифровизации в свою пользу, ей уже не надо врываться в банк с оружием в руках и требовать деньги, достаточно обладать хорошими знаниями компьютера и можно похитить гораздо больше денег, чем при разбоях и грабежах, при этом, еще и остаться не замеченным. Поскольку деньги могут прогоняться по многочисленным счетам подставных, несуществующих или неподозревающих об этом уголовном правонарушении лиц.

К сожалению, жажда получения легких и быстрых денег преобладает у большинства людей. Криминальная среда развивается быстрее чем, уголовное, уголовно-процессуальное право и правоохранительная система, преступники зачастую владеют лучшими орудиями преступления, технического оснащения, финансируются без бюрократической проволочки, вследствие чего могут себе позволить подкупать чиновников, использовать новейшие технические оборудование и брать к себе на службу высококлассных специалистов из любой профессиональной среды, в т.ч. IT-технологии.

Данные обстоятельства служат для государства веским основанием для принятия мер противодействия криминалу. В целях применения в уголовном процессе цифровых доказательств, выражающихся в различных цифровых информациях, в т.ч. компьютерной нужно на законодательном уровне провести границы этих понятия и уточнить их правовой статус.

По итогам магистерской работы нами предложены три составляющие:
1) внедрение в науку новых терминов;
2) изменение в правовые акты РК;
3) практическая составляющая сторона, об обязательном участии специалиста при изъятии исследований цифровых доказательств.

Несмотря на то, что многие считают, что вопрос на законодательном уровне понятии «цифровые или электронные доказательства», «цифровые (компьютерная) информация» принимать еще рано, думаем, настало время для их закрепления как самостоятельных доказательств в уголовном процессе.

При этом, предлогам свою версию терминов в следующей редакции:

- «цифрового (электронного) доказательства» - сведения, полученные в соответствии с требованиями настоящего Кодекса, из показаний участников уголовного процесса и иных лиц участвующих в нем, запечатленных на видео или аудио носителях, а также любые иные сведения, полученные путем считывания с электронных устройств, имеющее значение для правильного разрешения уголовного дела [35].

- цифровая (компьютерная) информация - сведения, в электронно-цифровом формате, создаваемые различными техническими средствами и устройствами, программами фиксации, обработки и передачи информации.

Вышеуказанными терминами предлагаем дополнить п.59 и п.60 ст.7 УПК РК, раскрывая их, предлагаем на законодательном уровне детально регламентировать вопросы, связанные с правовым режимом цифровой - компьютерной информации, выделив ее как самостоятельный вид доказательства. Таким образом, целесообразно расширить список видов доказательств, в ч.2 ст.111 УПК РК, дополнив их цифровой (компьютерной) информацией. Предлагаем свои вариант ч.2 ст.111 УПК РК в следующей редакции: «Фактические данные, имеющие значение для правильного разрешения уголовного дела, устанавливаются: показаниями подозреваемого, обвиняемого, потерпевшего, свидетеля, свидетеля имеющего право на защиту, эксперта, специалиста; заключением эксперта, специалиста; вещественными доказательствами; протоколами процессуальных действий; цифровой (компьютерной) информацией и иными документами».

Таким образом, точное определение этих терминов позволит на практике и в науке отграничить цифровую информацию от иных документов и вещественных доказательств, что решит процессуальный режим цифровой информации, добываемых ОУП, приобщаемых и предъявляемых сторонами на досудебной и судебной стадии уговорного процесса.

Информация о практической деятельности человека и различных событиях, существующие в электронно-цифровой среде на просторах Интернета в специальных хранилищах и процессорах, требуется в правовом смысле рассматривать как самостоятельный вид доказательств, разграничив их от традиционных видов, в т.ч. бумажных, т.к. они не могут быть тождественны. Одним способов разрешения этого вопроса может быть предложенный нами вариант, с определением понятий «цифровых доказательств», «компьютерной или цифровой информации», способах изъятия и приобщения к уголовному делу этого вида доказательств с обязательным участием специалиста и разбирающихся в технике и программах понятых либо фиксацией видеосъемки всего процесса. Поскольку не все люди еще понимают вопросы цифровизации и находящейся информации в сети.

В этой связи, предлагаем дополнить главу 11 Доказательства УПК РК ст.120-1 «Цифровая (компьютерная) информация» в следующей редакции:

Статья 120-1 «Цифровая (компьютерная) информация».

1. Цифровая (компьютерная) информация используются в качестве доказательств, если имеет значение для разрешения уголовного дела.
2. При обнаружении цифровой (компьютерной) информации имеющей значения для дела, ОУП принимают меры для их осмотра, выемки или копирования на электронный материальный носитель в целях сохранения и использования в качестве доказательств, о чем составляется протокол.
3. Осмотр цифровой (компьютерной) информации производится с участием специалиста и понятых, с обязательной видео фиксацией происходящих событии, при этом выемка и копирование компьютерной информации осуществляется по правилам главы 31 настоящего Кодекса.
4. Изъятая цифровая (компьютерная) информация, вместе с протоколом приобщается к материалам уголовного дела и хранится до окончательного разрешения уголовного дела.

Возможно, предложенная нами версия по участию специалиста уже устарела и целесообразно готовить должностных лиц ОУП самостоятельно заниматься сбором и изъятием цифровых информации, но этот процесс является в настоящее время долгосрочным, поскольку обучение этому процессу довольно сложный. Не каждый специалист сможет восстановить удаленную информацию с материального носителя, найти и изъять в целостность цифровую информацию без повреждения и вообще разобраться в специальных программах.

Между тем, уже сейчас нужно задумываться и принимать меры по обучению такого вида специалистов, искать для этого средства финансирования для привлечения высококвалифицированных преподавателей из числа практиков в области цифровизации.

В любом случае процесс этот долгий и кропотливый, при этом, одновременно с этим нужно решать вопрос о выявлении уголовных правонарушении с применением компьютерных технологии, расследовать уголовные дела данной категории и уметь собирать, а также приобщать цифровые доказательства к делу.

Следовательно, предложенный нами вариант в магистерской работе и вынесенные положения на защиту наиболее применимы в настоящий момент.

Вместе с тем, работу по исследованию в данной области нужно продолжить и искать более практически применимые средства и развивать юридическую науку в этом направлении.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ:

1. Д. Утепов. Проблемные вопросы сбора и фиксации доказательств в цифровом формате. Правовой научо-пратичесий жрнал «Заң және заман». №9-10 (213-24) Қыркүйек – Қазан, 2018. С.32-34;
2. С. Горбачев. Цифровые (электронные) доказательства в арбитражном процессе. Электронный ресурс: https://legis-group.ru/publications/cifrovie-elektronnie-dokazatelstva-v-arbitrazhnom-processe/;
3. Kazpravda.kz. О роли электронных доказательств в уголовном процессе рассказали в Астанинском районном суде. Электронный ресурс: https://www.kazpravda.kz/multimedia/view/o-roli-elektronnih-dokazatelstv-v-ugolovnom-protsesse-rasskazali-v-astaninskom-raionnom-sude/;
4. Новицкий В.А., Новицкая Л.Ю. Понятие и виды цифровых доказательств. Ленинградский юридический журнал 1(55), Санкт-Петербург, 2019, С.213-221;
5. Уголовно-процессуальный кодекс РК от 4.07.2014 г. № 231-V ЗРК;
6. Вершинин А.П. Электронный документ: правовая форма и доказательство в суде. – М., 2000;
7. ЗРК «Об электронном документе и электронной цифровой подписи» от 7.01.2003 г. № 370;
8. Фаткулин С.Т. Проблемы применения электронных документов в уголовном и арбитражном процессе. Правопорядок: История, теория, практика. №4 (19) 2018. С.40-44;
9. Лисиченко В.К. Криминалистическое исследование документов (правовые и методологические проблемы): дисс. ... д.ю.н. Киев, 1973. - С. 49;
10. Зигура Н.А. Компьютерная информация как вид доказательств в уголовном процессе России: дисс. ... к.ю.н. Челябинск, 2010. - С. 11;
11. Уголовный кодекс РФ от 13.06.1996 г. № 63 ФЗ (принят ГД ФС РФ от 24.05.1996) // СЗ РФ. 1996. № 25. Ст. 2954;
12. Уголовно-процессуальный кодекс РФ от 18.12.2001 г. № 174-ФЗ (принят ГД ФС РФ 22.11.2001 г.) // СЗ РФ. 24.12.2001 г., № 52 (ч. I), ст. 4921.
13. Уголовный кодекс РК от 3.07.2014 г. № 226-V ЗРК;
14. Соглашения о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации, ратифицированный Указом Президента РК от 25.06.2002 г. N 897.
15. Оконенко Р.И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства США и РФ: дис. ... канд. юрид. наук. М., 2016;
16. Основы теории электронных доказательств : монография / под ред. Д.юр.наук С. В. Зуева. М.: Юрлитинформ, 2019. С. 253, 254;
17. Пастухов П.С. О развитии уголовно-процессуального доказывания с использованием электронных доказательств // СПС «КонсультантПлюс»;

18. Мурадьян Э.М. Машинный документ как доказательство в гражданском процессе // Советская юстиция 1975. №22.; Мурадьян Э.М. Использование в гражданском судопроизводстве машинных документов //Советское государство и право. 1976, №2; Венгеров А.Б., Мурадьян Э.М., Фалькович М.С., ЭВМ и договорные отношения в народном хозяйстве // Советское государство и право. 1980. № 7. С. 51,52;
19. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. ГОСТ 6.10.4-84 (утв. Постановлением Госстандарта СССР от 09.10.1984 № 3549);
20. Яковлев А.Н. Электронный документ как средство компьютеризации // Актуальные проблемы компьютеризации потребительской коммерции: тезисы докладов научно- методического семинара. Саратов, 1996. С. 132;
21. Лукьянова И.Н. Использование документов и материалов, изготовленных посредством электронной связи, в качестве средств доказывания в арбитражном процессе РФ // Государство и право. 2000. № 6. С. 96-102;
22. Постановление Пленума ВС СССР от 9.07.1982 г. № 7.0 судебном решении // Бюллетень ВС СССР 1982. № 4;
23. Постановление Пленума ВС СССР от 3.04.1987 г. № 3 «О строгом соблюдении процессуального законодательства при осуществлении правосудия по гражданским делам» // Бюллетень ВС СССР 1987. № 3.;
24. Приказ Генерального прокурора РК от 3.01.2018 г. №2, зарегистрированного в Министерстве юстиции РК 23.01.2018 г. №16268, утверждена Инструкция о ведении уголовного судопроизводства в электронном формате;
25. Правила оптимизации и автоматизации государственных услуг, утвержденные приказом и.о. Министра по инвестициям и развитию РК от 18.02.2015 г. №133;
26. ЗРК «О почте» от 9.04.2016 г. № 498-V ЗРК;
27. ФЗ РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ;
28. Лукьянова И.Н. Использование документов и материалов, изготовленных посредством электронной связи, в качестве средств доказывания в арбитражном процессе РФ / И.Н. Лукьянова // Государство и право. - 2000. - № 6. - С. 96 – 102;
29. ФЗ РФ от 06.04.2011 №63-ФЗ (ред. от 23.06.2016) «Об электронной подписи» (с изм. и доп., вступ. в силу с 31.12.2017);
30. Правила документирования, управления документацией и использования систем электронного документооборота в государственных и негосударственных организациях, утверждены постановлением Правительства РК от 31.10.2018 г. № 703;

31. Соглашения о свободном доступе и порядке обмена открытой научно-технической информацией государств-участников СНГ, утверждена Постановлением Правительства РК от 4.03.1999 г. N 204;
32. Концепция формирования информационного пространства СНГ. Москва, 18.10.1996 г.;
33. ЗРК «О государственной правовой статистике и специальных учетах» от 22.12.2003 г. №510;
34. Вехов В.Б. Электронные документы как доказательства по уголовным делам. Электронный ресурс: http://kriminalisty.ru/stati/yelektronnye-dokumenty-kak-dokazatelstva.html ;
35. Абзелов А.А. «О некоторых вопросах примени термина цифровые доказательства, компьютерная информация в уголовном процессе». Сборник Международной научно-практической конференции: «Актуальные проблемы правотворчества и правоприменительной деятельности в РК», Институт экономики и права Костанайского государственного университета им. А.Байтурсынова. Костанай, 24.04.2020 г.
36. УПК Республики Беларусь от 16.06.1999 г. № 295-З (с изменениями и дополнениями по состоянию на 09.01.2019 г.);
37. УПК Украины от 13.04.2012 г. № 4651-VI (с изменениями и дополнениями по состоянию на 19.12.2019 г.)
38. Полевой И.С. Криминалистическая кибернетика. М., 1989. С. 61.
39. Аверьянова Т.В. Судебная экспертиза: курс общей теории. М., 2006. С. 385.
40. Гадасин В.А. Конявский, В.А. От документа - к электронному документу: системные основы. Гадасин В.А. Конявский В.А Системное отличие традиционного и электронного документа. Электронный ресурс: http://www.accord.ru/index_otl.html ;
41. Венгеров А.Б. Право и информация в условиях автоматизации управления (Теоретические вопросы). М., 1978. С. 105;
42. Эйсман, А.А. Заключение эксперта. Структура и научное обоснование / А.А. Эйсман. — М.: Юридическая литература, 1967. — 152 с;
43. Безлепкин, Б.Т. Уголовный процесс России / Б.Т. Безлепкин. - М., 2003.-664 с.;
44. Кудрявцева А.В., Худякова Ю.В.Вещественные доказательства в уголовном процессе России: монография. / А.В.Кудрявцева, Ю.В. Худякова, — Челябинск: Полиграф-Мастер, 2006. - 176 с.;
45. Кертэс, И. Основы теории вещественных доказательств / И. Кертес. - М.: ВНИИ МВД СССР, 1973.- 104 с.;
46. Остроушко, А.В. Организационные аспекты методики расследования преступлений а сфере компьютерной информации: автореферат дисс. ... канд. юрид. наук / А.В. Остроушко. - Волгоград, 2000. - 27 с.;

47. Мещеряков В.А. Преступления в сфере компьютерной информации. Основы теории и практики расследования / В.А. Мещеряков. — Воронеж: Изд-во Воронежского ун-та, 2002. - 154с.;
48. Лыткин, Н.Н. Использование компьютерно-технических следов в • расследовании преступлений против собственности: автореферат дис.... канд. юрид. наук / Н.Н. Лыткин - М., 2007.;
49. Краснова, Л.Б. Компьютерные объекты в уголовном процессе и криминалистике: дис. ... канд. юрид. наук / Л.Б. Краснова. - Воронеж, 2005.;
50. Орлов, Ю.К. Основы теории доказательства в уголовном процессе / Ю.К. Орлов. М.: Проспект, 2000. - 144 с.;
51. Дорохов В.Я. Природа вещественных доказательств // Советское государство и право. 1971 № 10. С. 112;
52. Вандер, М.Б. Использование микрочастиц при расследовании преступлений / М.Б. Вандер. - СПб.: Питер, - 2001. - 224 с.;
53. Турчин, Д.А. Микроследы — новое в криминалистике / Д.А. Турчин // Проблемы советсткого государства и права. Вып. 7. — Иркутск, 1974. - С. 106- 107.;
54. Завидов Б.Д. Проблемы доказательств и доказывания в уголовном судопроизводстве // Подготовлен для системы Консультант Плюс, 2004.;
55. Зуев В.Л. Доказывание по делам о преступлениях с административной преюдицией: дне. ... канд. юрид. наук: М., 1991. С. 91.;
56. Строгович М.С. Курс советского уголовного процесса: Основные положения науки советского уголовного процесса. Т. 1. - М., 1968 - С. 109-118.; Чельцов М.А. Советский уголовный процесс. М., 1962. С. 207.;
57. Камышин, В.А. Иные документы как «свободное» доказательство в уголовном процессе: дис. ... канд. юрид. наук / В.А. Камышин. - Ижевск, 1998.
58. Селиванов Н. А. Вещественные доказательства. Криминалистическое и уголовно-процессуальное исследование / Н.А. Селиванов. М., 1971. -200 с.;
59. Кукарникова, Т.Э. Электронный документ в уголовном процессе и криминалистике: дис. ... канд. юрид. наук. - Воронеж, 2003.;
60. Янковая В.Ф. Электронный документ как объект документоведения. Вестник Волгоградского государственного университета. Сер. 2, 2013. № 3 (19). с.229-235;
61. Кедров Б.М. Классификация наук. Прогноз К. Маркса о науке будущего. М., 1985. 543 с.;
62. Трусов, А.И. Основы теории судебных доказательств / А.И. Трусов- М.: Госюриздат, 1960. - 176 с.;
63. Кац Ц.М. Доказательства в советском уголовном процессе. Саратов, 1960. С. 32.;
64. Теория доказательств в советском уголовном процессе / под ред . Н.В. Жогина. - М., Юридическая литература, 1973. 735 с.;

65. Царева, Н.П. Иные документы, допускаемые в качестве доказательств по УПК РФ.: дис. ... канд. юрид. наук / Н.П. Царева. - Саратов, 2003;
66. Амерханов Р.А., Утепов Д.П., Абзелов А.А. Применение цифровых данных автомобиля при установлении времени, места и обстановки дорожно-транспортных преступлений. Современные проблемы гуманитарных и социальных наук: Материалы международной научно-практической конференции / Под общей редакцией А.К. Кусаинова. – Нур-Султан: Евразийский гуманитарный институт, 2019. – 370 с.;
67. Першиков, В.И., Савинков, В.М. Толковый словарь по информатике / В.И. Першиков, В.М. Савинков. - М.: Финансы и статистика, 1991. - 543 с.;
68. Иванов Н.А. Теоретические и методические основы судебной компьютерно-технической экспертизы и судебно-технической экспертизы документов: дисс. ... канд. юрид. наук. М., 2005. С. 54-59;
69. Яковлев А.Н. Теоретические и методические основы экспертного исследования документов на машинных магнитных носителях информации: дис. ... канд. юрид. наук. Саратов, 2000.;
70. Кукарникова Т.Э. Электронный документ в уголовном процессе и криминалистике: дис. ... канд. юрид. наук. - Воронеж, 2003;
71. Вехов В.Б. Аспекты криминалистического исследования компьютерной информации и ее носителей // Вестник Муниципального института права и экономики (МИПЭ). Вып. 1. Липецк, 2004. С. 15-17;
72. Мещеряков В.А. Основы методики расследования преступлений в-сфере компьютерной информации: дис. ... докт. юрид. наук / В.А. Мещеряков. - Воронеж, 2001.;
73. Иванов Н.А. Допустимость компьютерных доказательств в процессуальном праве России и США / Н.А. Иванов // Адвокат. - 2000.-№5.
74. Лисиченко В.К. Криминалистическое исследование документов (правовые и методологические проблемы): дис. докт. юрид. наук. Киев, 1973.;
75. Орлов Ю.К. Основы теории доказательства в уголовном процессе / Ю.К. Орлов. М.: Проспект, 2000. - 175 с.;
76. Гражданский кодекс РФ (часть четвертая) от 18.12.2006 № 2Э0-ФЗ. Электронный ресурс: http://www.consultant.ru/document/cons_doc_LAW_64629/dffcf0b87b80ff38f430dc822a0074e76ccd41a0/;
77. ЗРК «Об авторском праве и смежных правах» от 10.06.1996 г. № 6;
78. Антонова Е.В. Применение компьютерных технологий в судебной экспертизе аварийных взрывов // Теория и практика судебной экспертизы в современных условиях: материалы международной научно-практической конференции. М., 2007. С. 460, 461;
79. Никонов В.Н. Допустимость использования математических моделей ДТП в судебном процессе // Теория и практика судебной экспертизы в

современных условиях (г.Москва, 14-15 февраля 2007г.): материалы международной научно-практической конференции. М,, 2007. С.500;
80. ЗРК «О персональных данных и их защите» от 21.05.2013 г. №94-V;
81. Арсеньев В.Д. Основы теории доказательств в советском уголовном процессе. Иркутск, 1970. С.41-42;
82. Белкин Р.С. Собирание, исследование и оценка доказательств. М., 1966. С.28-95;
83. Курс советского уголовного процесса: (Общая часть)/под ред. А.Д. Бойкова И.И. Карпеца. М.: Юрид. лит., 1989. С. 612-615;
84. Винберг А.И., Шавер. Б.М. Криминалистика. М., 1949. С. 195.
85. Волынская О.В.Доказывание истины в уголовном процессе // Вестник МВД РФ. 1999. № 4. С. 128;
86. Зинатуллин З.З. Уголовно-процессуальное доказывание: Учебн. пособие. Ижевск, 2003;
87. Тертышкин, В.М. Нетрадиционные способы и формы собирания и исследования доказательств при расследовании преступлений. Учебное пособие / В.М. Тертышник- Харьков: изд-во Харьк. ин-та внутр. дел, 1994.-56 с.;
88. Хмыров А.А. Косвенные доказательства в уголовных делах. СПб., 2005. С. 11.;
89. Шейфер С.А. Доказательства и доказывание по уголовным делам: проблемы теории и правового регулирования. М.: Норма, 2008. С. 92.;
90. Доля Е.А. О собирании и формировании доказательств по УПК РФ // Новый уголовно- процессуальный кодекс России в действии. Материалы круглого стола. 13.11.2003 г. М., 2004 С. 125.;
91. Доля Е.А. Научно-практический комментарий к УПК РФ / под. ред. В.М. Лебедева, В.П. Божьева. 3-е изд., перераб. и доп. М,, 2007. С. 223.;
92. Семенцов В.А.Формирование доказательств в структуре уголовно-процессуального доказывания // Актуальные проблемы права России и стран СНГ: материалы IX Международной научно-практической конференции 29-30 марта 2007. С. 353-354.;
93. Строгович, М. С. Курс советского уголовного процесса. М., 1968. в двух томах. Т.1. С.302;
94. Балакшин В.С. Доказательства в теории и практике уголовно-процессуального доказывания: Монография. Екатеренбург, 2004. С. 65.;
95. Колмаков В.П. Способы собирания и закрепления судебных доказательств // Социалистическая законность, 1955. № 4;
96. Дектярь, Т.С. Собирание и формирование доказательств в процессе расследования преступлений: дис. ...канд. юрид. наук / Т.С. Дектярь - М., 2001.;
97. Махов В. Н. Теория и практика использования знаний сведущих лиц при расследовании преступлений: автореф. дис. ...докт. юрид. наук. М., 1993. С. 23.;

98. Зезянов В.П. Роль, место и значение специальных знаний в криминалистической методике: автореф. дис. ... канд. юрид. наук: Ижевск, 1994. С. 16-17.;
99. Российская Е.Р. Применение специальных познаний в расследовании преступлений, связанных с движением компьютерной информации // Подготовка специалистов по раскрытию преступлений в области информационных технологий: Материалы Круглова стола (30 марта 2000 г.). М: МГУ, 2000.;
100. Орлов Ю. К. Производство экспертизы в уголовном процессе. М., 1982. С. 26.;
101. Курс советского уголовного процесса. Общая часть // Под ред. А.Д. Бойкова и И. И. Карпеца. М,, 1989. С. 613.;
102. Ищенко Е.П., Топорков А.А. Криминалистика: учебник. 2-е изд., испр. и доп. М., 2006. С. 51.;
103. Исаенко В.Н. Следственные действия и полномочия прокурора по надзору за ними. // Законность. 2003. № 2.;
104. Доля Е.А. Формирование доказательств на основе оперативно-розыскной деятельности: монография / Е.А. Доля - М. Проспект, 2009. 197 с.;
105. Приговор Алмалинский районный суд города Алматы от 4.06.2018 г. в отношении Омарова А.О. Дастарова Б.Е., Рахимова Н.Р. осужденных по ст.188 ч.4 п.1, 208 ч.3 п.1,2, 210 ч.3 п.1,2, 262 ч.1 УК РК. Дело № 7511-17-00-1/1006;
106. Шейфер С.А. Проблемы допустимости доказательств, требуют дальнейшей разработки // Государство и право. 2001. № 10. С. 52.;
107. Когамов М.Ч. Комментарий к уголовно-процессуальному кодексу Республики Казахстан 2014 года. Т.1. Общая часть. – Алматы: Жеті Жарғы, 2015. 648 с. С.491-495;
108. Арсеньев В.Д. Вопросы общей теории судебных доказательств. М., 1964. С. 15.;
109. Официальный сайт Комитета по правовой статистике и специальным учетам ГП РК http://infopublic.pravstat.kz/dtp ;
110. Ожегов С.И. Словарь русского языка: / под ред. Н.Ю. Шведовой. 20-е изд., М.: Рус. яз., 1989. С. 524.;
111. Нормативное постановление ВС РК от 20.04.2018 г. № 4 «О судебном приговоре»;
112. Рыжаков А.П. Проверка достоверности содержащихся в доказательстве сведений как самостоятельный элемент уголовно-процессуального доказывания. Комментарий к ст.87 УПК РФ // Подготовлен для Системы КонсультантПлюс, 2005.;
113. Смирнов А.В., Калиновский К. Б.Уголовный процесс: учебник / А.В. Смирнов, К.Б. Калиновский; под общ. ред. проф. А.В. Смирнова. - 4-е изд., перераб. и доп. - М. : КНОРУС, 2008. - 704 с.;

114. Головко, Л.В. От проверки доказательств к исследованию доказательств: постановка вопроса / В.А. Головко // Академия управления МВД России Материалы межвузовской научно- практической конференции. - М., 2005. - С.5 - 52.;
115. Комментарий к УПК РФ / под ред. И.Л. Петрухина — М.: Велби, 2002. — 896 с.;
116. Аверьянова Т.В.Некоторые проблемы практики судебной экспертизы и пути их решения / Т.В. Аверьянова // Эксперт-криминалист, 2008, № 4. С. 3, 4.
117. Алиев Т.Т., Громов Н.А., Царева Н.П. Понятие и свойства доказательств // Юрист. 2003. №2;
118. Курылев С.В. Основы теории доказывания в советском правосудии. Минск, 1969. С. 156.;
119. Дорохов В.Я. Понятие доказательств // Теория доказательств в советском уголовном процессе / Под ред. Н.В. Жогина. М., 1973. С. 212 -213,
120. Шейфер С.А. Понятие доказательства: спорные вопросы теории // Государство и право. №3.2008. С. 19.;
121. Шалумов М. УПК РФ: Вопросы доказательственного права / М. Шалумов // Законность. - 2004. - № 4;
122. Завидов Б.Д. Кузнецов Н.П. Проблемы доказательств и доказывания в уголовном, судопроизводстве. - 2004. // Электронный ресурс: КонсультантПлюс;
123. Головко Л.В. От проверки доказательств - к исследованию доказательств: постановка вопроса // Фундаментальные и прикладные проблемы управления расследованием преступлений: сборник научных трудов. ч.1. М., 2005. С. 51 – 52;
124. Конституция РК (принята на республиканском референдуме 30.08.1995 г.), (действующая редакция от 10.03.2017 г.);
125. Шейфер С.А. Проблемы правовой регламентации доказывания в уголовно-процессуальном законодательстве РФ. // Государство и право. 1995. № 10. С. 102 - 103.;
126. Кудрявцева А. В. Уровни решения задач как основания разграничения компетенции эксперта и специалиста // 50 лет кафедре уголовного процесса УрГЮА (СЮИ). Материалы международной научно-практической конференции. Екатеринбург, 2005. Ч. 1. С. 488.;
127. Мухин И.И. Объективная истина и некоторые вопросы судебных доказательств при осуществлении правосудия. Л.,1971. С. 95;
128. Белкин, А.Р. Теория доказывания в уголовном судопроизводстве /-М.: Норма, 2005. - 528 с.;
129. «Суд улицы». Как в России работают суды присяжных и зачем Путин предложил расширить их полномочия. 12.02.2020. 11:37. Электронный ресурс: https://www.znak.com/2020-02-

12/kak_v_rossii_rabotayut_sudy_prisyazhnyh_i_zachem_putin_predlozhil_rasshirit_ih_polnomochiya;
130. Уголовно-процессуальное право РФ: учебник / под ред. П.А. Лупинской. М.: Юристъ, 2005. С. 253.;
131. Пашкевич П.Ф. Объективная истина в уголовном судопроизводстве. - М.: Госюриздат, 1961. - 171 с.;
132. Ульянова Л.Т. Оценка доказательств судом первой инстанции. - М.: Юридическая литература, 1959. -180 с.;
УПК Беларусии16.07.1999 г. № 295-З. Принят Палатой представителей 24.06.1999 г. Одобрен Советом Республики 30.06.1999 г.
133. Кудрявцева А.В. Основания и критерии оценки заключения эксперта следователем и судом // Актуальные проблемы совершенствования экономики и законодательства России и стран СНГ: 2001: Материалы международной конференции. Челябинск, 2001.;
134. Давлетов А.А. Нормативная модель общей части доказательственного права в уголовном процесс / А.А. Давлетов // Государство и право.- 1992. - №2
135. Кудрявцева А.В. Концепция теории доказывания в свете проблемы единства процесса / А.В. Кудрявцева // Актуальные проблемы права России и стран СНГ - 2006: материалы VIII международной научно-практической конференции. - Челябинск, 2006.;
136. Костенко Р.В. Оценка уголовно-процессуальных доказательств: монография. - М.: Юрлитинформ, 2012. - С. 28-29.;
137. Левченко О.В. Внутреннее убеждение как метод оценки доказательств в уголовном судопроизводстве. Вестник Волжского университета имени В.Н. Татищева №2(78);
138. Матюшин Б.Т. Внутреннее убеждение судей и оценка доказательств // Вестник МГУ. Сер. 11 «Право». - 1977. - № 3. - С. 58.;
139. Смирнов, А.В. Состязательный процесс. - СПб., 2001. - С. 97.;
140. Мухин И.И. Важнейшие проблемы оценки судебных доказательств/ И.И. Мухин. - Л: Ленинградский университет, 1974. - 108 с.;
141. Кореневский Ю.В. Доказывание в уголовном процессе (закон, теория, практика) / В кн. Доказывание в уголовном процессе. Традиции и современность / под ред. В.А. Власихина. - М.: Юристь, 2000. С. 154.;
142. Миньковский Г.М. Допустимость доказательств. Теория доказательств в советском уголовном процессе. 2-е изд. М., 1973. С. 231, 232.;
143. Соколов А.Ф. Процессуальный порядок признания в суде доказательств, не имеющих юридической силы // Российская юстиция. 1994. №10. С. 14-15.;
144. Карнеева Л.М. Доказательства и доказывание в уголовном процессе. - М., 1994.;
145. Золотых В.В. Проверка допустимости доказательств в уголовном процессе. Ростов-на-Дону, 1999. С. 58.;

146. Типовой закон ЮНСИТРАЛ об электронной торговле и Руководство по принятию 1996 год, с дополнительной статьей 5 бис, принятой в 1998 году. Организация Объединенных Наций, Нью-Йорк, 2006 год, Электронный ресурс: https://www.uncitral.org/pdf/russian/texts/electcom/05-89452_Ebook.pdf;
147. Кореневский Ю.В. Вопрос допустимости доказательств // Прокурор в суде присяжных: Методическое пособие. М., 1995. С. 34;
148. Лупинская П.А. Основания и порядок принятия решений о недопустимости доказательства // Российская юстиция. 1994. №11.С. 2-5;
149. Миронов В. Правила оценки допустимости доказательств // Законность. 2006. №. 5. С. 35;
150. Нуркен Мусабаев, UIB: Карантин ускорил цифровизацию высшего образования. Inform Buro. 21.05.2020. 17.51. Электронный ресурс: https://informburo.kz/special/nurken-musabaev-uib-karantin-uskoril-cifrovizaciyu-vysshego-obrazovaniya-.html ;
151. Коронавирус ускорил цифровизацию экономики в 10 раз». Ведомости. 12.04.2020. 20.02. Электронный ресурс: https://www.vedomosti.ru/technology/characters/2020/04/12/827841-koronavirus-uskoril-tsifrovizatsiyu-ekonomiki ;
152. Технологии карантина. Ускорила ли пандемия цифровизацию? / STARTUP VILLAGE / 21.05.2020. 10:15 -10:55. Электронный ресурс: https://startupvillage.ru/program/session/144 ;
153. «Подозрительность к онлайну сходит на нет»: как карантин повлиял на работу интернет-магазинов / spot / 18.05.2020. 18.20. Электронный ресурс: https://www.spot.uz/ru/2020/05/18/online/ .