АКАДЕМИЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ
ПРИ ГЕНЕРАЛЬНОЙ ПРОКУРАТУРЕ РЕСПУБЛИКИ КАЗАХСТАН

ЖИЛХАЙДАРОВА БАЯН АБЛАЕВНА

# Проблемы и перспективы использования цифровых доказательств в досудебном производстве

Диссертация на соискание степени
магистра юридических наук
по образовательной программе 7М04203 «Юриспруденция»
(научно-педагогическое направление)

Научный руководитель:
Доцент кафедры
прокурорского надзора
Института профессионального
обучения, Утепов Д.П.,
младший советник юстиции
_____

Соруководитель:
Жилкайдаров Р.Р.
_____

г.Косшы, 2024 г.

## РЕЗЮМЕ

Структура диссертационной работы соответствует цели и задачам исследования, состоит из введения, двух разделов, включающих шесть подразделов, сокращений и обозначений, заключения, списка использованной литературы и приложений.

В работе представлена выборка сведений из уголовного законодательства различных государств в сравнении с отечественным законодательством по предмету диссертационного исследования, таблицы, результаты анкетирования.

Цель исследования заключалась в анализе проблем и перспектив развития государственной политики по вопросам использования цифровых доказательств.

Результаты исследования нашли отражение в положениях, выдвинутых на защиту.

## ТҮЙІНДЕМЕ

Диссертациялық жұмыстың құрылымы диссертациялық зерттеудің мақсаты мен міндеттеріне сәйкес құрастырылған, кіріспеден, екі бөлімнен (оның ішінде алты бөлімшеден), қорытындыдан, пайдаланылған әдебиеттер тізімінен және қосымшалардан тұрады.

Жұмыста статистикалық мәліметтері бар кестелер, сауалнама түріндегі социологиялық сауалнама нәтижелері, сонымен қатар диссертациялық зерттеу тақырыбы бойынша дүние жүзінің әртүрлі елдерінің қылмыстық заңнамасынан алынған ақпараттар таңдалған.

Зерттеудің мақсаты цифрлық дәлелдемелерді пайдалану бойынша мемлекеттік саясатты дамытудың проблемалары мен перспективаларын талдау болды.

Зерттеу нәтижелері қорғауға ұсынылған ережелерде бекітілді.

## SUMMARY

The structure of the dissertation is constructed in accordance with the purpose and objectives of the thesis study, consists of an introduction, two sections (including six subsections), a conclusion, a list of used literature and applications.

The paper presents tables with statistical data, the results of a sociological survey in the form of a questionnaire, as well as a sample of information from the criminal legislation of various countries of the world on the subject of a thesis study.

The aim of the study was to analyse the problems and prospects for the development of public policy on the use of digital evidence.

The results of the study are reflected in the protective provisions.

СОДЕРЖАНИЕ

# ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

РК, Казахстан - Республика Казахстан
УК - Уголовный кодекс
УПК -Уголовно-процессуальный кодекс
КР КоАП - Кодекс Республики Казахстан об административных правонарушениях
ГП РК - Генеральная прокуратура Республики Казахстан
ИКТ - информационно- коммуникационная технология
ИС - информационная система
MD5 - это программа хэш-функции
МЦД - международная корпорация данных
GPS - системы глобального позиционирования
ООН - Организация объединенных наций
ЕРДР - единый реестр досудебных расследований
и т.д. - и так далее
и т.п. - и тому подобное
ст. - статья
ч. - часть
ус.номер - условное обозначение номера уголовного дела закрытого доступа

# ВВЕДЕНИЕ

Актуальность проводимого исследования. Стремительное развитие информационно-коммуникационных технологий во всех сферах жизнедеятельности современного электронного правительства в Республике Казахстан, в том числе в сфере осуществления досудебного производств, предопределяют актуальность темы исследования.

Внедрение высоких информационных технологий в уголовный процесс является одной из сфер, позволяющий обеспечить защиту высших конституционных ценностей, минимизировать коррупцию, бюрократию, волокиту в досудебном расследовании, повысить качество, ускорение и уровень прозрачности правосудия.

Глава государства в ежегодном послании народу Казахстана уделяет особое внимание вопросам цифровизации, для достижения национальной конкурентоспособности.

Стратегическим планом развития Казахстана до 2025 г. и государственной программой «Цифровой Казахстан» определен поэтапный переход судебных производств в электронный формат.

Современные тенденции развития общества, общественных отношений, провоцируют эволюционное развитие преступности и совершенствование средств и методов преступного посягательства, в частности на права личности, человека и гражданина, общества и государства в целом, а также устранение последствий такового, требует соответствующего нормативного закрепления и совершенствования практики его применения.

Оценка современного состояния решаемой научной проблемы или практической задачи.

С 2018 года по отдельным категориям уголовного расследования введено электронное уголовное дело в модуле «Е-УД» на базе информационной системы Единого реестра досудебных расследований (далее – ИС ЕРДР), судебное рассмотрение происходит в ИС «Төрелік», посредством публичного сектора участники процесса и адвокаты имеют доступ к оцифрованным материалам, протоколам следственных действий, допроса и экспертиз. Однако в настоящее время на базе информационной системы отсутствует функционал фиксации электронных доказательств и приобщения их к электронному уголовному делу.

Юридическим инструментом правового регулирования нового формата досудебного расследования с использованием информационно-коммуникационных технологий является «Инструкция о ведении уголовного судопроизводства в электронном формате» (далее – Инструкция), утвержденная приказом Генерального Прокурора Республики Казахстан №2 от 03.01.2018 года.

«Ведение электронного судопроизводства заключается в осуществлении досудебного расследования в электронном формате путем ввода электронного документа либо вложения сканированного файла в ИС ЕРДР на основании принятых должностным лицом процессуальных решений и действий».

«Порядок заполнения реквизитов электронных форм определяется «Правилами приема и регистрации заявления, сообщения или рапорта об уголовных правонарушениях, а также ведения ИС ЕРДР», утвержденных приказом ГП РК № 89 от 19.09.2014 года. По всем процессуальным решениям и действиям составляется опись, а также к материалам электронного уголовного дела приобщаются все необходимые медиа-файлы (видео, фото и аудио материалы), отображающих ход следственных действий».

«Данная информационная система предназначена для хранения в цифровом формате всей информации из материалов конкретных уголовных дел. В идеале цифровая информация уголовного дела должна полностью заменить собой бумажный вариант, формируемый высоким уровнем безопасности. Имеется возможность назначения экспертизы по вещественным доказательствам и получения результатов исследования. Однако, сами вещественные доказательства предоставляются на исследование в материальном носителе и приобщаются к электронному уголовному делу».

«Несомненно, в ходе правоприменительной практики все еще встречаются недочеты и ошибки, связанные с техническим оснащением и бесперебойной работой каналов связи, но в целом эти вопросы характерны для первоначальной стадии любого процесса и поправимы в ходе дальнейшей модернизации».

К примеру, в рамках уголовного дела было изъята компьютерная информация о преступной деятельности, которая копируется в CD-R диск, после чего приобщается к уголовному делу на материальном носителе.

Учитывая упростившийся процесс назначения экспертизы, вопросы передачи, фиксации и интеграции цифровых вещественных доказательств требуют научного и практического решения. Действующее уголовно-процессуальное законодательство не в полной мере адаптировано к данной категории информации.

Степень научной разработанности темы исследования. Переход досудебного расследования на электронный формат производства безусловно является предметом исследования ученых, однако, вопрос по безопасной фиксации и интеграции цифровых доказательств в электронном уголовном процессе на сегодняшний день мало исследован. Вместе с тем, данный вопрос интересен для многих практиков и научных деятелей, особенно среди молодых ученых. Среди отечественных работ в данном направлении имеются исследования А.А. Абзелова, А.Т. Ахметова, Н.Ш.Жемпиисов, А.К.Жумадиллаева, Е.Б. Курманбаева, А.Б. Оракбаева, А.В., Д.П. Утепова.

Всесторонним изучением института компьютерных или цифровых доказательств в России занимается большое количество практических и научных работников. К ним, можно отнести: Б.В.Андреев, В.Б.Вехов, В.Н. Долинин, А.Г. Зигура, Н.А. Иванов, Д.Б. Игнатьева, Л.Б. Краснова, С.А. Ковалев, В.А. Мещеряков, У.А. Мусаева, Е.В. Никитина, Б.П. Смагоринский, П.С.Пастухов, Н.А.Попова, Д.М.Цехан, В.Н. Чернышов и другие.

Цель диссертационного исследования состоит в выработке предложений и рекомендаций для оптимизации действующего законодательства с целью использования информационных систем при фиксации и интеграции электронных цифровых доказательств правоохранительными органами.

Задачи диссертационного исследования:

- Определение проблемных вопросов закрепления цифровых доказательств, тенденции реализации и их интеграции на базе «Е-УД».
- Изучение законодательной и нормативной правовой базы в части процессуального закрепления цифровых доказательств.
- Установление наиболее эффективных моделей и практик деятельности зарубежных органов досудебного расследования при фиксации и интеграции цифровых доказательств к электронному уголовному делу.
- Анализ нормативной правовой базы, регламентирующей процесс собирания и использования цифровых доказательств в расследовании уголовных дел.
- Выявление проблем закрепления и использования цифровых доказательств.
- Выработка предложения по разработке функционала фиксации и интеграции цифровых доказательств на базе «Е-УД».

Объектом исследования выступает механизм формирования, способ фиксации и интеграции цифровых доказательств в электронное уголовное дело.

«Предметом 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.

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

Теоретическая база исследования. В магистерской диссертации использованы источники зарубежного и отечественного законодательства, которые сформированы на основе официальных данных и результатов исследований, представленных в печатных изданиях и в сети Интернет, а также материалы правоприменительной практики по рассматриваемым вопросам.

Методы и «методологическую основу исследования составили базовые положения всеобщего метода познания, позволяющие отразить взаимосвязь теории и практики, формы и содержания предмета исследования, процессы развития и качественных изменений, рассматриваемых правовых явлений, а также совокупность общенаучных методов исследования, таких как восхождение от абстрактного к конкретному, анализ, синтез, сравнение, динамические и статистические методы и т.д».

Эмпирическую базу исследования составили разнообразные источники, такие как: документы и законодательные акты (законы, правила сбора и аутентификации цифровых данных, а также правила обработки и представления электронных доказательств), судебные решения и материалы уголовных дел (связанные с использованием цифровых доказательств, а также акцентированные на них), экспертные заключения (связанные с анализом цифровых доказательств), результаты анкетирования (анкетирование представителей органов уголовного преследования по цифровым доказательствам, представителями органов уголовного преследования с выявлением существующих проблем и перспектив), статистические данные (связанные с использованием цифровых доказательств, чтобы определить тенденции и распространенность проблем в данной области).

Обоснование научной новизны.

Исследование объединяет как юридические, так и технические аспекты проблемы, предоставляя глубокий анализ взаимодействия между ними. Это обеспечивает комплексное понимание темы и предоставляет инновационное рассмотрение проблемы.

Вместе с тем, результаты исследования раскрывают новые вопросы и вызывают интерес к дальнейшему исследованию в области цифровых доказательств и их использования в уголовном производстве.

Эти аспекты делают данное исследование научно-новаторским и важным для развития понимания и практики использования цифровых доказательств в досудебном производстве, способствует созданию новых теоретических моделей, описывающих взаимосвязь между цифровыми доказательствами, уголовным процессом и информационными технологиями.

Это может быть полезно для будущих теоретических разработок в данной области.

Положения, выносимые на защиту:

Современные тенденции развития общества, общественных отношений, провоцируют эволюционное развитие преступности и совершенствование средств и методов преступного посягательства, противодействие которым, а также устранение последствий такового, требует соответствующего нормативного закрепления и совершенствования практической деятельности.

По результатам настоящего исследования автор выносит на защиту следующие положения:

1) Внесение в постановление Правительства Республики Казахстан от 9 декабря 2014 года №1291 «Правила изъятия, учета, хранения, передачи и уничтожения вещественных доказательств, изъятых документов, денег в национальной и иностранной валюте, наркотических средств, психотропных веществ, по уголовным делам судом, органами прокуратуры, уголовного преследования и судебной экспертизы».

Дополнить пункт 2 Правил подпунктом 5:

5. Цифровые активы, адрес и ключ криптокошелька, а также «SEED фраза» (мнемоническая фраза), обнаруженные у подозреваемого лица, либо при производстве следственного действия. Вышеуказанное может храниться в программных продуктах, цифровых устройствах, специализированных криптокошельках, на бумажных носителях.

Изъятие цифровых активов (криптовалюта) осуществляется путем их перечисления на криптокошелек органа, осуществляющего досудебное расследование, о чем делается отметка в протоколе.

Для получения доступа к криптовалюте, определяются или идентифицируются данные, относящиеся к криптокошельку (логин, пароль, адрес, «SEED фраза»).

В случае возможности поступления цифровых активов на изъятый криптокошелек (активный) органом уголовного преследования принимается одно из следующих решений:

- направляется ходатайство на биржу об аресте имеющихся цифровых активов на криптокошельке и замораживании всех последующих поступлений;

- запуск программного обеспечения «автоматический снимок» для автоматического снятия поступающих цифровых активов на платформе правоохранительного органа (настройка правил на основе различных технических индикаторов и условий).

Данные меры позволят принимать меры и решения в отношении цифровых активов, учитывая львиную долю незаконного вывода активов за пределы Республики Казахстан безналичным способом.

2) Внедрение технологии- алгоритмизации сбора и учета цифровой информации в качестве вещественного доказательства в рамках уголовного судопроизводства.

- внедрение функционала в ЕРДР «Журнал учета вещественных доказательств и других изъятых по делам денег и ценностей, не признанных вещественными доказательствами, находящимися в камере хранения».

- возможность создания карточки для ввода информации по каждому отдельному вещественному доказательству в базу данных, в том числе сохранение введенных данных также в карточку Е5 в уголовном деле.

Алгоритмизация позволит владеть достоверной картиной процедуры сбора и учета цифровой информации в качестве вещественного доказательства.

3. Авторская классификация цифровых доказательств (Приложение 1).

Полагаем, что с целью повышения эффективности доказательственной деятельности по уголовным делам, при совершении которых использовались IT-технологии, необходимо разработать процессуальные механизмы собирания, проверки и оценки различных видов электронных доказательств. Для этого нужно проанализировать виды электронных доказательств, исследовать основания их классификации.

Это имеет крайне важное значение, потому что для понимания особенностей использования того или иного вида доказательств в уголовно-

процессуальном доказывании необходимо понять его сущность, его особенности, что невозможно без выявления внутренних видовых различий электронных доказательств.

Эта классификация имеет значение, поскольку различна методика установления достоверности, отсутствия вмешательств в исходный документ при проведении судебной экспертизы или оценки специалистом данных видов электронных доказательств

Апробация и внедрение результатов.

Положения исследования магистерской диссертации отражены в опубликованных автором научных статьях:

1. «Правовые основания закрепления и приобщения цифровой информации к материалам электронного уголовного дела» в сборнике материалов международной научно-практической конференции «Теория и практика противодействия киберпреступности» (г.Минск Белоруссия, декабрь 2022г.).

2. «Проблемные Вопросы закрепления и приобщения цифровых доказательств к электронному уголовному делу» в материалах VI международной научно-практической конференции, приуроченной к празднованию 100-летнего юбилея У.С. Сеитова «Развитие современной юридической науки: теория и практика» (г.Косшы, АПО при ГП РК, апрель 2023г.).

3. Теоретический аспект применения цифровых доказательств используется в учебном процессе Высшей школы права Международного университета Астана по дисциплине «Проблемы квалификации уголовных правонарушений».

4. Разработана «Книга учета вещественных доказательств документов, изымаемых или полученных органом, ведущим уголовный процесс», «Журнал учета вещественных доказательств и других изъятых по делам денег и ценностей».

Внедрение результатов подтверждается актами внедрения в учебный процесс (Приложение 2) и в практическую деятельность (Приложение 3).

# 1 Основания закрепления и приобщения цифровой информации к материалам электронного уголовного дела

## 1.1. Теоретические аспекты цифровых доказательств

Современную жизнь невозможно представить без упорядоченного движения информации, которое широко используется во всех сферах общественной жизни. Развитие курса на цифровизацию в Казахстане было дано государственными программами по формированию и развитию "электронного правительства" и "Информационный Казахстан-2020». [1]

Технический прогресс и появление новых средств связи, которые облегчают обмен информацией между людьми, привели к появлению математической теории коммуникации и науки кибернетики (наука о контроле и коммуникации в жизни и технике).

Следствием этих процессов стало появление машинных документов, потому что для обозначения процессов, которые происходили в машинах, алфавитной письменности, как одного из средств общения между людьми, не подходит, и поэтому был заменен на цифровое письмо как язык программирования. Переход к цифровым технологиям ознаменовал новый этап в истории человечества - глобальное информационное общество и замена бумажных документов на механические, то есть такими документами, созданными с использованием информационных и коммуникационных систем, основанных на цифровых технологиях, в которых информация обозначается цифрами. Их восприятие человеком, то есть перевод на алфавитный, требует использования специальных устройств. Один из первых машинных документов в мире под термином сообщение данных ("сообщения данных") был определен в статье 1.2 Типового закона "Об электронной торговле" 1996 года в качестве информации, подготовленной, отправленной, полученной или хранимой с помощью электронных, оптических или аналогичных средств, включая электронный обмен данными (ЭОД), электронную почту, телеграммы, телекс или телефакс, но не ограничиваясь ими [2].

В Республике Казахстан нормативное закрепление вопроса об электронном документе было отражено в 2003 году с принятием Закона «Об электронном документе и электронной цифровой подписи», согласно пункта 12 статьи 2 которого электронный документ представлен в электронно-цифровой форме информации и удостоверен посредством электронной цифровой подписи. [3] Данная норма в аналогичной форме содержится в статье 7 пункт 15 УПК.

Цифровой документ может быть создан, передан, сохранен и преобразован в электронном виде в визуальную форму. Последний отражает данные, которые содержатся в нем в электронном виде или на бумаге в форме, которая может быть воспринята человеком. Такие данные по своей сути представляют собой информацию, представленную в форме, пригодной для ее обработки с помощью электронных средств.

В свою очередь, статья 1 Закона Республики Казахстан "О доступе к информации" [4] определяет информацию как сведения о лицах, предметах, фактах, событиях, явлениях и процессах, зафиксированных в любой форме, то есть могут храниться на материальных носителях или отображаться в электронном виде. Отсюда следует двойственность сущности электронного документа, который, с одной стороны, состоит из информации, а с другой - из материальной среды, на которой фиксируется эта информация.

Другое определение электронного документа содержится в «Правилах отображения и использования электронных документов в сервисе цифровых документов», утвержденных приказом Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан, в качестве электронной формы информации и способа ее документирования. [5] Это означает создание, запись, передачу или хранение информации в цифровой или иной нематериальной форме с помощью электронных, магнитных, электромагнитных, оптических или иных средств, способных воспроизводить, передавать или хранить информацию. Поэтому электронная форма представления информации - это ее документация, которая позволяет воспроизводить информацию в визуальной форме, подходящей для восприятия человека. Поэтому мы вновь говорим о двойственности электронного документа, который в совокупности состоит из информации и материальных носителей - электронных средств связи, на которых эта информация фиксируется и с которыми она воспроизводится.

Информация, которая распространяется в обществе и используется в любых социальных процессах, называется социальной информацией. В правоохранительной сфере юридическая информация меняется - любая информация о законе, его системе, источниках, осуществлении, правовых фактах, правовых отношениях, правопорядке, правонарушениях и борьбе с ними, их предотвращении и т.д.

Из этого следует, что юридическая информация на ее функциональной основе может быть связана с правовым конфликтом, возникшим вокруг нее или в ней. Для его решения используются различные правовые источники и процессуальные формы. Очевидно, что такая информация, имеющая отношение к сфере уголовного процесса в виде предметов материального или виртуального мира, может приобретать доказательное значение, признаваться доказательством.

В статье 118 УПК в уголовном судопроизводстве признаются фактические данные, полученные в соответствии с процедурой, предусмотренной настоящим Кодексом, на основании которых следователь, прокурор, следственный судья, суд устанавливает наличие или отсутствие фактов и обстоятельств, имеющих отношение к досудебному расследованию и подлежащих доказыванию. [6] Для нашего исследования в этом определении ключевое значение имеет такая особенность, как "фактические данные".

Рассмотрим эти вопросы более подробно. В большом юридическом словаре данные определяются как:

1) информация, показатели, необходимые для ознакомления с тем-то-то-то-то или для определенных выводов, решений;

2) тексты, таблицы, инструкции, сведения о фактах, явлениях и т.д., представленные в буквенно-цифровой, цифровой, текстовой, звуковой или графической форме, которые хранятся в электронных компьютерах (далее именуемые компьютерами) и отправляются и обрабатываются. [7]

В то же время Закон «О доступе к информации" определяет информацию как информацию и/или данные, которые могут храниться на материальных носителях или отображаться в электронной форме. То есть термины "фактические данные", "информация" и "информация" являются синонимами. Однако под влиянием процессуальных норм они приобретают особое содержание. Кроме того, в Законе "Об электронных документах и электронной цифровой подписи" данные определяются как информация, представляемая в форме, пригодной для ее обработки электронными средствами. [3]

Следует также отметить, что в настоящее время, с учетом развития онлайн торговли, участились случаи совершения уголовных правонарушений с помощью компьютерных технологий. Поэтому очевидно, что судьба уголовного судопроизводства, а именно формирование информации в качестве доказательства и ее оценка с точки зрения наличия таких качественных критериев, как принадлежность, достаточность, надежность, относимость и допустимость зависит от того, каким образом можно фиксировать информацию.

В свою очередь, проверка подлинности цифровых доказательств напрямую зависит от способа их сбора и фиксации. Ответом на такие вызовы является цифровизация и оптимизация уголовного преследования, особенно на досудебной стадии, что привело к внедрению научно-технических достижений и появлению новых средств связи с компьютерами.

В результате оцифровки уголовного процесса возникает важный аспект - возможность создания и применения электронных документов в качестве доказательства, параллельно с их бумажными аналогами, их заменой. Это первое и ключевое последствие цифровизации уголовного процесса. С возрастанием числа электронных документов возникают вопросы об их использовании как доказательств.

В соответствии со статьей 118 УПК, такие материалы, включая другие источники информации (в том числе электронные), признаются документами в качестве доказательств.

Документ, согласно уже отмеченному, является материальным объектом, специально предназначенным для сохранения информации, содержащего данные, зафиксированные письменными, звуковыми или графическими средствами и другими, которые могут быть использованы в качестве доказательств фактов или обстоятельств, установленных в процессе уголовного расследования. Исходя из этих положений, можно заключить, что документ в

качестве доказательства сочетает в себе форму фиксации информации (физический объект, хранящий информацию и его характеристики) и саму информацию (данные, которые могут служить доказательством).

Тем самым, имеет большую значимость непосредственной формы существования информации, без которой она ничто. По мнению ученых, разница между информацией и доказательствами заключается в их использовании.

Доказательства - это формальный термин информации, которая является частью судебного процесса в том смысле, что она используется для доказывания или опровержения преступлений. Таким образом, информация является первоначальной, не обработанной формой доказательства: все доказательства являются информацией, но не вся информация является доказательством.

Основанная на доказательствах информация связывает предполагаемое преступление (уголовная база) с подозреваемыми преступниками: она содержит доказательства того, как такие лица могли совершить его.

При анализе доказательственной ценности электронной информации важно учитывать, что значимость заключается не в физических характеристиках материального носителя компьютерной информации - его форме, текстуре и внешнем виде, как это характерно для материальных доказательств, а в самом содержании передаваемой информации.

Введя специальный термин «виртуальный след», В.А. Мещеряков определил его как «…любое изменение состояния автоматизированной информационной системы (образованного ею “кибернетического пространства”), связанное с событием преступления и зафиксированное в виде компьютерной информации (то есть информации в виде, пригодном для машинной обработки) на материальном носителе, в том числе на электромагнитном поле». [8]

Вместе с тем, В.А. Мещерякову принадлежит авторство понятию «электронно-цифровой объект», определив его как «помеченную систему дискетных электронных сигналов, предназначенную для обозначения (по установленной системе кодирования) какой-либо информации и представленную в форме, пригодной для её автоматизированной обработки, хранения и передачи с использованием средств вычислительной техники (компьютеров)» [9].

Эти объекты используются автоматизированными информационными системами. Этот класс должен занимать промежуточное положение между представлением информации в виде дискретных электронных сигналов и объектами, содержащими конкретное смысловое значение (информацию о чем-либо), которые могут быть восприняты человеком напрямую.

В наиболее полном виде теория о цифровых следах преступлений сформулирована В.Б. Веховым. Он определяет такие следы следующим образом: «Электронно-цифровой след - это любая криминалистически важная компьютерная информация, то есть данные (сообщения, информация), находящаяся в цифровой форме, зарегистрированная на носителе с помощью

электромагнитных сигналов. Эти следы представляют собой материальные, невидимые следы». [10]

В основе механизма их образования лежат электромагнитные взаимодействия двух и более материальных объектов – объективных форм существования (представления) компьютерной информации.

«Для компьютерной информации неприменимо механическое элементарное отражение фактов. Механизм формирования компьютерной информации определяется алгоритмом, который задан разработчиком (коллективом разработчиков) и реализуется в конкретной программе; таким образом, программа является средством отражения фактов. В данном случае мы имеем дело с отражением, происходящим посредством аппаратных и программных средств опосредованно через интеллектуальное сознание человека (разработчика программы)» [11].

Информационные объекты, используемые при совершении киберпреступлений, могут быть классифицированы как "вещественные доказательства" в рамках теории судебных доказательств.

Однако, с учётом их техногенной природы, более точным будет рассматривать их как отдельный вид вещественных доказательств - "техногенные объекты" или "техногенные процессы".

Вещественные доказательства - это элементы той среды, в которой произошло преступление. Они всегда отражают изменения, произошедшие в окружающей среде в результате преступления, и служат средством их установления. Эти изменения могут быть самыми разнообразными: перемещение предметов, их повреждение, уничтожение, создание новых объектов и т.д.

Таким образом, вещественные доказательства - это предметы, являвшиеся частью среды, в которую преступлением или другими установленными по делу обстоятельствами были внесены (или должны быть внесены) изменения. Используя более простые и понятные формулировки, уточнена классификация информационных объектов - вещественных доказательств как часть среды. Расширено описание изменений, отражаемых вещественными доказательствами, дана более чёткая связь между вещественными доказательствами и изменениями в среде преступления.

Таким образом, вещественные доказательства необходимо рассматривать как предметы, бывшие частью той среды, в которую преступлением либо иными установленными по делу обстоятельствами внесены (или должны быть внесены) какие-либо изменения. [12]

Допуская отражение на информации отображение специфической, электронной (цифровой) среды, полагаем обоснованным применение к некоторым электронным доказательствам формулировку «цифровой след».

Электронное доказательство понимается как объект, несущий информацию, имеющую смысловое значение, и существующий только в электронной среде. [13]

Утверждая, что электронные доказательства возникают из электронной среды, они не всегда могут быть квалифицированы как документы. Есть электронные доказательства – документы (электронные), и есть электронные вещественные доказательства.

Вопрос о форме электронного доказательства вызывает разногласия из-за неоднозначного понимания концепции "вещественного доказательства" в теории. Споры касаются не столько физических особенностей электронных доказательств, сколько самого определения вещественного доказательства. Некоторые ученые пришли к выводу, что возможно имеет смысл отказаться от данного понятия и исключить вещественное доказательство из перечня видов доказательств, упомянутых в ст.118 УПК РК.

Вместе с тем возникает вполне обоснованный вопрос о том, достаточны ли вышеупомянутые положения УПК для идентификации электронных (цифровых) доказательств в качестве документов, необходимо ли идентифицировать такие доказательства в качестве отдельного процессуального источника. Проанализировав мнения ученых, мы отмечаем, что эта проблема не обязательно решается отечественными учеными.

В данном случае будет интересна работа Конвенции Совета Европы «О киберпреступности, о расширении сотрудничества и раскрытия электронных доказательств», подписанной в Будапеште 23.11.2001 года, [14] стала инструментом, участниками которого являются государства во всех частях мира и который оказывает воздействие в каждом из этих регионов.

В 2003 году Конвенция была дополнена протоколом относительно введения уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем (СЕД № 189, далее — «Первый протокол»). [15] Первые такого рода рекомендации били опубликованы в 2018 году. В обновленные рекомендации-2024 были включены сведения о гибридных угрозах, которые могут негативно отразиться на безопасности выборов — вмешательство иностранных агентов посредством манипуляции информацией, распространение дезинформации в соцсетях, технологии искусственного интеллекта (ИИ), включая функцию Deepfake.

С момента открытия Конвенции для подписания в 2001 году информационно-коммуникационные технологии изменились и поразительным образом преобразили общества во всем мире. Вместе с тем с тех пор наблюдался значительный рост случаев использования технологий в преступных целях. Сегодня многие Стороны считают, что киберпреступность представляет собой серьезную угрозу правам человека, верховенству права и функционированию демократических обществ.

Угрозы, связанные с киберпреступностью, многочисленны. Например, сексуальное насилие, совершаемое в Интернете в отношении детей, и другие правонарушения против чести и достоинства физических лиц; кража и неправомерное использование персональных данных, влияющее на частную

жизнь физических лиц; вмешательство в выборы и другие нападки на демократические институты; атаки на критическую инфраструктуру, такие как распределенные атаки типа «отказ в обслуживании» (Ddos-атаки) и атаки вирусов вымогателей; или незаконное использование подобных технологий для террористических целей. В 2020 и 2021 годах во время пандемии Covid-19 в государствах наблюдался значительный рост киберпреступлений, связанных с Covid-19, включая атаки на больницы и медицинские учреждения, разрабатывающие вакцины от вируса, неправомерное использование доменных имен для продвижения фальшивых вакцин, лекарств и методов лечения и другие формы мошеннических действий.

Несмотря на рост технологий, основанных на данных, и опасное распространение и развитие киберпреступности, концепции, охватываемые в Конвенции, являются технологически нейтральными с тем, чтобы нормы материального уголовного права могли применяться как к существующим, так и к будущим технологиям, и чтобы Конвенция продолжала иметь ключевое значение в борьбе с киберпреступностью.

К сожалению, на данный момент Казахстан не ратифицировал Конвенцию, в связи с чем многие моменты противодействия киберпреступности в отечественной практике западают.

Стоит отметить и определить для себя неизбежность информационных угроз правам человека и гражданина, общества и государства в целом, что ведет в направлении к следующим целям:

1. гармонизация составов уголовных правонарушений в национальных нормах уголовного материального права и связанных с ними положений в области киберпреступлений;

2. обеспечение внутренних уголовно-процессуальных полномочий, необходимых для проведения расследований и судебных разбирательств в связи с такими правонарушениями и иными уголовно наказуемыми деяниями, совершенными посредством компьютерной системы или связанными с использованием электронных доказательств других преступлений;

3. создание быстрых и эффективных механизмов международного сотрудничества.

В «Концепции цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023 - 2029 годы», регламентированы дополнительные меры, направленные на укрепление кибербезопасности страны, в частности предусмотрены мероприятия по технической защите, совершенствования радиоконтроля, защиты персональных данных и повышения осведомленности населения. Однако в полной мере они не соответствуют требованиям, так как полагаем, что назрела необходимость дать определение этому явлению следующим образом:

1) либо путем включения в УПК специального определения концепции электронных доказательств;

2) или внесения таких изменений в общее определение доказательств, которые позволили бы с должной точностью и предсказуемостью утверждать, что новое определение охватывает доказательства в электронной форме.

В УПК РК, с учетом положений статей 118-120 не запрещено, а даже отражена возможность различной формы фиксации документов, представляющих фактическую значимость для дела.

Однако формат сбора таких материалов и документов в специализированной статье не конкретизирован.

Для определения вопроса следует установить сам предмет вещественного доказательства отдельно в качестве нового его вида.

Так, в соответствии со ст.99 Конвенции, электронное доказательство рассматривается в качестве информации в электронной (цифровой) форме, включающую фактические данные об обстоятельствах уголовного правонарушения, в частности электронные документы (текстовые документы, графические изображения, фото-, видео- и звуковые записи и т.д.)веб-сайты (страницы) и другие данные в электронной форме.

Такие данные могут храниться, в частности, на портативных устройствах (карты памяти, мобильные телефоны и т.д.), серверах, системах резервного копирования, других местах хранения данных в электронной форме (включая Интернет), что требует привлечения соответствующего специалиста. [16]

В аспекте нашего исследования интересным является опыт других стран по внедрению уголовно-процессуальных инструментов для получения доказательственной информации из электронных средств.

Например, законодательство балтийских государств по-разному решает вопрос о принадлежности таких доказательств к видам материальных ценностей, собранных в ходе разбирательства. Уголовно-процессуальным законодательством Литвы предусмотрена классификация электронных доказательств в качестве документов, а в Эстонии -как вещественные доказательства. В отличие от этих положений УПК Латвии проводит различие между электронными доказательствами в качестве отдельного источника (статья 136 УПК) и определяет их в качестве информации в электронной форме об обстоятельствах, связанных с объектом доказательства, которое было обработано, хранение или передача данных с использованием устройств или автоматизированных систем обработки данных.

Мы также располагаем другим опытом в области правового регулирования получения доказательств путем обращения к электронным источникам. Например, французское доказательное право, основанное на принципе свободы доказательств, закрепленное в статье 17. 427 Уголовно-процессуального кодекса Франции, отличается широким следственным инструментарий; который содержит как модифицированные традиционные следственные действия, так и новые "высокотехнологичные".

В соответствии с этим принципом, законом не запрещена возможность установления обстоятельств уголовных правонарушений любым способом

доказывания, при этом судебное решение провозглашается на основе оценки доказательств с учетом внутреннего убеждения судьи. Если доказательства собраны органами уголовного преследования, они допускаются при условии их надлежащего получения без нарушения прав защиты. Результаты внедрения электронных доказательств отражены в Руководстве по электронным доказательствам в гражданском и административном производстве, принятом Комитетом министров Совета Европы 30 января 2019 года. (далее - Руководство) [17].

Хотя эти принципы касаются гражданского и административного производства, мы считаем, что некоторые из их руководящих положений могут служить практическим инструментом для формирования унифицированных подходов к использованию электронных доказательств в национальной правоприменительной практике, в том числе в области уголовного правосудия. В частности, в Руководящих принципах говорится, что под электронными доказательствами понимаются любые доказательства, содержащиеся или полученные с помощью любого устройства, функционирование которого зависит от программного обеспечения или данных, хранящихся или передаваемых через компьютерную систему или сеть. Поэтому двойственность информационных и материальных средств - электронных средств связи, на которых закреплена цифровая информация, - вновь поражает.

Что касается основных принципов в исследуемой области, то проанализированный документ включает следующее:

1) вопрос об урегулировании потенциальной доказательственной ценности электронных доказательств принадлежит судам в соответствии с национальным законодательством;

2) электронные доказательства должны оцениваться так же, как и другие виды доказательств, в частности в отношении допустимости, надежности, точности и целостности;

3) обработка электронных доказательств не должна ставить стороны в невыгодное положение или давать справедливое преимущество одной из них;

4) в целом суды не должны отрицать действительность электронных доказательств только потому, что они не имеют расширенной формы. Электронная подпись, имеющая определенные или аналогичные гарантии.

Наконец, принимая во внимание более высокий риск возможного уничтожения или утраты электронных доказательств по сравнению с неэлектронными доказательствами, Руководящие принципы обязывают государства - члены СЕ установить процедуры для безопасного привлечения и сбора электронных доказательств, а также их сохранение на основе таких компонентов, как ясность, доступность, целостность, надежность и, при необходимости, конфиденциальность и конфиденциальность.

Таким образом, в проанализированном документе электронное доказательство не рассматривается в качестве новой категории доказательств. Основная дискуссия вращается вокруг таких вопросов, как вопрос о том,

являются ли электронные доказательства новым типом доказательств, а если нет, то какое место они занимают в системе источников доказательств, а именно необходимость соотнесения к вещественным или письменным.

Д.М. Цехан утверждает, что цифровая информация и ее носители, учитывая уникальные характеристики, прежде всего нематериального характера, не могут быть отнесены к какой-либо классификационной группе, и предлагает ввести новую категорию "цифровое доказательство" [18, стр. 259].

Ссылаясь на достижения науки в изучении электронных доказательств автор, заключает, что цифровую доказательственную информацию следует получать из отдельно назначенного процедурного источника - носителя цифровых доказательств, которым будет соответствующий файл.

Таким образом, формируется цифровая триада: цифровой носитель данных (машинный носитель) - источник цифрового доказательства (цифровой носитель информации - файл) - цифровое доказательство (информация).

Поэтому, с целью обеспечения эффективности правового регулирования назрела необходимость выделения носителей цифровых доказательств в отдельный процессуальный источник, учитывая характер связи, механизм формирования, способ восприятия, что разграничивает как от материальных доказательств, так и от документов.

В то же время ученые ссылаются на невозможность использования таких характеристик, как форма фиксации информации, признаки носителя информации или метод воспроизведения данных для их разграничения. Предлагается определить "электронное доказательство" как информацию, хранящуюся в электронной форме на любых электронных носителях, электронных устройствах или электронных информационных системах, которая отвечает требованиям уголовно-процессуального законодательства Республики Казахстан.

В то же время важно отметить, что рассматривать также стоит не в контексте отдельного нового источника доказательств, а явления как такового. Следует обратить внимание на дуалистический характер электронной информации, поскольку по своей сути она является нематериальным объектом, но ее необходимо закрепить на носителе для обеспечения долгосрочного хранения, транспортировки, и т.д. Носителем информации является материальный объект, предназначенный для записи, передачи и хранения информации, наличие различных типов носителей информация дополняет и расширяет возможности их использования.

Из этого следует, что электронная информация становится доказательством при ее использовании в уголовном судопроизводстве и процессуальных процедурах в соответствии с УПК. В сущности, это представляет собой объединение формы и содержания электронного доказательства с материальным носителем информации и его нематериальной природой, то есть обязательную связь электронного документа с материальным носителем, без которого он не может существовать.

Таким образом, мы делаем вывод о том, что цифровая информация является одним из видов документарной информации как таковой, которая создается, хранится и передается с использованием электронного оборудования. И не имеет значения, в какой форме создается процессуальный документ - бумажный или электронный, он может выполнять лишь одну функцию - быть доказательством в уголовном процессе. Выводы и перспективы дальнейших исследований. В результате мы отмечаем, что электронные документы представляют собой определенный правовой феномен, участие которого в судебных процедурах в качестве доказательства возможно только на условиях использования технических и программных средств для получения информации, которая на них закреплена. они не могут восприниматься напрямую, а требуют использования технических и программных средств для получения соответствующей информации с использованием метаданных, которые характеризуют ее и могут идентифицировать ее, определить происхождение или историю создания доказательств; а также соответствующие даты и время его создания.

## 1.2 Правовые аспекты цифровых доказательств в Республике Казахстан

Благодаря стремительному развитию информационно-коммуникационных технологий в Республике Казахстан стало возможным ведение досудебного расследования и их судебного рассмотрения в электронном формате. [19, с.49-52].

Стратегическим планом развития Республики Казахстан до 2025 года, утвержденным Президентом Республики Казахстан от 15 февраля 2018 года, правоохранительным органам поручено обеспечить поэтапный переход уголовных дел в электронный формат. [20]

Ведение электронного уголовного дела Генеральной прокуратурой реализовано в модуле Е-УД на базе информационной системы Единого реестра досудебных расследований (далее - ИС ЕРДР), а судебное рассмотрение происходит в ИС «Төрелік» (перевод с казахского – «арбитраж»). Однако сейчас в информационных системах отсутствует функционал фиксации электронных доказательств и приобщения их к электронному уголовному делу.

В настоящее время, электронным доказательством являются сведения о фактах, имеющих значение для установления обстоятельств, подлежащих доказыванию по уголовному делу, зафиксированные в форме цифровой информации, восприятие содержания которой невозможно без применения технических средств.

При оценке допустимости электронных доказательств должно учитываться следующее:

1) надежность способа, с помощью которого обеспечивалось ограничение на внесение изменений в цифровые данные;

2) надежность способа, при помощи которого идентифицировался его составитель;

3) правильность способа фиксации информации.

Указанное свидетельствует, что при формировании электронного уголовного дела необходимо учесть особенность таких доказательств. «Инструкция о ведении уголовного судопроизводства в электронном формате» (далее - Инструкция) является юридическим инструментом правового регулирования нового формата досудебного расследования, которая утверждена приказом Генерального Прокурора Республики Казахстан. [21]

Ведение электронного судопроизводства заключается в осуществлении досудебного расследования в электронном формате путем ввода электронного документа либо вложения сканированного файла в ИС ЕРДР на основании принятых должностным лицом процессуальных решений и действий.

Порядок заполнения реквизитов электронных форм определяется «Правилами приема и регистрации заявления, сообщения или рапорта об уголовных правонарушениях, а также ведения ИС ЕРДР», утвержденные приказом ГП РК № 89 от 19.09.2014 года. [22]

Конечно же, по всем процессуальным решениям и действиям составляется опись, а также к материалам электронного уголовного дела приобщаются все необходимые медиа-файлы *(видео, фото и аудио материалы)*, отображающих ход следственных действий.

При этом, специальные шифровальные комплексы обеспечивают безопасность защищенных каналов связи и гарантируют тайну следствия, препятствуют искажению собранных доказательств, либо разглашению охраняемой законом тайны. Но вместе с тем, участники уголовного процесса не ограничены в использовании своих прав и обязанностей в рамках действующего уголовно-процессуального законодательства.

В частности, пункт 26 Инструкции предусматривает, что участники процесса получают доступ к соответствующим материалам электронного уголовного дела посредством функционала «Публичный сектор» ИС ЕРДР (Qamqor.gov.kz), через который возможна подача ходатайств *(жалоб)* и их своевременное рассмотрение.

Для работы с «Публичным сектором» нужно лишь подключение к Интернету и электронно-цифровая подпись.

По данным Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан за 11 месяцев текущего года, число оконченных уголовных дел в электронном формате по правоохранительным органам составило 80 % (55092 из 69193), в т.ч. с рассмотрением их суде 74 % (32140 из 43654). (приложение №1)

Также, электронное судопроизводство положительно повлияло на процессуальную экономию времени и финансовых средств, сокращение сроков расследования, получения электронных санкций и других справочных

материалов, прозрачности уголовного процесса, обеспечение прав участников, системный и качественный ведомственный контроль, и прокурорский надзор.

В частности, орган ведущий уголовный процесс уже не обременен вопросами затрат на почтово-телеграфную корреспонденцию, командировочных затрат и иных административных ресурсов. Уведомления участникам уголовного процесса поступают посредством СМС сообщений (онлайн).

Несомненно, в ходе правоприменительной практики все еще встречаются недочеты и ошибки, связанные с техническим оснащением и бесперебойной работы каналов связи, но в целом эти вопросы характерны первоначальной стадии любого процесса и поправимы в ходе дальнейшей модернизации.

В целях дальнейшего совершенствования электронного судопроизводства в ИС ЕРДР планомерно запущена такая опция как – «интеллектуальный помощник следователя *(помощь при расследовании)*» и «OFFLINE приложение». Система ориентирует молодого следователя принимать правильные процессуальные действия и не будет допускать принятие незаконных решений.

Кроме того, в системе имеется возможность назначения экспертизы по вещественным доказательствам и получения результатов исследования. Однако, сами вещественные доказательства предоставляются на исследование в материальном носителе и приобщаются к электронному уголовному дело.

К примеру, в рамках уголовного дела было изъято компьютерная информация о преступных махинациях, которая копируется в CD-R диск, после чего приобщается к уголовному делу на материальном носителе.

Учитывая упростившийся процесс назначения экспертизы, остались неразрешёнными вопросы передачи вещественных доказательств. По нашему мнению, следует более шире применять возможности цифровых технологий в закреплении цифровых доказательств. Фиксацию и интеграцию цифровых доказательств (следы, существующие на электронно-цифровых носителях средств вычислительной техники и в виртуальном пространстве) необходимо автоматизировать без привлечения специалиста в данной области, используя информационные системы, устройства для подключения с блокираторами связи и создавая безопасный канал передачи данных (без доступа к сети интернет).

При этом доказательством по уголовному делу должен признаваться не электронный носитель, а сама цифровая информация. Следователем выносится соответствующее постановление, в котором указывается на электронный характер доказательственной информации, определяется носитель, на котором она хранится при уголовном деле, наименование и вид программного обеспечения, информационного сервиса с помощью которого можно осуществить доступ к сведениям, имеющим значение для уголовного дела.

При указанных условиях внесения какого-либо дополнения или изменения в нормы действующего кодифицированного уголовно-процессуального законодательства Республики Казахстан не требуется, однако есть необходимость конкретизировать условия и алгоритмы осуществления

фиксации ряда характерных некоторым видам преступлений электронные доказательства, что в последующем будет использовано в качестве базы.

Так, в ставшее наиболее актуальными, «Правила изъятия, учета, хранения, передачи и уничтожения вещественных доказательств, изъятых документов, денег в национальной и иностранной валюте, наркотических средств, психотропных веществ, цифровых активов по уголовным делам судом, органами прокуратуры, уголовного преследования и судебной экспертизы» предлагаем внести изменения в части изъятых цифровых активов, а именно дополнив категорией «цифровые активы» перечень вещественных доказательств.

Вместе с тем, с учетом специфики цифрового доказательства, пункт 4 данных Правил следует дополнить подпунктом 5 относительно алгоритма изъятия, фиксации, учета и хранения, выразив в следующей редакции:

5) цифровые активы, адрес и ключ криптокошелька, а также «SEED фраза» (мнемоническая фраза), обнаруженные у подозреваемого лица, либо при производстве следственного действия. Вышеуказанное может храниться в программных продуктах, цифровых устройствах, специализированных криптокошельках, на бумажных носителях.

Изъятие цифровых активов (криптовалюта) осуществляется путем их перечисления на криптокошелек органа, осуществляющего досудебное расследование, о чем делается отметка в протоколе.

Для получения доступа к криптовалюте, определяются или идентифицируются данные, относящиеся к криптокошельку (логин, пароль, адрес, «SEED фраза»).

В случае возможности поступления цифровых активов на изъятый криптокошелек (активный) органом уголовного преследования принимается одно из следующих решений:

- направляется ходатайство на биржу об аресте имеющихся цифровых активов на криптокошельке и замораживании всех последующих поступлений;
- о запуске программного обеспечения «автоматический снимок» для автоматического снятия поступающих цифровых активов на платформе правоохранительного органа (настройка правил на основе различных технических индикаторов и условий).

## 1.3 Зарубежный опыт использования цифровых доказательств в уголовном судопроизводстве

В эпоху цифровых технологий новые технологии и достижения в области компьютерных разработок изменили осознание того, как потенциально значимые доказательства преступлений будут оцениваться в международном уголовном праве. Новые технологии делают возможным архивирование данных, связанных с вооруженным конфликтом, из широкого спектра источников, включая, помимо прочего, спутниковые и геопространственные изображения,

системы глобального позиционирования (GPS), данные мобильных телефонов, видео, фотографии, социальные сети и другие данные.

На примере практики Международного уголовного суда (МУС или «Суд») рассмотрены ряд важных проблем, связанных с проверкой подлинности цифровых доказательств, и адаптацией к этим изменениям. Учитывая тот факт, что положения МУС ратифицированы 134 государствами мира, полагаем следует рассмотреть вопрос его практику относительно цифровых доказательств. [23]

Именно судебная практика, как конечная стадия оценки соблюдения процессуальных требований «обращения» с вещественными доказательствами, а также с учетом специфики уголовно-процессуального законодательства, вызывает огромный интерес в части результативности позитивности и негативности опыта.

Созданный в 1998 году МУС является первым в мире постоянным международным уголовным судом, которому поручено расследование и уголовное преследование за самые тяжкие преступления, представляющие опасность для международного сообщества: геноцид, преступления против человечности, военные преступления и преступления против мира и безопасности.

На момент своего создания МУС, возможно, не мог предвидеть грядущую революцию в цифровых технологиях и ее влияние на Суд.

Однако, спустя два десятилетия, процедуры Суда по доказыванию и проверки подлинности доказательств не соответствуют развитию современной эпохи. Хотя новые технологии во многом способствуют «осовремениванию» уголовного процесса, связанного с совершением международных преступлений, вместе с тем Суд не готов в полном объёме взять на себя сложную задачу по аутентификации и исследованию (проверке) цифровых доказательств.

Международные суды, уже давно пытаются оценить сложные области вне своей компетенции, включая, среди прочего, судебно-медицинскую, баллистическую, геномную экспертизы и многое другое.

По настоящее время остается проблемным вопросом обеспечение судебного контроля за законностью и достоверностью экспертных исследований в данном случае.

Дебаты относительно оценки научных доказательств служат аналогичной полезной отправной точкой для разработки соответствующей системы судебного контроля для аутентификации цифровых доказательств, что позволяет разрешить следующие вопросы относительно и отечественного законодательства:

1. Определить проблемы и риски нынешнего подхода к аутентификации и проверке цифровых доказательств;

2. Изучить мнения ученых по поводу анализа научных данных как аналогичной проблемы;

3. Определить наиболее прагматичный подход к проверке подлинности цифровых доказательств в дальнейшем.

Несмотря на то, что существует множество серьезных проблем с представлением цифровых доказательств в Суд, особенно в сборе и сохранении цифровых доказательств, основное внимание уделено проверке подлинности цифровых доказательств.

В условиях развития технологий открываются возможности для модернизации уголовного судопроизводства, связанного с международными, трансграничными уголовными правонарушениями, где, однако, Суд не может в полной мере реализовать функции по аутентификации и проверке цифровых доказательств.

Прежде чем продолжить, важно уточнить термины, которые будут представлены в последующих разделах.

Аутентификация — это одновременно термин кибербезопасности и юридический термин, используемый для описания процесса доказательства того, что цифровой файл является подлинным или не поддельным. По сути, аутентификация гарантирует, что рассматриваемый элемент является тем, за что он выдает себя, и что он не подвергался манипуляциям или изменениям.

Верификация (проверка) — это процесс обеспечения того, чтобы утверждение или утверждение, сделанное в каком-либо средстве связи, было надежным и/или правдивым.

Верификация и аутентификация тесно взаимосвязаны, но различны. Например, возможно, что подлинный цифровой файл либо правдив, либо ложен; однако недостоверное доказательство следует считать предположительно не поддающимся проверке, поскольку было обнаружено, что этот цифровой файл был подделан, преобразован или изменен.

В МУС судьям предоставлена широкая свобода действий в принятии доказательств по своему усмотрению. Римский статут («Статут») является учредительным договором МУС и служит руководящим правовым инструментом Суда. Именно ратификация Римского статута 134 государствами мира, позволяет более широко рассмотреть международный и зарубежный опыт и характер его эффективности. [24]

Правила процедуры и доказывания (RPE или «Правила», приложение к «Римскому статуту») предлагают дополнительную конкретику в отношении приема и обработки доказательств. Правило Регламента гласит: «Палата имеет право в соответствии с правом усмотрения, описанным в пункте 9 статьи 64, свободно оценивать все представленные доказательства, чтобы определить их относимость или допустимость в соответствии со статьей 69 Статута.

Другими словами, судьи обладают полномочиями принимать решения по любым вопросам, возникающим в отношении подлинности или проверяемости цифровых доказательств. Суд во многом полагается на усмотрение и опыт судей при надлежащей оценке принятых доказательств.

Этот гибкий подход к допуску доказательств также является результатом ограничений полномочий МУС. В отличие от внутренних уголовных расследований, где правоохранительные органы имеют право принуждать стороны посредством вызова в суд и ордеров на обыск, следственные группы МУС не обладают такими полномочиями.

Общий подход МУС к допустимости доказательств включает последовательный трехэтапный тест, в котором должен быть соблюден каждый из следующих критериев: относимость и доказательная ценность.

Относимость: «В соответствии со статьями 64(9)(a) и 69(4) Римского статута и далее сформулированными в прилагаемых Правилах процедуры и доказывания, доказательства будут считаться относящимися к делу, если «представленные доказательства подтверждают наличие факта и проблема более или менее вероятная». Другими словами, доказательства могут считаться относящимися к делу, если они *prima facie* имеют отношение к делу». [25]

Доказательная ценность: Доказательная ценность обычно понимается как то, является ли доказательство достаточно полезным для доказательства важной части судебного разбирательства. По сути, доказательная ценность измеряет степень, в которой представленные доказательства могут повлиять на определение факта или проблемы. Согласно статье 69 Статута, доказательная ценность предмета должна быть оценена, прежде чем он может быть принят в качестве доказательства. [26]

Другими словами, вес, придаваемый доказательствам, должен полностью обеспечивать (не нарушать) права всех сторон и не быть явно несправедливым по отношению ни к обвинению, ни к защите, а также не наносить ущерба принципу справедливости судебного разбирательства.

Основное внимание в этом исследовании уделяется механизмам и проблемам аутентификации цифровых доказательств, и соответствующим процессам судебного рассмотрения. Однако концепции проверки и аутентичности могут запутаться, поскольку судьи начинают принимать решения о приемлемости, релевантности, доказательной ценности и весе цифровых доказательств.

Например, в деле «Прокурор против Жан-Пьера Бембы Гомбо» сторона обвинения предоставила десять аудиозаписей радиопередач, чтобы установить предысторию и контекст конфликта. Когда защита высказала возражения против допуска этих записей, Палата суда постановила, что «записи, подлинность которых не была подтверждена в суде, все же могут быть приняты к рассмотрению, поскольку аутентификация в суде является лишь одним из средств, которые Палата должна учитывать при определении подлинности предмета и доказательное значение». [27]

Однако определение допустимости каких-либо доказательств не имеет никакого влияния на доказательную силу, которую им придает сама Палата. Доказательственный вес означает относительную важность, придаваемую части признанных доказательств при принятии решения о том,

доказан ли определенный вопрос или нет. Поэтому, в отличие от доказательной силы, вес доказательств оценивается судьями в конце судебного разбирательства, после заслушивания всей совокупности доказательств, принятых по делу.

В деле «Прокурор против Жан-Пьера Бембы Гомбо» МУС подтвердил, что у судей нет строгих требований выносить отдельное решение относительно подлинности представленных доказательств. Основная аргументация Палаты в этом деле заключалась в содействии справедливому и быстрому судебному разбирательству, как того требует статья 64 Статута.

Учитывая гибкий подход Суда к доказательствам, определение подлинности доказательств в конечном итоге остается на усмотрение судей. Это становится проблематичным при оценке цифровых доказательств, ввиду сложности технической стороны и необходимости соответствующих познаний.

При реализации полномочий суда создан Единый технический протокол или («Протокол электронного суда» или «Протокол»), который предназначен для обеспечения техническими протоколами и средством определения подлинности цифровых доказательств.

Большая часть Протокола электронного суда представляет собой относительно стандартное описание соглашений о наименованиях и характере процедур подготовки и подачи документов в электронную систему Суда. Однако методы аутентификации, предусмотренные Протоколом, требуют тщательного изучения. [28]

Кратковременный характер цифровых доказательств поднимает вопрос о том, какие меры по сохранению необходимы или даже возможны в соответствии с действующим Статутом. Хотя полномочия прокурора ограничены до начала расследования, безграничный характер Интернета и распространение цифровых коммуникаций могут потребовать смягчения этих ограничений во время предварительного расследования.

Ценная цифровая информация, доступная во время развития или на ранних стадиях конфликта, может быть потеряна, если не обеспечить сохранность этой информации криминалистически обоснованным путем до начала расследования.

Например, прокурор должен иметь возможность использовать рамки сотрудничества, предусмотренные Римским статутом, которые призваны обеспечить помощь Суду на государственном уровне, чтобы обращаться к поставщикам услуг связи с просьбой сохранить пользовательские данные сверх обычных сроков их хранения.

Хотя сотрудничество государства на этапе предварительного расследования является добровольным, государства-участники должны рассматривать запросы информации к поставщикам услуг как часть своей обязанности по поддержке Суда.

То есть данный момент подразумевает обеспечение сохранности массива цифровой информации сверх установленного времени. Учитывая

непродолжительный и нормативно не определенный характер хранения такой информации на серверах поставщиков услуг, а также сроки исковой давности в Республике полагаем Казахстан, полагаем необходимым определить конкретные обязательные сроки хранения цифровой информации (фото, видео фиксация и т.д.) в течении срока исковой давности.

Да, действительно, установлено обязательное хранение на электронном носителе материалов кредитного досье на заемщиков в течение 5 лет, вместе с тем имеется оговорка обязательности при условии наличия такой возможности формирования досье в электронном формате у банков [29].

Данные моменты конечно предполагают дополнительные финансовые затраты поставщиков услуг.

Статья 56 Римского статута допускает сбор доказательств, которые впоследствии могут быть недоступны для целей судебного разбирательства.

На этапе расследования статья 56 может быть применена для сохранения цифровой информации в странах, где прокурору физически ограничен вход на территорию предприятия, связанного с преступлением, но не являющегося участником уголовного процесса. Цифровые доказательства могут храниться в нескольких местах, и их сбор может не требовать физического доступа на территорию объекта или государства в целом. Это важнейшее подспорье для следователей МУС, которые полагаются на сотрудничество государственных органов, чтобы иметь возможность получить доступ и изъять доказательства.

Отсутствие международной помощи препятствовало расследованиям в прошлом, но, поскольку данные хранятся без учета физических границ и проходят через серверы, расположенные во многих странах, рассматриваются новые способы как государства-участники могут способствовать сохранению цифровых доказательств при транспортировке на сервера, доступ к которым возможен на территориях, находящихся под юрисдикцией Суда.

Вместе с тем, следует отметить, что возможности сети Интернет способствуют, а возможно даже компенсируют ограничения проверочных действий прокурором, в целях соблюдения требований законов о кибербезопасности и конфиденциальности, без официального запроса помощи государств вне юрисдикции Статута.

Протокол электронного суда требует, чтобы всем цифровым файлам, загружаемым в электронную систему, была присвоена цифровая подпись, которая «может использоваться для проверки подлинности доказательств, если подлинность оспаривается».

Цифровая подпись — это «математический алгоритм, обычно используемый для проверки подлинности и целостности сообщения» (CISA, без даты). Цифровые подписи уникальны для конкретного физического или юридического лица и используются для защиты и надежной аутентификации происхождения, целостности и неотречения подписи цифрового файла. Протокол электронного суда требует, чтобы участники торгов проверяли подлинность файлов с помощью алгоритма хеширования цифровых подписей,

называемого MD5. Хотя в целом для Суда является хорошей практикой обеспечения безопасности требование цифровых подписей для целей аутентификации, использование MD5 следует рассматривать как проблему, вызывающую непосредственную и серьезную озабоченность МУС.

MD5 — это программа хэш-функции, первоначально созданная в 1992 году. Каждая цифровая подпись генерирует «хэш-функцию» или строку цифр и букв, созданную алгоритмом, уникальным для файла или документа. Хэш — это односторонняя функция. Это означает, что процесс, создавший хэш, не может быть отменен для поиска других файлов, генерирующих такое же значение хеш-функции. MD5 использует 128-битный «цифровой отпечаток» для создания одностороннего хеша, который по современным стандартам имеет относительно небольшое количество бит. MD5 не соответствует одному из основных требований любой криптографической хэш-функции — вычислительно невозможно найти два разных файла с одинаковым значением хеш-функции. Это явление, когда несколько файлов имеют совпадающие хеш-функции, известно, как коллизия. Из-за известной уязвимости к коллизиям к 2008 году MD5 был признан во всем мире криптографически взломанным. [30]

В 2011 году Инженерная группа Интернета (IETF), ведущая международная организация по протоколам Интернета, предупредила всех пользователей компьютеров, что «MD5 больше не приемлем там, где требуется устойчивость к коллизиям, например, цифровые подписи». [31]

В 2012 году коллизионные уязвимости в MD5 были широко использованы с помощью сложного вредоносного ПО под названием Flame, которое в то время считалось «одной из самых сложных угроз, когда-либо обнаруженных». Flame заразил сети в Иране, Израиле, Судане, Сирии, Ливане, Саудовской Аравии и Египте, что позволило хакерам записывать аудио, делать снимки экрана, контролировать нажатия клавиш и открывать конфиденциальные файлы. Flame воспользовался слабой криптографией MD5 и обманом заставил зараженные компьютеры поверить в то, что вредоносное ПО имеет действительную цифровую подпись. Коллизионная атака Flame возобновила призывы исследователей прекратить использование MD5 для аутентификации цифровых подписей в любых целях. [32]

Использование MD5 не только делает аутентификацию цифровых доказательств технически невозможной, но и подрывает легитимность Суда и объективность судебного процесса. Кроме того, любая сторона, желающая оспорить подлинность любых цифровых доказательств, представленных в Суд, может указать на широко разрекламированную и хорошо известную небезопасность MD5 и немедленно признать доказательства недостоверными, что фактически сводит на нет огромное количество времени и энергии, затраченных на сбор, защиту и представление доказательств в суд.

MD5 делает хранилище цифровых доказательств МУС небезопасным. Неспособность МУС обновить свою сломанную криптографию сродни тому, как сломать замок на воротах, где хранятся доказательства самых страшных

преступлений в мире. Данные в электронных системах судебных органов могут быть подвергнуты соответствующим вредоносным атакам.

Замена MD5 более надежной криптографической программой устранит непосредственную уязвимость безопасности в системе. Однако удаление и замена MD5 более надежными криптографическими стандартами требует как криптографической гибкости, так и совместимости. [33]

Криптографическая гибкость описывает способность машин добавлять новые криптографические алгоритмы или функции к существующему оборудованию или программному обеспечению, а также эффективно выводить из эксплуатации уязвимые или устаревшие криптографические системы. Функциональная совместимость описывает способность общаться и обмениваться информацией между различными системами. [34]

Это непростая задача для всех сторон. Некоторые устаревшие машины и системы могут не поддерживать обновления безопасности, или пользователи могут не захотеть платить за обновления безопасности.

Суд также должен учитывать время и затраты на обновление протоколов безопасности для менее технологически продвинутых сторон. Например, сила более предпочтительной современной криптографии может замедлять работу старых машин, делая систему электронного суда менее доступной для менее технологически продвинутых пользователей. Таким образом, любые обновления протокола электронного суда должны тщательно сбалансировать соображения логики и безопасности всех участников процесса.

Разработка системы, сочетающей в себе криптографическую гибкость и функциональную совместимость, является необходимым шагом на пути к более безопасной электронной системе подачи заявок.

Однако это не решает проблему того, как Суду следует обращаться со всеми документами и файлами, заверенными с помощью MD5, по делам, находящимся на рассмотрении. В таких случаях могут быть только две возможные стратегии смягчения последствий. Суд может потребовать от всех сторон повторно представить каждую часть цифровых доказательств с использованием новых, более безопасных алгоритмов хеширования. Это будет трудоемкий процесс для сторон и может нарушить статью 64 Статута, которая гласит: «Судебная палата должна обеспечить, чтобы судебное разбирательство было… оперативным».

К примеру по делу в отношении бывшего сотрудника ООН Калликста Мбарушиманы, обвиненного в содействии геноциду, в 2011 году в ответ на просьбу обвинения о внесении поправки в протокол электронного суда по делу по вопросам объективности алгоритма хеширования Суд отметил, что любые изменения затронут «сотни тысяч электронных документов», которые имели отношение к делу.[35] В последующем МУС большинством в два голоса против одного отклонила обвинения против Мбарушиманы на том основании, что не было достаточных доказательств для предположения о том, что он способствовал военным преступлениям в Северном и Южном Киву.

В последующем МУС неоднократно пересматривал требования использования MD5 (последний раз в 2019 году) и до сих пор не отказался от MD5 и не обновил свои протоколы цифровых подписей. Неспособность Суда обновить свои устаревшие и небезопасные процедуры аутентификации демонстрирует, что Суд все еще крайне неподготовлен к проблемам аутентификации, с которыми он сталкивается в эпоху цифровых технологий. Это подрывает авторитет МУС и его способность рассматривать будущие дела, в которых цифровые доказательства гарантированно будут играть центральную роль.

Тот факт, что МУС по настоящее время требует использование цифровых подписей, предполагает, что Суд признает важность целостности и безопасности данных. [36]

Поэтому крайне важно уделять приоритетное внимание надежным стандартам криптографии для защиты своей электронной системы при формировании, фиксации и хранении документов.

Подводя итог, можно сказать, что MD5 опасно устарел, и ему нельзя доверять в выполнении основной функции его предполагаемого использования — аутентификации цифровых файлов. Однако на территории Республики Казахстан, не смотря на известность данной проблемы с 2012 года, по настоящее время вопрос объективности прерогативы использования MD5, как способа идентификации и аутентификации, не рассматривается.

# 2 Сбор и оценка цифровых доказательств в уголовном судопроизводстве.

## 2.1 Особенности сбора цифровых доказательств

В теории уголовно-процессуальных доказательств под вещественными доказательствами понимаются предметы, вещи, в том числе документы. Содержанием вещественного доказательства являются те следы, свойства, признаки, которые непосредственно запечатлелись на предмете, доступны непосредственному восприятию и могут быть обнаружены путем осмотра [11].

Ряд ученых предлагает компьютерную информацию рассматривать в качестве вещественного доказательства.

Если совершается преступление с использованием компьютера, будет оправданным считать, что его информационные следы могут по праву считаться аналогом материальных следов, оставляемых обычным преступлением.

Как известно, основным признаком вещественного доказательства является его объективная связь с предметом доказывания; в силу этой связи оно и может служить средством установления доказываемых фактов. Этот признак в полной мере можно отнести к электронной информации, которая может служить и орудием преступления (например, компьютерная программа, содержащая вирус), выступать предметом преступления (например, перевод денежных средств с одного счета на другой) и представлять собой след преступления, вроде попытки несанкционированного доступа, зафиксированного в журнале регистрации конкретной программы. Деньги, ценности и иное имущество, полученные в результате совершения преступления, скажем акции, иные ценные бумаги, средства электронного платежа, также могут быть в электронном виде и, таким образом, выступать средством доказывания.

Некоторые ученые пришли к выводу о целесообразности отказа от такого понятия и исключения вещественного доказательства из числа видов доказательств, названных в ч. 1 ст. 118 УПК РК.

Итак, предметность электронного доказательства относительна; вещественность вторична, информативность первична. А потому, во-первых, электронным доказательством необязательно должен быть документ (протокол), а во-вторых, само по себе вещество по своей сути не информативно, доказательством не является, пока не будет субъекта доказывания.

А вот кем будет резюмироваться в законе этот субъект – следователем, который проводит всестороннее, полное, объективное предварительное расследование (доказывание), или сотрудником, уполномоченным на досудебный уголовный розыск (уголовное преследование), который осуществляет поиск обвинительных доказательств, – это принципиальный вопрос.

В первом случае следователь формирует доказательство, во втором – это только обвинительный материал, из которого в суде, возможно, будет сформировано доказательство. Так же и в случае с электронной информацией:

она становится доказательственной тогда, когда субъект доказывания интерпретирует ее в качестве таковой, делая объектом познания / доказывания изменения, произошедшие в информационной среде.

Свойства любого вещественного доказательства –«незаменимость и уникальность» [37].

В основе данного признака лежит тот факт, что ни у одного образа события нет и не может быть тождественного ему двойника.

Специфика электронного вещественного доказательства состоит в способности сохранения в неизменном виде информации при ее копировании и других операциях (при условии корректности их проведения). Это родовое свойство всех электронных доказательств, которому оно обязано вычислительной технике и программному обеспечению. Безличный, бессубъектный характер позволяет отнести определенную разновидность электронной информации к категории вещественных доказательств. В отличие от обычного вещественного доказательства, каковым выступает предмет, а его доказательственное значение определяется физическими свойствами или местоположением, электронное вещественное доказательство – это след, оставленный преступлением в информационной среде, т.е. это информация.

Механизм формирования электронного доказательства определяется алгоритмом, который реализуется в конкретной программе. Но не программа выступает определяющим условием или средством формирования электронного доказательства. Главным условием его формирования являются процессуальная форма и правовой статус субъекта, уполномоченного оценивать эту информацию как факт. Исходная характеристика вещественного доказательства как информационного следа остается.

След преступления – это то изменение, которое произошло в информационной среде вследствие действий преступника. То, что преступные действия осуществлялись особым способом в особой среде, не меняет сути феномена электронного вещественного доказательства. Его исходные свойства – объективность и уникальность – присущи и электронному вещественному доказательству. Как известно, ни одно действие в электронно-информационной среде не остается бесследным. При всех технических трудностях, с которыми сопряжено выявление субъекта действий в этой среде, это возможно.

И наконец, по признаку среды существования электронных вещественных доказательств, разумеется, есть отличие от вещественных доказательств, являющихся частью аналоговой среды. Компьютерная информация – это среда программных и технических средств, т.е. электронная среда. Данная особенность сказывается на работе с этими доказательствами, но не затрагивает их правовой сущности.

Главное, что делает некоторые электронные доказательства доказательствами вещественными, – это их отличие от личных доказательств, в том числе любых документов, которые являются в принципе производными личными доказательствами. Отличие это состоит в том, что электронные

вещественные доказательства формируются объективно, как следы преступной деятельности, а не создаются специально для передачи информации о фактах.

Особую группу вещественных доказательств в силу свойственной им определенной электронной специфики составляют электронные носители информации. В свою очередь, существенность этой электронной специфики рассматриваемого вида вещественных доказательств, особых условий его познания и использования в уголовном процессе и, наконец, особенностей его хранения и определения его последующей судьбы (после завершения уголовного дела) требует более подробного рассмотрения.

Категория вещественных доказательств является достаточно объемной. В связи с чем в научной литературе выделяют достаточно много оснований построения классификаций этого вида доказательств. Например, по материальному воплощению, по количественным характеристикам, по отношению к предмету обвинения, по отношению к доказываемым обстоятельствам, по наличию или отсутствию промежуточного носителя между фактом и источником доказательственной информации, криминалистическая (по характеру изменения материальной обстановки) [38, с. 50-72; 39, с.15-16] и т.д.

Данные классификации не исключают друг друга, они отражают различные аспекты этого явления. Рассмотрим некоторые из них, применительно к носителям компьютерной информации как вещественным доказательствам.

По отношению к версии обвинения или противостоящим им версиям [40, с.134] доказательства делятся на обвинительные и оправдательные. Обвинительными будут доказательства, способствующие установлению события преступления, вины обвиняемого, отягчающие наказание обстоятельства и т.д. К типичным обвинительным доказательствам относятся, например, следы пребывания обвиняемого на месте преступления, обнаруженные при обыске у обвиняемого орудия преступления.

Оправдательными - позволяющие убедиться в отсутствии события преступления, невиновности лица, наличии смягчающих наказание обстоятельств.

Следующим критерием для классификации вещественных доказательств является их отношение к любому из обстоятельств, подлежащих доказыванию и по способу доказывания. По этому основанию вещественные доказательства можно разделить на прямые и косвенные.

Прямым считается вещественное доказательство, если оно своим содержанием однозначно устанавливает или опровергает факт, входящий в предмет доказывания. Косвенным считается вещественное доказательство, если оно своим содержанием устанавливает промежуточный, не входящий в предмет доказывания, но в своей объективной связи с ним дающий основание для вывода о наличие или отсутствии обстоятельств исследуемого преступления [41].

Далее рассмотрим деление вещественных доказательств на первоначальные и производные (т.е классификация вещественных доказательств по наличию или отсутствию промежуточного носителя между фактом и

источником доказательственной информации). Первоначальными называют доказательства, полученные из первоисточника, т. е. это те объекты, которые либо имели непосредственную связь с самим преступлением, либо возникшие, как правило, в ходе его подготовки, совершения или сокрытия (например, предметы, служившие орудием преступления или бывшие объектом преступных действий, или следы преступления и др.).

Однако вещественные доказательства не всегда являются первоначальными. Очень часто на практике объекты – первоначальные вещественные доказательства заменяются на копии, повторяющие интересующие признаки и свойства объектов оригиналов, которые могут быть воспроизведены. Таким образом, возникают так называемые производные вещественные доказательства.

Такая возможность закреплена в действующем законодательстве в ст. 199 УПК, в которой говориться, что «к протоколу прилагаются фотографические негативы и снимки, киноленты, диапозитивы, фонограммы, кассеты видеозаписи, иные носители информации, чертежи, планы, схемы, слепки и оттиски следов, выполненные при производстве следственного действия». К этому будут относиться материалы, скопированные с большого массива носителя информации.

Создание копии объекта оригинала, является оправданным в случае, его громоздкости, хрупкости, изменчивости, невозможности отделения от объекта-носителя и т.д. Несмотря на то, что производное вещественное доказательство существенно отличается от первоначального тем, что оно, как правило, состоит из другого материала, и имеет, поэтому другой вес, цвет, форму, размер и т. п. оно точно передает характер тех признаков, которые имеют доказательственное значение.

Так и электронные носители информации, с записанной на них информацией, обнаруженной в ЭВМ, в ходе следственного действия, являются производными вещественными доказательствами, естественно только в том случае, когда процесс записи на этот носитель осуществлялся с использованием сертифицированной и апробированной техники и технологии, гарантированно обеспечивающей получении копии компьютерной информации без изменений.

Получение таких электронных информации при проведении следственных действий, разрешает некоторые проблемы, связанные с поиском и изъятием компьютерной информации, до сих пор являющейся объектом, обладающим определенной новизной при исследовании. Так основной рекомендацией при обнаружении ЭВМ в ходе проведения следственного действия является его изъятие с обязательным участием специалиста и фиксация ее конфигурации на месте обнаружения и упаковка таким образом, чтобы аппаратуру можно было бы успешно, правильно и точно так же, как на месте обнаружения, соединить в лабораторных условиях или в месте производства следствия с участием специалистов [42; 43, с.16; 7] т е. обнаружив компьютер, следователь и специалист обесточивают компьютер, разъединив устройства, запаковывают их,

и поиск информации осуществляют непосредственно на рабочем месте эксперта или специалиста.

Такой способ без сомнения, позволяет полностью и тщательно изучить информацию, хранящуюся на компьютере. Однако очень часто в ходе следствия складывается ситуация, когда есть данные о том, что на компьютере содержится информация, которая может способствовать более плодотворному или целенаправленному осмотру (различные планы помещений, коды доступа и т.д.) и проведению других следственных действий (например, допросу подозреваемого) и ее необходимо получить в короткий срок.

«Результаты просмотра электронной информации могут существенным образом повлиять на дальнейший ход расследования. Процессуально значимым последствием может явиться формирование основания для назначения судебной экспертизы по установлению фактических данных, имеющих значение для дела, при этом формулирование вопросов для экспертного исследования может потребовать специальных знаний.

Может сложиться ситуация, когда первичный просмотр может способствовать решению ориентировочных задач, например: специалисты какого профиля должны принимать участие при повторном просмотре электронной информации с последующим определением характера назначаемой экспертизы.» [44, с.35].

Так, например, в феврале 2000 года Управлением ФСБ РФ по Воронежской области было расследовано уголовное дело по обвинению Г. и Р. в том, что они неоднократно, в течение длительного времени распространяли по сети Интернет в г. Воронеже и Воронежской области вредоносные программы для ЭВМ, не санкционированно скопировали охраняемые Законом и договором сведения об учетных именах и паролях для доступа в сеть Интернет и незаконно работали в ней под данными именами.

В ходе обыска по месту работы Г. были обнаружены и изъяты средства компьютерной техники, записи с похищенными учетными именами и паролями пользователей сети Интернет, которые были осмотрены и приобщены к делу. При осмотре компьютера была обнаружена важная информация: исходящие и входящие электронные сообщения, доказывающие факт распространения Г. и Р. нескольких вредоносных программ; файлы, представляющие собой изображения экрана монитора удаленного компьютера – скриншоты, являющиеся доказательством использования вредоносной компьютерной программы Hack'a'tack неправомерного доступа к охраняемой законом информации в ЭВМ, повлекшего копирование; Web-страницы, содержащие вредоносные программы и т.д. В свою очередь, осмотр, например, электронных сообщений, позволил установить хронологию переписки между Г. и Р., находящимся в то время в Англии, и факт распространения одной из вредоносных программ через компьютер, расположенный в Лондонском Интернет-кафе [45].

Данные проблемы и могут быть решены, на наш взгляд, путем использования соответствующих сертифицированных методик применения

программных средств, для обнаружения и фиксации компьютерной информации в ходе следственных действий.

Действующая редакция соответствующих статей УПК прямого указания на то, что следственный осмотр представляет собой непосредственное восприятие объектов, их признаков и свойств, не содержит.

Более того, ч. 5 статьи 199 УПК определяет необходимость указания в протоколе следственного действия технических средств, условий и порядка их использования при его производстве, тем самым косвенно допуская возможность проведения и опосредованного восприятия с использованием различных искусственных объектов и методик их применения.

Полученные таким образом электронные носители информации должны иметь статус вещественного доказательства. Так как они обладают признаками, присущими исключительно вещественным доказательствам:

1. Данные, имеющие отношение к делу, содержатся на них во внешних признаках (намагничивание определенных секторов диска), а не находятся в вербальной форме.

2. Могут служить средством к обнаружению преступления, установлению фактических обстоятельств дела, выявлению виновных либо к опровержению обвинения или смягчению ответственности, так как на электронные носители информации переносится не только информация, но и, следы воздействия на нее, то есть следы преступления.

3. В них имеется материальный способ получения, сохранения и передачи невербальной информации, имеющей отношение к делу.

Кроме уже указанных выше причин использования электронных носителей информации в качестве производных вещественных доказательств, может возникнуть необходимость использовать их наряду с первоначальными, например, если предполагается видоизменение или уничтожение компьютерной информации, так как известно, что отличительной особенностью компьютерной информации является легкость ее уничтожения и модификации.

Достаточно полно вопросы раскрываются в исследовании Утепова Д.П. по вопросам теоретических и практических аспектов использования цифровой информации по уголовным делам, где автор приводит особенности осмотра и изъятия электронного носителя информации, просмотр, содержащейся в нем информации с участием специалиста. [16]

Выезжая на осмотр места происшествия, лицо, производящее данное следственное действие (следователь, дознаватель) не всегда знает с чем ему придется столкнуться при производстве осмотра и какие предметы, имеющие значение для уголовного дела, будут обнаружены и изъяты с места происшествия. Например, при осмотре в квартире, где распространялись наркотические средства были помимо наркотиков обнаружены электронные носители информации (флеш -карты и ноутбук) они также были изъяты следователем, так как на данных информационных носителях могла быть информация, которая имела значение для расследования уголовного дела

(возможно, совместные фото виновных по уголовному делу лиц, для того, чтобы подтвердить их знакомство между собой). Осмотр в данном случае проводится без специалиста.

Так как перед осмотром не было известно имелись ли там какие — либо электронные носители информации или нет. Таким образом, при обнаружении электронных носителей информации целесообразна следующая последовательность действий:

1. Внешний осмотр электронных носителей информации, а также фиксация обстановки и обстоятельств обнаружения компьютерных объектов, с целью установления относимости данного объекта к расследуемому уголовному делу. Сведения об обстановке позволяют судить об условиях как использования лицом, совершившим преступление, электронных носителей информации, так и условиях обнаружения и изъятия этих носителей органами внутренних дел.

Это, в свою очередь, может иметь значение для придания информации на электронных носителях качества доказательств (например, обнаружение электронного носителя с пиратской бухгалтерской программой в помещении финансового подразделения проверяемой организации может свидетельствовать об относимости электронного носителя к уголовному делу) [13]

2. В случае, если при производстве следственного действия присутствует специалист по информационным технологиям, то просмотр информации, содержащейся в обнаруженном электронном носителе информации, для решения вопроса о дальнейшем его исследовании и использовании в доказывании.

3. Если специалист в производстве следственного действия не участвует, то изъятие электронного носителя информации, с последующим исследованием с помощью специалиста или назначение экспертизы.

Учитывая возможности функционала АРМ ЕРДР полагаем необходимым и целесообразным внедрение технологии- алгоритмизации сбора и учета электронной информации в качестве доказательства в рамках уголовного судопроизводства.

- внедрение функционала в ЕРДР «Журнал учета вещественных доказательств и других изъятых по делам денег и ценностей, не признанных вещественными доказательствами, находящимися в камере хранения».

- возможность создания карточки для ввода информации по каждому отдельному вещественному доказательству в базу данных, в том числе сохранение введенных данных также в карточку Е5 в уголовном деле.

Вместе с тем, полагаем необходимым обеспечить интеграцию «Журнал учета вещественных доказательств и других изъятых по делам денег и ценностей, не признанных вещественными доказательствами, находящимися в камере хранения» с иными информационными системами для оптимизации уголовного процесса:

- с системой «Е-экспертиза» Министерства юстиции в части назначения судебных экспертиз с получением результатов в электронном формате;

- с системой «Төрелік» Верховного Суда Республики Казахстан для обеспечения требований ст.118 УПК, при разрешении судьбы вещественных доказательств по результатам рассмотрения уголовного дела по существу (актуально так же в случае начала досудебного расследования по частному определению суда по результатам рассмотрения гражданских дел).

## 2.2 Оценка цифровых доказательств

В начале XXI века, из-за значительного увеличения объема информации и необходимости ее обработки и передачи во всех развитых странах мира, начато активное использование электронных (технические и программные) средств обработки информации, которая хранится и передается в электронном виде.

Согласно исследованию Международной корпорации данных (МЦД), объем такой информации (коллективные данные мира) удваивается каждый год на полтора, а в 2025 году составит 175 зеттабитов (триллионов гигабайтов) [46].

Различные электронные ресурсы хранятся в облачных, сотовых системах, компьютерах, смартфонах, устройствах и т.д. переход общества в глобальном масштабе на цифровые технологии, геометрический рост объема данных, а также количество пользователей Интернета, которых в мире уже более 5 миллиардов, в отсутствие надлежащего правового урегулирования социальных отношений в этих областях, повышает риски безопасности, создает угрозу кибербезопасности государств, в частности в банковском секторе, экономической деятельности, защите функционирования критически важной инфраструктуры, и т.д. личные данные, киберпреступность является одной из серьезных угроз для кибербезопасности.

Национальный сегмент Интернета насчитывает более 120 тысяч Интернет-ресурсов в доменах .KZ и ҚАЗ, в соответствии с законодательством физически размещаемых на территории Республики Казахстан. В целях оказания содействия владельцам и пользователям информационных ресурсов и систем по вопросам безопасного использования ИКТ с 2010 года функционирует национальная Служба реагирования на компьютерные инциденты KZ-CERT. Служба является участником ряда международных организаций, в т.ч. FIRST (Forum of Incident Response and Security Teams), TI (Trusted Introducer for Security and Incident Response Teams), OIC-CERT (Организация исламского взаимодействия Служб реагирования на компьютерные инциденты).[47]

Службой заключено 20 меморандумов о взаимопонимании и сотрудничестве с профильными структурами зарубежных стран, зафиксировано и обработано более 66 тысяч инцидентов информационной безопасности.

На казахстанском рынке появились первые отечественные компании, занимающиеся инструментальным аудитом по оценке защищенности (тестированием на проникновение) на соответствие требованиям информационной безопасности и специализирующиеся на исследовании обстоятельств, причин и условий инцидентов информационной безопасности, а

также техническом исследовании вредоносного программного обеспечения. Разработаны первые отечественные средства антивирусной защиты.

Планируется ратификация Казахстаном Конвенции ООН о киберпреступности, где помимо преступлений, непосредственно связанных с конфиденциальностью, неприкосновенностью и доступностью компьютерных данных и систем (глава 7 УК РК), киберпреступность включает также мошенничество и подлог, связанные с использованием компьютеров, преступления, связанные с размещением незаконной информации в сетях, преступления, связанные с авторскими и смежными правами и т.д. [48]

Таким образом, киберпреступность в современном смысле включает в себя многие виды преступной незаконной деятельности с использованием компьютерных технологий: незаконный оборот наркотиков через Интернет, оружие через Даркнет, распространение детской порнографии, кибермошенничество, фишинг, Доходы от такой незаконной деятельности постоянно растут, и, по данным исследования Herjavec Group и Cybersecurity Ventures, потери от киберпреступности в 2021 году составили 6 триллионов. USD, по сравнению с 3 триллионами в 2016 году. [49]

Глобальные расходы на киберпреступность, как ожидается, будут расти на 15 процентов ежегодно в течение следующих пяти лет, достигнув 10,5 триллионов USD к 2025 году.

В Казахстане, как и во всем мире, постоянно растет число киберпреступлений. Так, в 2019 году по сравнению с 2023 годом, согласно официальной статистической отчетности Генеральной прокуратуры, количество уголовных преступлений по главе 7 УК РК увеличились на 16,92% (2019г.-108, 2020г.-110, 2021г. –120, 2022г.-142, 2023г.-130). (Таблица 1)

Значительно увеличилось количество уголовных правонарушений, предусмотренных главой 7 УК РК, совершенных группой лиц (2019г.-0, 2020г.-0, 2021г. –1, 2022г.-22, 2023г.-13).

**Таблица 1**

| период | 2019 | 2020 | | 2021 | | 2022 | | 2023 | |
|---|---|---|---|---|---|---|---|---|---|
| Всего зарегистрировано правонарушений по главе 7 УК РК | 108 | 110 | +1,85% | 120 | +9% | 142 | +18,3% | 130 | -8,4% |
| Из них совершено в группе лиц | 0 | 0 | 0 | 1 | +100 | 22 | +2100% | 13 | -40% |

Для обеспечения необходимого уровня кибербезопасности, в дополнение к различным мерам кибер-защиты практически во всех странах мира, сегодня создаются не только специальные подразделения, сотрудники которых специализируются на выявлении, документировании и расследовании киберпреступлений, кроме того, в настоящее время разрабатывается

соответствующее законодательство для обеспечения эффективного противодействия киберпреступности, в том числе на международном уровне.

В отличие от других стран, в Казахстане по-прежнему актуальной остается проблема использования значительного объема информации, зарегистрированной в электронной форме в качестве доказательства в уголовном процессе, а не только при расследовании киберпреступлений. Специальный Указанная проблема становится существенной при расследовании транснациональных преступлений, совершенных на территории Казахстана, с последующим взаимодействием на межгосударственном уровне.

Информация, записанная в электронной (цифровой) форме, может быть легко изменена, уничтожена, передана, скопирована. Особенность информации в электронной форме заключается в том, что она доступна людям не напрямую, а только после обработки специальным программным обеспечением (например, текстовым редактором Word), которая, в свою очередь, работает под управлением операционной системы на определенном компьютерном устройстве.

То есть просмотр различными программными средствами физически идентичной информации в виде битов (минимальной единицы объема информации) на жестком диске приведет к различным типам фактических данных на экране монитора или принтере распечатки. Таким образом, электронная форма информации означает ее существование и хранение в форме "компьютерных данных", что, согласно Конвенции о киберпреступности, означает любое представление фактов, информации или концепций в форме, пригодной для обработки в компьютерной системе, включая программу, подходящую для выполнения определенной функции компьютерной системой [50].

Отсюда осознание специфики электронной (цифровой) информации, особенностей ее создания, хранения, преобразования, а также учет таких особенностей в Уголовно-процессуальном кодексе, введение отдельной процессуальной категории электронных доказательств позволит использовать имеющиеся в цифровом формате фактические данные в такой сфере связей с общественностью, как уголовный процесс.

Исследования по использованию информации, записанной в цифровой форме (электронные доказательства), в судопроизводстве проводятся иностранными учеными и практиками с конца прошлого столетия. Сегодня в развитых странах разработаны руководства, соответствующие руководящие принципы и научные работы.

Однако безуспешные попытки законодателя как-то ситуативно решить проблему нормативной определенности в электронной (цифровой) форме информации и ее использование в процессе доказывания при расследовании уголовных преступлений становятся основанием для продолжения научного обсуждения конкретного характера таких доказательств и их места в системе процессуальных источников доказательств в уголовном судопроизводстве.

Так, в части 5 ст.232 УПК законодатель отмечает, что "для выявления, пресечения и раскрытия других уголовных правонарушений, не предусмотренных частью четвертой настоящей статьи, могут проводиться негласные следственные действия, предусмотренные только пунктами 7), 9) статьи 231 настоящего Кодекса».

Напрямую снятие информации об обстоятельствах уголовного преступления предусмотрены в главе 30 УПК «Негласные следственные действия», где прямо предусмотрено проведение негласных следственных действий, посредством которых уголовное преследование имеет возможность получения электронной и цифровой информации (звукозаписи и записи изображений, фотографии, другие зафиксированные с помощью научно-технических средств).

Оценка и исследование данной информации прямо предусмотрена ст.239 УПК, где конкретизирована юридическая значимость результатов в доказывании наравне с доказательствами, полученными в результате следственных действий.

Обзор компьютерных данных проводится следователем, прокурором путем отображения в протоколе обзора содержащейся в них информации в форме, подходящей для восприятия ее содержания (с помощью электронных средств, фотографии, видеозаписи, съемки и/или видеозаписи экрана и т.д., или в бумажной форме).

Для того чтобы субъект расследования мог обеспечить отображение информации, содержащейся в компьютерных данных, и зафиксировать ее в протоколе, он должен ознакомиться с ней, иными словами, воспринять ее с помощью органов восприятия, как и другие объекты материальной среды, которые могут быть восприняты им во время осмотра - ландшафт, помещения, вещи, документы. Но, учитывая характер информации, записанной в электронной форме, и даже само понятие "компьютерных данных" (любое представление фактов, информации или концепций в форме, пригодной для обработки в компьютерной системе, включая программу, которая подходит для выполнения определенной функции компьютерной системой, такое восприятие непосредственно субъектом расследования физически невозможно [51].

Кроме того, пытаясь воспроизвести определенные компьютерные данные в протоколе осмотра, предполагается, что объект расследования уже фактически вносит определенные изменения в такую информацию, оставляя "цифровой след" в результате своей деятельности, то есть необратимо изменяет фактические данные, записанные в цифровой форме.

Спорным также является вопрос о том, что в процедурном аспекте становится такой информацией- компьютерные данные, после его рассмотрения. С учетом методов их отражения, предложенных законодателем, компьютерные данные становятся документом по смыслу Закона «Об электронном документе и электронной цифровой подписи».

Но определяющим фактором процессуальной категории "документ" является ее материальный характер- свойство, которым компьютерные данные

не обладают в обычном для нас смысле: У нас нет возможности воспринимать их без специальных технических средств, преобразующих такие фактические данные.

То есть, по сути, компьютерные данные не могут быть объектом проверки ни в качестве следственного (следственного) действия, ни в качестве документа в качестве процессуальной категории. В этой связи мы вынуждены заявить, что законодатель упорно игнорирует особый характер электронных средств (цифровых) информацию и попытки ситуационного решения проблемных вопросов, связанных с использованием такой информации в процессе доказывания в уголовном процессе, что проявляется в многочисленных изменениях и дополнениях уголовно-процессуальных норм, ведет лишь к углублению проблемы процедурного обеспечения электронной (цифровой) информацией в качестве доказательства.

Таким образом, законодатель заявляет, что "копии информации, включая компьютерные данные, содержащиеся в информационных (автоматизированных) системах, системах электронной связи, информационных и коммуникационных системах, компьютерных системах, их составные части, подготовленные следователем, прокурором с участием специалиста, признаются судом подлинным документом " (п.п.15 статьи 7 УПК), тем самым утверждая, что помимо компьютерных данных в этих ресурсах имеется и другая информация, помимо компьютерных данных.

Анализ норм свидетельствует о несоответствии между ними уголовно-процессуальных норм и, как следствие, о возможности толкования некоторых процессуальных категорий, в частности "компьютерных данных"; "копию информации из электронных информационных систем, компьютерных систем или их частей, мобильных терминалов систем связи" и т.д. Кроме того, по нашему мнению, условием обязательного участия специалиста по копированию электронных (цифровых) информация свидетельствует о признании законодателем конкретного характера такой информации и необходимости профессиональных знаний субъекта, занимающегося ее сбором. Но в то же время законодатель не устанавливает каких-либо квалификационных требований для такого специалиста (в отличие от других случаев обязательного участия специалиста в уголовном судопроизводстве), который по существу принижает роль соответствующего специалиста и сводит его участие в разбирательствах, связанных с копированием информации, к формальности [52].

Важно понимать, что в современных условиях информатизации абсолютно всех видов социальной деятельности электронные (цифровые) информация, которая может содержать информацию о случае уголовного преступления и представлять интерес для его расследования не только обычные электронные документы, материалы фото-, аудио- и видеозаписи в социальных сетях и т.д., но и огромный массив электронной информации, отражая функционирование телекоммуникационных, сетевых и спутниковых систем, таких, как различные устройства искусственного интеллекта, системы безопасности и доступа,

платежные терминалы, навигационные системы, информационные ресурсы в виде определенных регистров, и т.д. Можно с уверенностью утверждать, что сегодня расследование всех уголовных преступлений без исключения каким-то образом связано с использованием цифровой (электронной) информации, особенно с учетом внедрения Е-дело.

И, учитывая особенности природы и сущности электронной (цифровой) информации, фактические данные, записанные в этой форме, наряду с "традиционной" доказательства должны отвечать условиям относимости и допустимости для установления наличия или отсутствия фактов и обстоятельств, имеющих отношение к уголовному разбирательству.

Это означает, среди прочего, четкую процедурную определенность как процедурного места такой информации, так и процедуры ее сбора, оценки и проверки. В этой связи мы настаиваем на необходимости введения отдельной процессуальной категории для информации, зарегистрированной и существующей в цифровой (электронной) форме - электронное доказательство, которое, с учетом надлежащей процедуры их сбора, по нормам УПК для всех участников уголовного процесса будут действовать в качестве процессуальных источников доказательств.

По нашему мнению, надлежащая процедура их сбора должна учитывать конкретный характер таких доказательств и обеспечивать их получение сторонами уголовного разбирательства без изменения содержания доказательств (то есть определенным специалистом, квалификация которого будет четко определена). И их оценка, и проверка (физическое восприятие участниками процедуры) должны быть возможны только путем изучения или исследования специальным предметом. Конечно, такие изменения должны стать возможными только после всесторонней работы по согласованию между собой всех норм УПК, относящихся к предлагаемой категории, и урегулирования некоторых аспектов на уровне подзаконных актов и положений (например, четкое определение полномочий владельцев, пользователей и управляющих электронными регистрами, разграничение концепций носителей информации и информации, установление квалификационных требований для определенных специалистов, определение специальностей специалистов и т.д.).

Но только такая сложная и систематическая работа по обеспечению процедурной осуществимости использования электронной (цифровой) информации в процессе доказывания уголовного судопроизводства, по нашему глубокому убеждению, способна обеспечить приемлемость и принадлежность таких доказательств в качестве доказательств. В противном случае мы станем свидетелями следующих судебных прецедентов и беспомощности правоохранительных органов в обеспечении выполнения функций уголовного судопроизводства.

Настоятельная необходимость обеспечения процессуальной правоспособности электронных доказательств в уголовном процессе Казахстана также провозглашается Советом Европы 17 ноября, 2021 года второго

Дополнительного протокола к Конвенции о киберпреступности об укреплении международного сотрудничества, который в перспективе намеревается ратифицировать Республика Казахстан.

Рационализация концептуального аппарата для таких доказательств и соответствующей процедурной процедуры их использования в процессе доказывания на государственном уровне будет ключом к последовательности и согласованности в международно-правовом пространстве при предоставлении взаимной правовой помощи; содействие, обеспечение процессуальной правоспособности электронных доказательств в уголовном судопроизводстве Казахстана возможно при условии включения этого определения в УПК РК и определения в подзаконных актах четких процедур их получения, обработки и хранения.

## 2.3 Цифровые доказательства в уголовном процессе: проблемы практики и повышение эффективности

Современная цифровая эпоха привела к тому, что большое количество информации, в том числе персональных данных о людях и их жизнедеятельности становится доступной в электронном виде. Изменения затронули и расследования уголовных дел.

Существуют объективные причины, по которым производство уголовных дел стало оцифровываться. Во-первых, это связано с тем, что цифровые технологии позволяют значительно упростить и ускорить процессы сбора и обработки информации. Во-вторых, цифровизация позволяет более точно и эффективно анализировать большие объемы данных, что в свою очередь способствует выявлению связи между различными случаями преступлений и принимать более обоснованные решения. В-третьих, оцифровка решает проблему использования бумажных носителей информации, которые могут быть уничтожены или утеряны. [52, с.486-492]

Таким образом, цифровизация ведения уголовных дел является закономерным и неизбежным процессом в современном мире.

Внедрение электронного уголовного дела в Казахстане требует правового закрепления процедуры сбора, обработки и приобщения цифровых доказательств. Для этого разработаны Закон «О цифровой подписи и электронных документах» [3], утвержден приказ Генеральной Прокуратуры «Об утверждении Инструкции о ведении уголовного судопроизводства в электронном формате» [20], Закон «О цифровых активах в Республике Казахстан» [53], регулирующие процедуры использования электронных документов, цифровых подписей и применение цифровых активов, включая цифровые доказательства в досудебных и судебных процессах.

Тем не менее, отсутствуют утвержденные процессуальные процедуры закрепления цифровых доказательств, что может усугублять практику их применения.

«Использование специалиста также весьма затруднительно из-за обстоятельств организационного характера, так и подвергнуто сомнению стороной защиты, поскольку до сих пор не решен существующий диссонанс между процессуальным статусом специалиста и его организационной диспозицией» [54]

Следовательно, требуется разработать и утвердить процедуры сбора, обработки и приобщения цифровых доказательств в уголовных делах. Кроме того, важно проводить регулярные обучающие программы для сотрудников правоохранительных органов и судей в области информационных технологий и цифровых доказательств.

Развитие электронного уголовного дела и использование цифровых доказательств в Казахстане обеспечит ускорение процесса судебных разбирательств, повышение качества судебных решений и более эффективную борьбу с преступностью. Однако, для достижения этой цели требуется оптимизировать работу по совершенствованию законодательства и повышению технической грамотности сотрудников правоохранительных органов и судей.

В Казахстане, как и во многих других развивающихся странах, существуют определенные проблемы технического и юридического характера, связанные с организацией процесса закрепления и приобщения цифровых доказательств к электронному уголовному делу. При их использовании необходимо соблюдать определенные требования, чтобы обеспечить правильность закрепления и приобщения к «е-УД».

Проблемой, связанной с закреплением и приобщением цифровых доказательств, является вопрос аутентичности. Аутентичность цифровых доказательств означает, что они после изъятия не изменены. Электронные доказательства эфемерны, могут быть подделаны или изменены, поэтому необходима разработка и внедрение специальных методов и технологий для обеспечения их целостности, подлинности и сохранности. Важно создать единую систему правил и процедур для работы с цифровыми доказательствами, в том числе аспекты сбора, приобщения, допустимости и достоверности.

Действительно, привычное понимание вещественных доказательств как материальных не всегда применимо к цифровым следам преступной деятельности. При изъятии цифровых доказательств противоправной деятельности с электронных носителей информации (USB-накопители, компьютеры, сервера), их традиционно относят к материальным средствам вычислительной техники. В случае проведения удаленного интерактивного обыска, при котором изымаются цифровые следы с сервера, находящегося в другой юрисдикции, возникают сложности в приобщении этих доказательств к «е-УД». Статья 123 Уголовного процессуального кодекса Республики Казахстан (далее-УПК РК) «в качестве документа признает материалы, содержащие компьютерную информацию, с оговоркой – если документы обладают, признаками, указанными в статье 121 этого же кодекса» [48].

При извлечении (либо записи) с USB-накопителя цифровой информации, основной интерес представляет только «цифровая информация». Хотя эта информация не может существовать вне электронного носителя. Некоторые следователи в протоколе осмотра указывают изначальное место нахождения цифровых доказательств (например, на сервере) и процессуально фиксируют перенос дубликата цифровых доказательств на USB-накопитель следователя с использованием криминалистических блокираторов записи и разделением на оригинал и дубликат.

Лицо, ведущее уголовный процесс, сталкивается с дилеммой о правильном алгоритме действий по официально не регламентированному снятию цифровых доказательств, которые на наш взгляд должны включать в себя следующие действия (основаны на рекомендациях специалистов [54,55]:

- Не изменять оригинальные файлы. Если попытаться снять доказательства с компьютера или телефона, нельзя запускать или удалять файлы, которые могут быть связаны с преступлением или инцидентом (в том числе оперативной памяти).

- Сделать резервную копию данных. Прежде чем пытаться снять доказательства, сделать резервную копию всех данных на компьютере или мобильном устройстве. Это гарантирует сохранение ценной информации и предотвращение случайного удаления или изменения данных.

- Использовать специализированные инструменты. Существует множество программ, которые способствуют извлечь цифровые доказательства с компьютера или мобильного устройства. Однако, не все софтверные продукты созданы равными, поэтому необходимо исследовать и выбирать только те, которые обеспечивают защиту всех данных.

- Важно учитывать, что цифровые доказательства могут быть подвержены подделке и изменению, поэтому при их использовании в суде необходимо убедиться в их подлинности и надежности. Для этого могут использоваться различные методы: использование «блокираторов записи», применение цифровых подписей и хэш-сумм.

В юридической литературе подчеркивается, что снятие цифровых доказательств без помощи специалиста является сложной задачей, требующей определенных знаний и навыков. «…участие компетентного лица, обладающего достаточными знаниями» [56].

Как было ранее отмечено, вопрос постоянного обучения сотрудников правоохранительных органов и судей в области цифровых доказательств, разработка и внедрение новых технологий и методы защиты и обработки цифровых доказательств, а также совершенствование законодательства и нормативных актов, регулирующих использование цифровых доказательств в уголовном процессе не просто рекомендация, а веление времени.

Национальное законодательство не делает различий в способах получения цифровых данных, что закономерно, учитывая, что разработчики УПК РК не обладают техническим образованием.

Компетенции сотрудника правоохранительного органа неопределённы и не позволяют проводить элементарное изъятие цифровых активов (следов) без участия специалиста. Поскольку УПК РК не регламентирует в какой форме специалист может участвовать, то привлечение специалиста онлайн имеет смысл.

Вот уголовно-процессуальный кодекс Федеративной Республики Германии (далее-УПК ФРГ), оперируя с цифровыми доказательствами, регламентирует такой способ их получения, как дешифровка изъятых данных, отнеся их к процессуальному действию, которое может правомерно осуществляться органом, ведущим уголовный процесс [57].

Необходимо отметить, что в УПК ФРГ не детализируется субъект получения цифровых данных, возлагая обязанность по соблюдению всех процессуальных аспектов получения указанного вида доказательств на правоохранительные органы.

Это подводит нас к тому, что лица ведущие уголовный процесс помимо юридических знаний должны обладать как минимум навыками снятия и процессуального закрепления информации из информационно-коммуникационных объектов.

Использование узкопрофильных специалистов по территориальному признаку в эру цифровых технологий также требует иного организационно-правового подхода. Если заинтересованные государственные органы смогут организовать сбор (через блокираторы записи), защищенное хранение, обеспечить доступ всем заинтересованным участникам уголовного процесса к цифровым доказательствам, то вполне разумным будет привлекать узкопрофильных специалистов для исследования цифровых активов через защищенные каналы связи. Поскольку есть риск, что через защищенные каналы связи в общее хранилище могут попасть вирусы нулевого дня полагаем целесообразно поступающую подобную информацию изолировать в «программной оболочке» по подобию «песочниц» в самих накопителях данных.

Целесообразно, чтоб первичные действия по документированию цифровых следов выполняли уполномоченные сотрудники правоохранительных органов без оглядки на специалистов. Бесценная информация в дампах оперативной памяти эфемерна и меры по фиксации принимать следует безотлагательно. Уже после того, как цифровые доказательства сохранены должным образом можно по мере необходимости привлекать необходимых специалистов. Важно процесс поиска и закрепления эфемерных документов сделать безотлагательно, исключить риск совершения ошибки сотрудником правоохранительного органа, процессуальный порядок и участие виртуального специалиста возложить по возможностям на IT структуру.

Если организационные проблемы, связанные с переподготовкой и оснащением правоохранительных органов для решения вопросов снятия цифровых данных вполне решаемы, то немалую проблему может создать экономический аспект данного вопроса. Общеизвестно, что отрасль IT с

финансовой точки зрения затратна и не терпит «бюджетного» подхода, поскольку экономия на цифровых технологиях неизбежно повлечет отставание в скорости расследования и помимо материально-технических проблем – отток компетентных профессионалов, поскольку специалист в области расследования «цифровых» преступлений на рынке труда имеет достаточно высокий спрос на квалифицированные услуги.

Совершенствование законодательства в области фиксации и сохранения электронных доказательств является важным шагом для обеспечения их законности и надежности при использовании в уголовном процессе. Это может включать в себя уточнение процедур сбора, хранения, обработки и приобщения цифровых доказательств, а также установление механизмов проверки и контроля за их правильным использованием. Также может потребоваться обновление и дополнение законодательства в свете новых технологических достижений и изменений в криминальной ситуации.

Сохранение доказательств означает, что правительство должно поддерживать целостность доказательств для последующего тестирования или анализа. Для этого хранители имущества и доказательств должны вести точные и полные записи цепочки сохранности, правильно хранить доказательства и предотвращать загрязнение, повреждение или уничтожение доказательств. Точный протокол будет варьироваться в зависимости от типа доказательств, например, правил сохранения биологических образцов по сравнению с цифровыми доказательствами.

В сегодняшнюю цифровую эпоху обилие цифровых доказательств в расследованиях невозможно переоценить. Как руководитель расследования или дела, вы, вероятно, слишком хорошо знакомы с проблемами управления цифровыми доказательствами. Вам необходимо не только убедиться, что он безопасен, актуален, законен и этичен, но вам также необходимо обеспечить его легкодоступность и презентабельность, если ваше дело дойдет до суда.

Хотя управлять физическими доказательствами так же просто, как и принести их с собой, этого нельзя сказать о цифровых доказательствах, поскольку разнообразие типов файлов и разнородность систем делают их консолидацию практически невозможной. Вот почему так важно использовать практические способы эффективного управления цифровыми доказательствами. В этом блоге мы обсудим ключевые стратегии и лучшие практики управления цифровыми доказательствами таким образом, чтобы они соответствовали вашим требованиям к отчетности и судебным слушаниям. Мы рассмотрим:

- Цифровые доказательства: что это такое на самом деле, где их можно найти и как они используются
- Самая большая проблема управления цифровыми доказательствами
- Острая необходимость в эффективности управления расследованиями
- Важность безопасности
- Почему важно управлять качеством доказательств
- Что есть в Comtrac, чего нет в других системах управления делами

На самом деле это любой тип электронных данных или информации, которые могут быть использованы в качестве доказательств в судебном расследовании или судебном разбирательстве, включая все, от электронных писем и текстовых сообщений до сообщений в социальных сетях, цифровых изображений и видеозаписей. Его можно найти практически на любом устройстве, которое мы используем сегодня, и он может храниться в различных форматах, включая текстовые, графические, аудио- и видеофайлы.

Цифровые доказательства часто используются в уголовных расследованиях, гражданских исках, делах, связанных с киберпреступностью, а также в расследованиях регулирующих органов. Мы также видим, что это становится все более распространенным в широком спектре юридических дел. Это означает, что, если вы участвуете в судебных расследованиях и судебных разбирательствах, вам необходимо иметь четкое представление о том, как эффективно управлять цифровыми доказательствами, включая обеспечение их безопасности, подлинности и допустимости в суде.

Какова самая большая проблема в управлении цифровыми доказательствами? Вы слышали термин «большие данные» — это одна из основных проблем, когда речь идет об управлении цифровыми доказательствами; огромный объем данных, которые необходимо собирать, обрабатывать и хранить. В отличие от традиционных форм доказательств, таких как физические документы или показания свидетелей, цифровые доказательства могут иметь широкий спектр форматов и храниться в разных местах, что затрудняет отслеживание.

Это приводит к неэффективности процесса расследования и потенциально может задержать судебное разбирательство. Необходимо также учитывать риски безопасности, поскольку цифровые доказательства должны храниться надежно, чтобы предотвратить несанкционированный доступ или подделку. Мало того, неспособность должным образом управлять цифровыми доказательствами может привести к тому, что они будут признаны неприемлемыми в суде, что потенциально подрывает общее качество дела.

Проблемы и перспективы использования цифровых доказательств в досудебном производстве являются важными аспектами в контексте цифровых трансформаций в правоприменительной сфере.

Президент страны в своем ежегодном Послании отметил о необходимости обеспечить верховенство права и качество отправления правосудия [58]. Для реализации этой цели, правоохранительные органы планомерно внедряют электронное судопроизводство. Так, 21 декабря 2017 г. Законом РК в УПК введена ст. 42-1 «Формат уголовного судопроизводства», согласно которой уголовное судопроизводство в республике ведётся в бумажном и (или) электронном форматах [6]. Таким образом, электронный формат расследования был официально закреплён в уголовно-процессуальном законодательстве.

В ходе реализации проекта возникали сложности по 3 направлениям работы по внедрению Е-формата расследования: 1) техническое обеспечение

органов уголовного преследования и пропускная способность каналов связи; 2) недоработки самой платформы; 3) подготовка сотрудников следственных подразделений к расследованию дел в электронном формате, влияющая на его качество. С момента начала реализации проекта по цифровизации уголовного процесса проверки технического обеспечения органов и обучение проводились совместно с региональными управлениями КПС и СУ [59].

Несмотря на сложность нового формата расследования, правоохранительные органы приняли его положительные возможности [60]. Дальнейшее совершенствование процесса нами видится в повсеместном использовании цифровых доказательств в досудебном производстве.

Основные проблемы использования цифровых доказательств, заключаются в следующем:

- Аутентичность и целостность данных: один из основных вопросов при использовании цифровых доказательств - это обеспечение их аутентичности и целостности. Существует риск подделки или искажения цифровых данных, и правоохранительные органы должны принимать меры для защиты от этого.
- Проблемы конфиденциальности: сбор и использование цифровых доказательств может вмешиваться в частную жизнь граждан и нарушать их права на конфиденциальность. Необходимо соблюдать законы и нормы, чтобы обеспечить баланс между преследованием преступлений и защитой частной жизни.
- Техническая экспертиза: правоохранительным органам может потребоваться техническая экспертиза для анализа и интерпретации цифровых доказательств. Это может потребовать дополнительных ресурсов и специализированных навыков.
- Сроки хранения данных: в зависимости от юрисдикции, цифровые данные могут иметь определенные сроки хранения, и их удаление или изменение может вызвать проблемы при следственных действиях.

Для решения проблем, связанных с использованием цифровых доказательств в досудебном производстве, необходимо предпринимать ряд мер и разработать соответствующие стратегии. Вот некоторые шаги, которые можно предпринять:

1) Обучение и подготовка персонала: обучение сотрудников правоохранительных органов и юристов в области цифровых технологий и цифровой форензики позволит им более компетентно работать с цифровыми доказательствами.

2) Установление стандартов и правил: разработка и внедрение стандартов и правил сбора, анализа и хранения цифровых доказательств может помочь обеспечить их целостность и аутентичность.

3) Соблюдение законодательства о конфиденциальности: необходимо соблюдать законы и нормы о конфиденциальности данных и обеспечить соблюдение прав граждан при сборе и использовании цифровых доказательств.

4) Инвестиции в техническую экспертизу: правоохранительные органы могут инвестировать в оборудование и обучение специалистов по цифровой форензике, чтобы обеспечить адекватную экспертизу цифровых доказательств.

5) Разработка цифровых стратегий: государственные органы могут разрабатывать цифровые стратегии для улучшения сбора, анализа и обмена информацией между разными службами.

6) Сотрудничество с частным сектором: сотрудничество с технологическими компаниями и частными экспертами по цифровой безопасности может помочь в разработке современных методов обнаружения и анализа цифровых доказательств.

7) Общественное сознание и образование: образовательные кампании для граждан о правилах использования цифровых технологий и их последствиях могут способствовать снижению рисков в сфере цифровой безопасности.

8) Международное сотрудничество: в рамках международного сотрудничества можно разрабатывать стандарты и процедуры для обмена цифровыми доказательствами в масштабах мирового сообщества.

Решение проблем, связанных с цифровыми доказательствами, требует комплексного подхода, который включает в себя образование, техническую экспертизу, правовую поддержку и сотрудничество всех заинтересованных сторон.

Принятие указанных выше мер, откроет перспективы для использования цифровых доказательств, которые видятся в следующем:

- Улучшенная эффективность: цифровые доказательства могут быть легче обнаружены, анализированы и переданы между органами правопорядка, что способствует более эффективным расследованиям.
- Большая точность: с использованием технологий, таких как цифровая форензика и распознавание лиц, возможно повышение точности и надежности доказательств.
- Сокращение бюрократии: цифровые системы могут сократить бумажную работу и упростить процессы сбора и обработки информации.
- Глобальный доступ к данным: современные технологии позволяют обмениваться информацией и доказательствами между различными странами и юрисдикциями, что может быть полезным в расследованиях международных преступлений.

Важно учесть, что цифровые доказательства должны использоваться с соблюдением законодательства и правил судопроизводства, чтобы гарантировать справедливость и соблюдение прав граждан. Это также означает, что правоохранительные органы и суды должны развивать компетенции и навыки в области цифровых технологий и форензики.

По мнению О. Макаровой, дальнейшая модернизация досудебного производства в рассматриваемом аспекте должна происходить путём перехода на обязательное фиксирование с использованием средств аудиовидеозаписи и

иных технических средств всех процессуальных действий, проводимых следователями (дознавателями) [61].

В рамках настоящего диссертационного исследования проведено анкетирование представителей юридической общественности из числа сотрудников органов уголовного преследования. Целью проведения анкетирования явилось установление практических навыков закрепления и использования цифровых доказательств.

Результаты анкетирования обнажили проблему отсутствия практических и теоретических знаний, необходимости внесения изменений и дополнений в уголовно-процессуальное законодательство по определению цифровых доказательств в отдельную категорию, установлению и конкретизации отдельного порядка выявления, фиксации, осмотра, исследования и хранения такой информации (Приложение 4).

Таким образом, решение проблем, связанных с использованием цифровых доказательств в досудебном производстве, требует комплексного и многогранного подхода. Необходимо обеспечивать баланс между соблюдением законодательства о конфиденциальности данных и эффективным использованием цифровых технологий для борьбы с преступностью. Это включает в себя обучение и подготовку персонала, разработку стандартов и правил для сбора и анализа цифровых доказательств, инвестиции в техническую экспертизу и сотрудничество с частным сектором.

# ЗАКЛЮЧЕНИЕ

В ходе исследования, посвященного проблемам и перспективам использования цифровых доказательств в досудебном производстве, были рассмотрены важнейшие аспекты внедрения современных технологий в правовую практику. Полученные результаты говорят о значительном влиянии цифровых доказательств на эффективность и справедливость досудебного расследования.

Современные тенденции свидетельствуют о неотвратимости процесса цифровизации в различных сферах общества. В контексте правосудия, активное использование цифровых технологий предоставляет новые инструменты для сбора, анализа и представления доказательств.

Преимущества цифровых доказательств сопряжены с улучшением скорости, точности и объективности досудебного расследования. Электронные следы могут служить более надежными основаниями для вынесения судебных решений.

В ходе исследования выявлен ряд значимых проблем, сигнализирующих о необходимости детального изучения, нормативного закрепления с постоянным отслеживанием современных тенденций и развития науки в части обеспечения относимости и допусти цифровых доказательств, соблюдения безопасности цифровых данных, вопросов аутентичности электронных доказательств.

Правовой аспект важным выводом подчеркивает необходимость постоянного совершенствования правового регулирования в области цифровых доказательств, включая установление четких стандартов и процедур.

При этом развитие технологий, стандартизация процедур сбора и представления цифровых доказательств, а также обучение специалистов в данной области предоставляют перспективы для дальнейшего совершенствования системы досудебного расследования.

С учетом вышеизложенного, представляется, что дальнейшее интегрирование цифровых доказательств в досудебное производство требует системного подхода, учитывающего технические, правовые и организационные аспекты. Одновременно необходимо уделять внимание защите прав граждан и обеспечению надежности электронных данных.

В результате проведенного исследования были рассмотрены проблемы и перспективы использования цифровых доказательств в досудебном производстве. На основании анализа существующей литературы, нормативных актов и судебной практики были выявлены следующие основные выводы:

Цифровые доказательства представляют собой эффективный инструмент для установления обстоятельств уголовного правонарушения, их использование позволяет существенно ускорить процесс сбора, анализа и представления доказательств, что способствует более оперативному досудебному расследованию.

Выделяя технические сложности при проведении компьютерной экспертизы, вопросы аутентичности и целостности цифровых данных, а также необходимость обеспечения конфиденциальности и безопасности информации, необходимо разработать специализированные методики и стандарты проведения компьютерной экспертизы, обеспечить квалифицированное обучение сотрудников правоохранительных органов и судебных экспертов, а также совершенствовать правовую базу в области цифровых технологий и информационной безопасности.

Однако данный вопрос следует рассматривать, предварительно разграничив цифровые доказательства в отдельную категорию доказательств, наравне в вещественными доказательствами, учитывая нематериальный характер цифровой информации, а не качества ее носителя.

Исходя из вышеизложенного, можно сделать вывод о том, что использование цифровых доказательств в досудебном уголовном производстве имеет значительные перспективы развития, однако требует комплексного подхода и системной работы по решению выявленных проблем. Важно продолжать исследования в данной области и разрабатывать новые методики и технологии, чтобы обеспечить более эффективное применение цифровых доказательств в уголовном процессе.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Постановление правительства Республики Казахстан от 28 марта 2023 года № 269 «Об утверждении Концепции цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023 - 2029 годы». [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/P2300000269/ (дата обращения: 15.04.2024 ).

2. Типовой закон «Об электронной торговле» принят ЮНСИТРАЛ ООН от 12.06.1996г. [Электронный ресурс] – Режим доступа https://uncitral.un.org/ru/texts/ecommerce/modellaw/electronic_commerce/ (дата обращения: 15.04.2024 ).

3. Закон Республики Казахстан «Об электронном документе и электронной цифровой подписи» от 7 января 2003 года N 370. [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/ (дата обращения: 15.04.2024).

4. Закон Республики Казахстан «О доступе к информации» [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/Z1500000401/ (дата обращения: 15.04.2024).

5. Правила отображения и использования электронных документов в сервисе цифровых документов утверждены приказом Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 28 сентября 2020 года № 352/НҚ [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/V2000021329/ (дата обращения: 15.04.2024).

6. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V (с изменениями и дополнениями по состоянию на 02.01.2021 г.). [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/K1400000231 / (дата обращения: 15.04.2024).

7. Большой юридический словарь [Электронный ресурс] – Режим доступа: https://online.zakon.kz/Document/?doc_id=1999018/ (дата обращения: 15.04.2024).

8. Мещеряков В.А. Особенности специальных знаний, используемых в цифровой криминалистике [Электронный ресурс] // сайт научной электронной библиотеки «КиберЛенинка» – Режим доступа: https://cyberleninka.ru/article/n/osobennosti-spetsialnyh-znaniy-ispolzuemyh-v-tsifrovoy-kriminalistike/ (дата обращения: 15.04.2024)

9. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: дис. … д-ра юрид. наук. – Воронеж, 2001. – 387 с.

10. Вехов В.Б. Электронные следы в системе криминалистики / В.Б. Вехов, Б.П. Смагоринский, С.А. Ковалев // Судебная экспертиза. – №2.- С. 10-19.

11. Пастухов П.С. Электронное вещественное доказательство. [Электронный ресурс] – Режим доступа: https://cyberleninka.ru/article/n/elektronnoe-veschestvennoe-dokazatelstvo-v-ugolovnom-sudoproizvodstve/ (дата обращения: 15.04.2024).

12. Белкин А.Р. Теория доказывания в уголовном судопроизводстве. – М.: Норма, 2005 – 485 с.

13. Мещеряков В.А., Трухачев В.В. Формирование доказательств на основе электронной цифровой информации // Вестник Воронежского института МВД России. - №2 – 2012. - С. 14-18.

14. Конвенция Совета Европы «О киберпреступности, о расширении сотрудничества и раскрытия электронных доказательств» подписана в Будапеште 23.11.2001г. [Электронный ресурс] – Режим доступа: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rm.coe.int/1680aa2b7d/ (дата обращения: 15.04.2024).

15. Дополнительный протокол к Конвенции Совета Европы «О киберпреступности, о расширении сотрудничества и раскрытия электронных доказательств», СЕД №189 [Электронный ресурс] – Режим доступа: https://prosud.kz/news/rekomendatsii-po-obespecheniyu-kiberbezopasnosti-obnovili-v-es-8d2a7b/ (дата обращения: 15.04.2024).

16. Д.П. Утепов, Н.Ш. Жемписов, А.К. Жумадиллаева. Формы участия IT-специалиста в процессе получения цифровых следов по уголовным делам. Вестник Академии, №23 от 31.03.2022г. [Электронный ресурс] – Режим доступа: https://vestnikacademy.kz/?p=1955&lang=ru/ (дата обращения: 15.04.2024).

17. Руководство по электронным доказательствам в гражданском и административном производстве, принято Комитетом министров Совета Европы 30.01.2019 г. [Электронный ресурс] – Режим доступа: Chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rm.coe.int/russian-version-unofficial-translation-of-the-guidelines-on-electronic/16809f03ac/ (дата обращения: 15.04.2024).

18. Цехан Д. М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ: моногр. / Д. М. Цехан, –2011. – 216 с.

19. Жилхайдарова Б.А. Правовые основания закрепления и приобщения цифровой информации к материалам электронного уголовного дела. Материалы заочной Международной научно-практической конференции. Минск. 2022.- С.49-52. [Электронный ресурс] – Режим доступа: https://www.amia.by/activities/scientific-activity/conference/3159-zaochnaya-mezhdunarodnaya-nauchno-prakticheskaya-konferentsiya-teoriya-i-praktika-protivodejstviya-kiberprestupnosti/ (дата обращения: 15.04.2024).

20. Национальный план развития Республики Казахстан до 2025 года, утвержден Указом Президента Республики Казахстан от 15.02.2018г. [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/U1800000636/ (дата обращения: 15.04.2024).

21. Приказ Генерального прокурора Республики Казахстан «Об утверждении Инструкции о ведении уголовного судопроизводства в электронном формате» от 03.01.2018 года №2. [Электронный ресурс]. – Режим доступа: https://adilet.zan.kz/rus/docs/V1800016268 (дата обращения: 15.04.2024).

22. Приказ Генерального прокурора Республики Казахстан от 19.09.2014 года № 89 «Об утверждении Правил приема и регистрации заявления, сообщения

или рапорта об уголовных правонарушениях, а также ведения ИС ЕРДР» [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/V14W0009744/ (дата обращения: 15.04.2024).

23. Википедия. Международный уголовный суд. [Электронный ресурс] – Режим обращения: https://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D0%B6%D0%B4%D1%83%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D1%8B%D0%B9_%D1%83%D0%B3%D0%BE%D0%BB%D0%BE%D0%B2%D0%BD%D1%8B%D0%B9_%D1%81%D1%83%D0%B4/ (дата обращения: 15.04.2024).

24. Rome Statute. [Электронный ресурс] – Режим доступа: https://www.icc-cpi.int/sites/default/files/RS-Eng.pdf/ (дата обращения 15.04.2024).

25. Will Kenton Prima Facie: Legal Definition and Examples [Электронный ресурс] – Режим доступа: https://www.investopedia.com/terms/p/prima-facie.asp/ (дата обращения: 15.04.2024).

26. The United Nations Diplomatic Conference of Plenipotentiaries on the Establishment of an International Criminal Court. [Электронный ресурс] – Режим доступа: https://www.ohchr.org/en/instruments-mechanisms/instruments/rome-statute-international-criminal-court/ (дата обращения: 15.04.2024).

27. Бывший вице-президент ДРК получил 18 лет тюрьмы за военные преступления в ЦАР. [Электронный ресурс] – Режим доступа: https://ru.euronews.com/2016/06/21/icc-gives-former-rebel-warlord-18-years-for-war-crimes-and-crimes-against/ (дата обращения: 15.04.2024).

28. Unified technical protocol of the ICC [Электронный ресурс] – Режим доступа:https://www.icccpi.int/sites/default/files/RelatedRecords/CR2019_00267.PDF/ (дата обращения: 15.04.2024).

29. Об установлении Перечня основных документов, подлежащих хранению, и сроков их хранения в банках второго уровня, филиалах банков-нерезидентов Республики Казахстан Постановление Правления Национального Банка Республики Казахстан от 29 февраля 2016 года № 66. Зарегистрировано в Министерстве юстиции Республики Казахстан 17 мая 2016 года № 13710. [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/V1600013710/ (дата обращения: 15.04.2024).

30. Взлом хэш-функций. По материалам сайта [Электронный ресурс] – Режим доступа: http://www.server.md/. http://itsec.ru/articles2/tema/glavn_sobyt_2005_goda_8/ (дата обращения: 15.04.2024).

31. Pdated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms. [Электронный ресурс] – Режим доступа: https://datatracker.ietf.org/doc/rfc6151/ (дата обращения: 15.04.2024).

32. How does the Flame malware take advantage of MD5 collision? [Электронный ресурс] – Режим доступа: https://crypto.stackexchange.com/questions/44151/how-does-the-flame-malware-take-advantage-of-md5-collision/ (дата обращения: 15.04.2024).

33. Introduction to Security and Threat Mgmts. and Cybsec Resources [Электронный ресурс] – Режим доступа: https://www.coursesidekick.com/computer-science/1322885/ (дата обращения: 15.04.2024).

34. What is interoperability? [Электронный ресурс] – Режим доступа: https://www.techtarget.com/searchapparchitecture/definition/interoperability/ (дата обращения: 15.04.2024).

35. Калликст Мбарушиман передан в руки международного правосудия. [Электронный ресурс] – Режим доступа: https://news.un.org/ru/story/2011/01/1177031/ (дата обращения: 15.04.2024).

36. Chelsea Quilling. The Future of Digital Evidence Authentication at the International Criminal Court. [Электронный ресурс] – Режим обращения: https://jpia.princeton.edu/news/future-digital-evidence-authentication-international-criminal-court/ (дата обращения 15.04.2024).

37. Моругина Е.А., Сидорова Е.И. Понятие, признаки и природа вещественных доказательств в современном уголовном процессе РФ. [Электронный ресурс] – Режим доступа: https://cyberleninka.ru/article/n/ponyatie-priznaki-i-priroda-veschestvennyh-dokazatelstv-v-sovremennom-ugolovnom-protsesse-rossii/ (дата обращения: 15.04.2024).

38. Егоров Н.Н. Вещественные доказательства: уголовно-процессуальный и криминалистический аспекты. - М., 2007. –298 с.

39. Попова Н.А. Вещественные доказательства: собирание, представление и использование их в доказывании. Автореф. дисс. на соискание уч. ст. канд. юрид. наук. – Саратов 2007. – 15-16 с.

40. Уголовный процесс России: учебное пособие/ под ред. З.Ф. Ковриги, Н.П. Кузнецова. Воронеж, ВГУ, 2003. – 134 с.

41. Хмыров А.А. Косвенные доказательства/А.А. Хмыров. М., 1979.

42. Андреев Б.В., Пак П.Н., Хорст В.П. Расследование преступлений в сфере компьютерной информации. М., 2001. – 152 с.

43. Мусаева У.А. Розыскная деятельность следователя по делам о преступлениях в сфере компьютерной информации: автореф. дис. …канд. юрид. наук. Тула, 2002. – 201 с.

44. Толеубекова Б. Компьютерные преступления доказать сложно //ЗАҢГЕР. - 2005. - N11.

45. Краснова Л.Б. Электронные носители информации как вещественные доказательства. [Электронный ресурс] – Режим доступа: file:///C:/Users/%D0%96%D0%B0%D0%BD%D0%B0%D1%80%D0%B0/Downloads/elektronnye-nositeli-informatsii-kak-veschestvennye-dokazatelstva%20(2). pdf/ (дата обращения: 15.04.2024).

46. IDC: Expect 175 zettabytes of data worldwide by 2025. URL: [Электронный ресурс] – Режим доступа: https://www.networkworld. com/article/3325397/idc-expect-175-zettabytes-of-data-worldwide-by-2025.html/ (дата обращения: 15.04.2024).

47. Об утверждении Концепции кибербезопасности ("Киберщит Казахстана") Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407. [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/P1700000407/ (дата обращения: 15.04.2024).

48. Уголовный кодекс Республики Казахстан от 4 июля 2014 года № 231-V ЗРК. [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/ (дата обращения: 15.04.2024).

49. HG Threat Services [Электронный ресурс] – Режим доступа: https://www.herjavecgroup.com/services/managed-security-services/hg-threat-services/ (дата обращения: 15.04.2024).

50. Про кіберзлочинність: Конвенція. Ради Європи (Ратифікована із застереженнями і заявами Законом України від 07.09.05 р. № 2824-IV (2824-15). [Электронный ресурс] – Режим доступа: URL: https://zakon.rada.gov.ua/laws/show/994_575#Text/ (дата обращения 15.04.2024).

51. Гутсалюк М.В., Антонюк П.Е. О сущности электронной (цифровой) информации как источника доказательств в уголовном процессе. Судебно-медицинский бюллетень. 2020. - № 1(32). - С. 3749-3752.

52. Жилхайдарова Б.А., Жилкайдаров Р.Р. Проблемные вопросы закрепления и приобщения цифровых доказательств к электронному уголовному делу. Материалы VI Международной научно-практической конференции, приуроченной к празднованию 100-летнего юбилея У.С. Сеитова «Развитие современной юридической науки: теория и практика», с.486-492,2023г., [Электронный ресурс] – Режим доступа: https://academy-gp.edu.kz/?page_id=16232&lang=ru/ (дата обращения: 15.04.2024).

53. Утепов Д.П., Жемписов Н.Ш., Жумадиллаева А.К. IT-маманының қылмыстық істер бойынша сандық іздерді алу процесіне қатысу нысандары. Вестник Академии правоохранительных органов, №4 (23), 2022. – С. 66-71

54. Закон Республики Казахстан «О цифровых активах в Республике Казахстан» от 6 февраля 2023 года № 193-VII ЗРК. [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/Z2300000193/ (дата обращения: 15.04.2024).

55. Хан В.В. Правовой диссонанс процессуального статуса и организационной диспозиции эксперта и специалиста в уголовном процессе Казахстана //Теория и практика фундаментальных и прикладных исследований в сфере судебно-экспертной деятельности и ДНК-регистрации населения Российской Федерации. – 2022. – С. 205-209

56. Долинин В. Н., Кабитова Ю. Р., Елькина П.С. Технологии собирания, исследования и использования электронно-цифровых доказательств //Технологии XXI века в юриспруденции. – 2019. – С. 47-57.

57. Никитина Е. В. Некоторые вопросы собирания электронно-цифровых доказательств //Технологии XXI века в юриспруденции. – 2019. – С. 103-107.

58. Чернышов В.Н., Лоскутова Е.С. Проблемы собирания и использования цифровых доказательств // Социально-экономические явления и процессы. 2017.

№5. [Электронный ресурс] – Режим доступа: https://cyberleninka.ru/article/n/problemy-sobiraniya-i-ispolzovaniya-tsifrovyh-dokazatelstv/ (дата обращения: 15.04.2024).

59. Бродовски Д., Ян М. Цифровые доказательства в немецком уголовном процессе на стадиях предварительного расследования, рассмотрения дела по существу и ревизии // Российское право: образование, практика, наука. 2020. №3. [Электронный ресурс] – Режим доступа: https://cyberleninka.ru/article/n/tsifrovye-dokazatelstva-v-nemetskom-ugolovnom-protsesse-na-stadiyah-predvaritelnogo-rassledovaniya-rassmotreniya-dela-po-suschestvu/ (дата обращения: 15.04.2024).

60. Послание Главы государства К.К. Токаева народу Казахстана «Справедливое государство. Единая нация. Благополучное общество» 2023. [Электронный ресурс] – Режим доступа: https://www.akorda.kz/ru/poslanie-glavy-gosudarstva-kasym-zhomarta-tokaeva-narodu-kazahstana-181130/ (дата обращения: 15.04.2024).

61. Оракбаев А.Б. Проблемы и перспективы принятия прокурором ключевых решений в рамках электронного уголовного дела (на основе опыта Республики Казахстан) // Законность. - 2023. - № 3 (1061). - С. 14-17.

62. Алькенев Р.Б. О пилотной апробации процедуры согласования процессуальных решений с прокурорами в электронном формате // Сайт электронного журнала «Заң және заман». Вып. 5, С. 18–20. [Электронный ресурс]. – Режим доступа: https://zan-zaman.kz/wp-content/uploads/2020/11/zan-zaman-2020-05.pdf/ (дата обращения: 15.04.2024).

63. Макарова О.В. Совершенствование судопроизводства путем внедрения электронной формы уголовного дела. – Журнал российского права. - 2019. - № 1. - С. 159-168.

Приложение 1
Акт внедрения

Приложение 1
Акт внедрения

Акт внедрения 2

# Классификация

Анкетирование