АКАДЕМИЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ
ПРИ ГЕНЕРАЛЬНОЙ ПРОКУРАТУРЕ РЕСПУБЛИКИ КАЗАХСТАН

СЕРІМБЕТОВ НҰРБОЛ НҰРЛАНҰЛЫ

Особенности осмотра, изъятия и хранения информации в системах облачного хранения при производстве расследования

Диссертация на соискание степени
магистра юридических наук
по образовательной программе7М04203 «Юриспруденция»
(научно-педагогическое направление)

Заведующий кафедрой
общеюридических дисциплин
Института послевузовского
образования Сырбу А.В.,
кандидат юридических наук,
старший советник юстиции
_____

г.Косшы, 2024 г

РЕЗЮМЕ

Данная работа посвящена особенностям осмотра, изъятия и хранения информации в системах облачного хранения при производстве расследования. В основе настоящего исследования лежит исследование отечественного и зарубежного опыта обнаружения, осмотра, изъятия данных с облачных систем хранилищ и ее хранение. Автором предложены рекомендации по совершенствованию законодательства в области исследования, результаты работы апробированы.

ТҮЙІНДЕМЕ

ұмыс тергеу жүргізу кезінде бұлтты сақтау жүйелеріндегі ақпаратты тексеру, алу және сақтау ерекшеліктеріне арналған. Бұл зерттеудің негізінде бұлтты сақтау жүйелерінен деректерді табу, тексеру, алу және оны сақтаудың отандық және шетелдік тәжірибесін зерттеу жатыр. Автор зерттеу саласындағы заңнаманы жетілдіру бойынша ұсыныстар ұсынды, жұмыс нәтижелері тексерілді.

RESUME

Resume This work is devoted to the specifics of the inspection, seizure and storage of information in cloud storage systems during the investigation. The present study is based on the study of domestic and foreign experience in detecting, inspecting, removing data from cloud storage systems and storing it. The author offers recommendations on improving legislation in the field of research, the results of the work are tested.

СОДЕРЖАНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

Конституция – Конституция Республики Казахстан

МВД – Министерство внутренних дел

пп. – подпункт

п. – пункт

РК – Республика Казахстан

РФ – Российская Федерация

США – Соединенные Штаты Америки

СНГ – Содружество Независимых Государств

ст. – статья

СССР – Союз Советских Социалистических Республик

УПК – Уголовно-процессуальный кодекс

УК – Уголовный кодекс

ч. – часть

СМИ – средства массовой информации

ИС ЕРДР – Информационная система «Единый реестр досудебных расследований»

е-УД – Электронное уголовное дело

ВС – Верховный суд

ФЗ – Федеральный закон

ПО – Программное обеспечение

ВВЕДЕНИЕ

Актуальность темыисследования. Активное погружение в мир информационных технологий ставит вопрос обеспечения прав, свобод и законных интересов участников информационного обмена. Правовое регулирование отечественного информационного обмена находится на начальном этапе формирования.

Точкой отсчета признания роли информации является определение информационной безопасности в качестве неотъемлемого элемента национальной безопасности Республики Казахстан. Ключевой аспект риска информатизации общественных отношений заключается в отсутствии достаточных гарантий безопасности информационного обмена.

Интенсивно развивающаяся сфера сетевого обмена информацией привела к увеличению масштабов распространения криминальных практик: под угрозой может находиться целостность и конфиденциальность информации; угрозу может представлять и само негативное содержание информации либо отсутствие доступа к компьютерной информации, циркулирующей в сетевом пространстве.

Преступность использует достижения науки и техники, особенно ярко это проявляется в отношении преступлений в сфере компьютерной информации, что приводит к увеличению ее общественной опасности и причиняемого ею вреда. Вовлечение «информационного элемента» в орбиту уголовно-правовых отношений стало очевидным и требует дальнейшего совершенствования законодательства в данной сфере.

В последние годы компьютерная преступность в Республике Казахстан модифицировалась, приобретя организованный, профессиональный и экономически направленный характер, но этот процесс не сопровождался развитием соответствующей терминологической базы для целей квалификации преступлений, связанных с компьютерной информацией. Интернет дал

человеку безграничные возможности в области передачи, распространения и рассылки информации, позволил выполнять финансово-банковские операции, несмотря на расстояния и границы, однако, при этом, он выступает своеобразной площадкой не только для досуга и развлечений, но также и для новых деяний в сфере компьютерной информации. При квалификации данных преступлений продолжают возникать различные проблемы, связанные с определением признаков состава преступления, что во многом обусловлено несовершенством действующего законодательства. Несмотря на проводимые исследования, все больше имеющие место в последние годы, разрешить имеющие проблемы в полной мере так и не удается, что находит свое проявление как в дискуссиях среди исследователей по рассматриваемым вопросам, до настоящего времени не пришедших к единому мнению по многим аспектам, так и в разнообразии судебной практики, различных подходах, используемых органами предварительного расследования и судами при квалификации таких деяний. Все это и обусловило актуальность выбранной темы.

В настоящее время по поводу определения, содержания, а также процессуального порядка получения, оценки и использования информации на электронных носителях ведутся активные научные дискуссии. Высказываются различные точки зрения, подчас противоположные и взаимоисключающие друг друга. В числе актуальных вопросов находится правовая неопределенность понятия электронного носителя информации как источника доказательственной информации. Недостатки правовой регламентации процессуального порядка получения доказательственной информации на электронных носителях отражаются на качестве расследования уголовных дел, правильности сбора и оформления доказательств в виде информации на электронных носителях. Кроме того, противоречивость правоприменительной практики и недостаток научно-обоснованных рекомендаций относительно порядка проверки и

использования информации на электронных носителях негативно сказываются при решении задач уголовного судопроизводства.

Оценка современного состояния решаемой научной проблемы. Следует говорить о том, что исследование особенностей осмотра, изъятия и хранения информации в системах облачного хранения набирает обороты. Все больше научных трудов посвящаются данному вопросу. К числу таких авторов можно отнести следующих: Афанасьева С.И., Добровлянина О.В. [8],Зайцев О.А. [20], Карташов И.И., Лесников О.А. [26],Количенко А.А. [27], Костяная Ю.С. [28], Мустафина А.Х. [34],Телевицкая Ю.А. [44], Яковлева К.Ю. [48] и др.

Цель диссертационного исследования: совершенствование процессуальных методик осмотра, изъятия и хранения информации в системах облачного хранения при производстве уголовного судопроизводства.

Вышеуказанная цель обусловила следующие задачи диссертационного исследования:

- изучить зарубежный опыт обнаружения, осмотра, изъятия данных с облачных систем хранилищ и ее хранение.

- изучить отечественной и зарубежной научной литературы по использованию в ходе досудебного расследования информации с систем облачного хранения.

- проанализировать методы использования облачных систем хранения в уголовном судопроизводстве.

- выработать процессуальный порядок обнаружения, осмотра и изъятия информации с облачных систем и дальнейшее ее использование в ходе досудебного расследования.

- выработать предложения и рекомендации по совершенствованию законодательства с целью использования информации с облачных систем и синхронизации в электронное уголовное дело.

Объектом работы являются общественные отношения, связанные с осмотром, изъятием, хранением в системах облачного хранения при проведении расследования по уголовному делу.

Предметом являются нормы права, осуществляющие регулирование общественных отношений, связанных с осмотром, изъятием, хранением всистемах облачного хранения при проведении расследования по уголовному делу.

Методы и методологические основы проведения исследования. Методологическую основу исследования состовляют общенаучные и частнонаучные методы познания, к числу которых можно отнести анализ, синтез, индукцию и дедукцию, сравнительно-правовой, формально-юридический.

Обоснование научной новизны. Научная новизна данного исследования определяется в научно-обоснованных предложениях по решению выявленных проблем правового регулирования, реализация которых поможет решить выявленные проблемы.

Положения, выносимые на защиту:

1. Разработаны определения следующих понятий: «удаленный (онлайн) обыск» и «Облачное хранилище данных» (приложение 1);

Введение определений «удаленный (онлайн) обыск» и «облачное хранилище данных» в УПК РК является необходимым шагом для обеспечения законности, эффективности и защиты прав граждан при расследовании преступлений, совершаемых с использованием информационных технологий.

2. В целях обеспечения правовой регламентации возможности правоохранительных органов в использовании дистанционного следственного действия и эффективное расследование преступлений в сфере информационных технологий предлагается в статью 7 УПК РК дополнить новым подпунктом 59 следующего содержания:

59) «удаленный (онлайн) обыск – действия, проводимое лицом, осуществляющим досудебное расследование для поиска фактических данных правонарушении через интернет, в режиме онлайндоступа к персональному оборудованию обыскиваемого лица».

3. Разработана авторская редакция определения понятия «Облачное хранилище данных» – это модель онлайн - хранилища, данные в котором хранятся на множественных серверах,распределённых в сети»(приложение 1).

Введение данной нормы в статью 1 Закона Республики Казахстан «О персональных данных и их защите» дополнительным пунктом 14-1 обеспечит защиту конституционных прав и свобод граждан, включая право на конфиденциальность и защиту их персональных данных в облачных хранилищах.

4. Разработан проект нормы УПК РК 221-1 «Осмотр облачных хранилищ», регулирующий порядок осмотра облачных хранилищ данных (приложение 1).

Введение данной нормы обеспечит прозрачные и законные процедуры осмотра, а также защиту данных и приватности пользователей. Это дополнение законодательства позволит соответствовать современным технологическим реалиям, обеспечив эффективное расследование преступлений в цифровой среде и защиту прав и интересов граждан.

Апробация и внедрение результатов. Теоретические выводы и практические предложения приняты к сведению Следственного департамента Министерства внутренних дел Республики Казахстан(приложение 2).

Наряду с этим, отдельные выводы отражены в следующих научных публикациях:

1) Научная статья на тему: «Состояние и перспективы правового регулирования облачных систем» // сборник международной научно-практической конференции «Искусственный интеллект и большие данные

(Bigdata) в судебной и правоохранительной системе: реалии и требование времени», Республика Казахстан, г.Астана, май 2023 г.

2) Научная статья на тему: «Защита персональных данных в облачных хранилищ и права физических лице» опубликована в Международном научном журнале «Ғылым»Костанайской академии МВД РК им. Ш. Кабылбекова, Республика Казахстан, г.Костанай, март 2024 г.

3) Научная статья на тему: «Бұлттықоймалардағыдербесдеректердіңқұпиялығынжәнежекетұлғалардыңқұқықтарынқамтамасызету» опубликована в Международном научном журнале «Хабаршы - Вестник» Карагандинской академии МВД РК им Б.Бейсенова, Республика Казахстан, г.Караганда, март 2024 г.

4) Научная статья на тему: «Инновационные подходы противодействия киберугрозам» сборник международной научно-практической конференции: «Правоохранительная система Казахстана в новой глобальной реальности: состояние, реформы, развитие» Республика Казахстан, г.Алматы, март 2024 г.

Материалы научного исследования внедрены в учебные процессы кафедры «Конституционного и гражданского права» Евразийского национального университета имени Л.Н.Гумилева (по дисциплине «Антикоррупционная культура») (приложение 3).

Структура и объем диссертации. Работа состоит из введения, двух разделов, включающих 5 подразделов, заключения, списка использованных источников и приложения.

1 Использование систем облачного хранения: зарубежный и отечественный опыт

1.1 Зарубежный опыт обнаружения, осмотра, изъятия данных с облачных систем хранилищ и ее хранение

Как отмечают В.Л. Кулапов и А.В. Малько, для правовой системы характерна не только особая юридическая значимость нормативных актов, но и высокая степень теоретизации юридической терминологии. В то же время теория права носит характер, используемый в англосаксонской правовой системе, где юриспруденция играет важную роль в регулировании общественных отношений[30].

В Соединенных Штатах Америки, например, доказательства не делятся на различные виды. Важным является оценка допустимости доказательства. Таким образом, в отношении возможности существования «цифровых доказательств»и их места среди доказательств в уголовном процессе разногласий, по-видимому, нет. Главное, чтобы при сборе доказательств, в том числе и цифровых, соблюдались права и законные интересы.

Бытует мнение, что правовая система США основана исключительно на прецедентном праве и законодательстве штатов и что единого федерального законодательства не существует. На практике это не так. Несмотря на то, что уголовное право и процесс в разных штатах существенно различаются, существуют общие принципы уголовного процесса, которые в той или иной степени обязательны для правоохранительных органов и судов штатов. К таким источникам права относятся Конституция США, законодательные акты, международные договоры, нормы процессуального права, а также постановления и решения федерального правительства[11].

В 1961 г. комитет, назначенный председателем Верховного суда Эрлом Уорреном, опубликовал «Предварительный отчет о целесообразности и

практической осуществимости унифицированных правил доказывания для окружных судов США», в котором рекомендовал принять единые правила доказывания[82]. На основе этого отчета и последующих рекомендаций в 1965 г. был назначен комитет для разработки проекта. Федеральные правила доказывания были приняты Верховным судом США в 1972 г. и окончательно вступили в силу в 1975 г.[74].

Согласно пр.101 Федеральных правил доказывания, к письменным материалам относится, в частности, информация, хранящаяся в электронном виде. Форма, в которой представлена письменная информация, не имеет значения.

Нормативные акты устанавливают, что в случае информации на бумажном носителе, её истинное отражение – это та версия, воспринимаемая создателем или подписантом как подлинная; тогда как в контексте электронных данных, первейшую важность приобретает материализованный экземпляр, будь он отпечатанным или представлен в иной форме, пригодной для визуального восприятия. В отношении термина «копия», закон явно не вносит разграничений, утвердив её как доскональное отображение первоисточника, заверенное посредством использования разнообразных методологий воссоздания, включая механические, фотографические, электронные, химические либо другие подобные процедуры. Хотя американские законодатели не проводят различия между «электронными»и обычными доказательствами, они признают уникальность «электронных»доказательств.

Другим федеральным законом, регулирующим использование цифровых доказательств в уголовных делах в США, являются Федеральные правила уголовного судопроизводства[39]. В этих правилах не проводится конкретного различия между понятиями цифровых (электронных) доказательств. Согласно Правилу 41(a)(2)(A), и информация, и другие материальные объекты классифицируются как «собственность». Зарубежные ученые утверждают, что этот принцип, наряду с Четвертой поправкой к Конституции США, играет

основополагающую роль при сборе «цифровых доказательств». В соответствии с принципами Четвертой поправки, защита прав граждан перед лицом вмешательства государства в личное пространство зафиксирована жестко: ни одна особа не обязана терпеть несанкционированные проникновения в свою частную жизнь, в том числе в отношении дома, документов и финансов. Обязательным условием для выдачи судебного ордера на проведение обыска или изъятия является предъявление веских доказательств, удостоверенных клятвой или утверждением государственного чиновника. Акцентируется строгость в определении мест, предметов или персон, в отношении которых допускается описанные юридические процедуры.

Следует отметить, что термин «обыск»в законодательстве США трактуется иначе, чем в Казахстанскомправе. Согласно прецедентному праву, «обыск» - это любые действия государственных органов, нарушающие «разумное ожидание неприкосновенности частной жизни»и, естественно, требующие разрешения суда. Интерпретацию доктрины «разумного ожидания неприкосновенности частной жизни»можно найти в различных судебных решениях, согласно которым человек имеет право рассчитывать на неприкосновенность частной жизни в собственном доме, при разговоре по таксофону. Напротив, действия на публике или проникновение в жилище другого лица с целью ограбления не создают разумного ожидания неприкосновенности частной жизни. Что касается цифровых устройств и цифровой информации, то суды считают, что человек имеет такое же право на неприкосновенность частной жизни, как и предметы, хранящиеся в закрытых местах, включая портфели, кошельки и папки. В то же время люди не имеют разумного ожидания неприкосновенности частной жизни в отношении информации, размещенной на общедоступных компьютерах (библиотеках) или веб-сайтах. Однако, помимо понятия разумного ожидания неприкосновенности частной жизни, прецедентное право США также включает в себя доктрину «открытого обзора», означающую, что сотрудник полиции может осматривать

любой предмет, находящийся в поле его зрения, если он считает, что этот предмет имеет отношение к преступлению. При этом должна существовать четкая связь между предметом и преступлением.

В американской правовой системе цифровые устройства рассматриваются как закрытые контейнеры, для доступа к которым требуется ордер на обыск.

В деле Riley v California Верховный суд США постановил, что смартфоны могут быть конфискованы только по решению суда. Судьи обосновали свое решение следующим образом: «Цифровые устройства по своей доказательной силе ничем не отличаются от кошельков, портфелей и автомобилей. Какими бы маленькими они ни были, основные права человека распространяются на хранящиеся в них персональные данные». Таким образом, смартфоны могут быть проанализированы в трех аспектах:

1) какисточник цифровой информации

2) как орудие преступления

3) В качестве носителя материальных следов (вещественных доказательств).

Если смартфон выступает в третьем качестве, например, если преступник использует его для избиения жертвы или для сокрытия запрещенных в деле веществ, то судебное разрешение на конфискацию не требуется. В двух других случаях разрешение суда требуется, если информация на цифровом устройстве имеет значение для уголовного дела.

Согласно статье 41, обыск с целью ареста имущества может быть произведен на основании ордера на обыск, выданного судьей, с указанием лица или места, подлежащего обыску. Ордер не может исполняться более 14 дней, после чего он должен быть возвращен судье. На сегодняшний день данные процедуры обыска применяются также в делах, связанных с доступом к цифровой информации.

Как отмечает О.С. Керр, развитие цифровых технологий потребовало разработки новых процессуальных норм, регламентирующих сбор цифровых

доказательств в уголовном процессе[78]. В то время существовавшие процедуры получения и исполнения ордеров на обыск предполагали поиск доказательств на стадии обнаружения и изъятия вещественных доказательств следственным подразделением. С появлением цифровых устройств одноэтапный поиск трансформировался в двухэтапный: сначала необходимо было найти и изъять цифровые информационные устройства, и только после анализа носителей информации - найти и изъять цифровые доказательства. В этом отношении два расследования отличаются друг от друга. Они проводятся в разное время, в разных местах и, как правило, разными лицами[69].

Разделение традиционного одноэтапного ордера на два разных этапа ставит перед полицией четыре вопроса. Во-первых, в ордере должно быть указано, какие именно предметы подлежат изъятию: физическое оборудование, изъятое в ходе первоначального физического обыска, или цифровые доказательства, полученные в ходе электронного обыска?

Во-вторых, какое место должно быть указано в ордере на обыск: местонахождение цифрового оборудования или само цифровое оборудование, т.е. местонахождение цифровой информации? В-третьих, к какому сроку должен быть исполнен ордер на обыск: Должен ли этот срок подчиняться правилам, регулирующим исполнение обычных ордеров на обыск, другим правилам или вообще не подчиняться? И наконец, какие условия применяются к исполнению ордера на обыск цифровой информации и когда должна быть возвращена, изъята компьютерная техника [76]. Существенная проблема возникает также при необходимости поиска и доступа к цифровой информации с отдельных устройств и компьютерных сетей. Неясно, что искать - местоположение удаленного пользователя или реальное место хранения нужной цифровой информации. Во многих случаях определить место хранения информации сложно или невозможно. Что делать, если место хранения данных находится за пределами США?

Поправка к статье 41 Федеральных правил уголовного судопроизводства решает эти проблемы. Во-первых, она уточняет полномочия судей по выдаче разрешения на получение электронной информации путем удаленного доступа. Согласно параграфу (b)(6), судья, обладающий юрисдикцией в любом округе, в котором могла быть совершена преступная деятельность, имеет право выдать ордер на обыск электронных носителей и использовать удаленный доступ для изъятия или копирования информации, хранящейся в электронном виде, расположенной в округе или за его пределами. Во-вторых, правило 14-дневного ордера распространяется только на этап физического сбора (изъятие или копирование носителей или информации на месте), но не на последующие действия с изъятыми доказательствами (e)(2)(B). В этой связи отметим различия между отечественным уголовно-процессуальным законодательством и законодательством США в отношении правовой природы копирования цифровой информации.

Согласно положениям Уголовно-процессуального кодекса РК[1], копирование информации с изъятых носителей осуществляется для защиты интересов их владельцев, т.е. в качестве процессуальной гарантии. В законодательстве США копирование может осуществляться сразу после обнаружения информации, без необходимости изъятия оригинала, то есть, по мнению национальных правоохранительных органов, оно является самостоятельным следственным действием, в результате которого создаются доказательства по делу[37].

В ситуациях, когда электронные хранилища данных подвергаются конфискации или их содержимое дублируется, допускается сокращение перечня до определения физических параметров конфискованных или клонированных устройств. Регламентируется возможностью для офицера удерживать дубликаты изъятой электронной информации, соответствующие стандартам (f)(1)(B).

В соответствии с положениями Раздела 41, работники, осуществляющие дистанционный доступ с целью выполнения цифрового розыска и последующего экстрагирования или репликации данных, сохранённых в электронном формате, обязаны направить заинтересованному лицу, которое либо является владельцем целевого имущества, подвергшегося процедуре обыска, либо обладает правом владения экстрагированной либо скопированной информацией, дубликат официального разрешения на проведение таких операций и полученные подтверждения об их исполнении.Эта услуга может быть оказана любыми средствами, включая электронные, разумно рассчитанными для достижения цели, указанной в (f)(1)(C).

Доказательства по уголовным делам в США должны отвечать определенным требованиям, в том числе и по надежности. Цифровая информация может считаться надежной и приниматься в качестве доказательства, если она имеет характер обычного делового документа, поскольку заинтересованное лицо не будет полагаться на документ, считающийся ненадежным.

Доступ к цифровым доказательствам в уголовных расследованиях показал тенденцию не признавать чисто компьютерные деловые документы из-за сложных различий между документами, созданными компьютером, документами, созданными человеком, но хранящимися на компьютере, и документами, оцифрованными и хранящимися в виде архивных журналов[80].Ключевым фактором признания деловых документов в соответствии с Правилом 801 является то, что эти документы должны быть подлинными[74]. Именно этот принцип определяет сложность, неопределенность и конечную допустимость доказательств в большинстве случаев.

Цифровая информация, используемая для аутентификации, должна быть аутентифицирована, т.е. должна быть подтверждена, что она получена с определенного носителя.

В деле UnitedStates v. DeGeorgia подчеркивается, что стандарт доказывания подлинности электронного документа такой же, как и стандарт доказывания подлинности других документов. Основные требования одинаковы, если информация генерируется компьютером. Для того чтобы все доказательства были допустимыми, необходимо создать основу подлинности, что в большинстве случаев требует от свидетеля дать показания о подлинности цифровой информации.

Свидетели не должны обладать специальной квалификацией или статусом эксперта. Свидетелю достаточно знать факты, относящиеся к предмету его показаний. В деле U.S. v. Whitaker, 127 F.3d 595, 601 свидетель показал, что он присутствовал при изъятии компьютера обвиняемого и документов из него. Эти показания были признаны достаточными для установления истины.

Однако полиция использует в качестве свидетелей людей, имеющих опыт работы с цифровыми технологиями. Это связано с тем, что свидетель, не знакомый с компьютерами, может оказаться не в состоянии использовать цифровые доказательства в суде. Например, в деле AmericanExpressTravel-RelatedServices, Inc. vVinhnee суд по делам о банкротстве запретил использовать электронные документы в качестве доказательства задолженности, поскольку суд установил, что арбитражный управляющий не смог ответить на элементарные вопросы об аппаратном и программном обеспечении и базах данных, используемых для создания и ведения электронных копий.

Аналогичные положения существуют и в отношении изъятия цифровой информации и цифровых носителей в рамках уголовного судопроизводства в Канаде. Как правило, обыск должен быть санкционирован судом. Исключения составляют обыск с согласия обыскиваемого лица, обыск брошенного имущества[75], угроза полиции или общественной безопасности, а также исключительные обстоятельства[73]. Кроме того, существует ряд других

причин, по которым для поиска цифровой информации не требуется разрешение суда.

Речь идет об угрозе потери цифровой информации. Этот принцип проявился в деле R. v. Fearon, 2014 SCC 77, [2014] S.C.R. 621.

Самое главное, что смартфон был найден у одного из подозреваемых, арестованных за кражу ювелирных изделий. Проанализировав содержимое телефона, полицейские обнаружили текстовые сообщения и фотографии, указывающие на то, что именно этот подозреваемый совершил ограбление. Исследование содержимого смартфона было проведено без ордера на обыск. Судьи разошлись во мнениях относительно законности действий полиции. Однако четверо из семи судей постановили, что, несмотря на признаки вторжения в частную жизнь, полиция должна была срочно и объективно изучить содержимое мобильных телефонов, иначе доказательства могут быть утеряны.

Канадское законодательство не только устанавливает общие правила оценки доказательств, но и предъявляет дополнительные требования к электронным документам. Согласно статье 31.1 Закона Канады о доказательствах, подлинность электронного документа должна быть подтверждена, если его подлинность может быть установлена на основании целостности системы записи и хранения электронного документа (статья 31.3) или путем исследования под присягой (статья 31.5). Бремя доказывания подлинности электронного документа возлагается на лицо, представляющее документ в качестве доказательства (раздел 31.3)[70].

В статье 31(8) упомянутого законодательства предоставляется исчерпывающее описание компьютеризированных систем, информационных массивов, электронных носителей данных, а также их сетевой инфраструктуры. Среди прочего, понятие электронного документа характеризуется как информация, закодированная или сохраненная на любом устройстве хранения, в рамках компьютерных систем или аналогичных технологий, доступная для

интерпретации, как пользователем, так и машинной интеллектуальной системой. В то время как европейская консолидация набирает обороты, законодательная гармонизация в области уголовного правосудия остается разрозненной, не знающей единой юридической базы в пределах Европейского содружества. Легальные основы уголовно-правовых и процессуально-уголовных систем Союза ещё лежат в основе национальных правовых доктрин и исторически сложившихся норм [77].

Уголовно-процессуальный кодекс Германии подробно регламентирует сбор цифровой информации в рамках уголовного расследования. Для уголовного процесса Германии характерна возможность проведения «тайных»следственных действий, аналогичных следственным действиям нашей компании. В связи с этим цифровая информация может быть получена в ходе различных следственных действий: изъятие, обыск, досмотр, перехват, перехват телекоммуникаций и электронное расследование. Уголовно-процессуальный кодекс Германии ограничивает изъятие письменного обмена информацией между обвиняемым и лицом, пользующимся свидетельским иммунитетом (ст. 52 и 53 УПК Германии). Как и в отечественном уголовном процессе, контроль информации, передаваемой по телекоммуникационным каналам, осуществляется без уведомления получателя информации (§ 100a Уголовно-процессуального кодекса Германии).

К ним относятся, в частности, электронные письма, SMS-сообщения, текстовые и голосовые сообщения. Использование информации, связанной с частной жизнью, полученной в связи с мониторингом цифровых каналов связи, не разрешается. Сбор информации с помощью цифровых технологий разрешается только судом по ходатайству стороны обвинения[81]. Следует отметить, что возможность получения цифровой информации, передаваемой по телекоммуникационным сетям, зависит от тяжести совершенного преступления. Другое предположение заключается в том, что установить

реальные обстоятельства дела и местонахождение обвиняемого, не прибегая к перехвату цифровой информации, будет слишком сложно.

В Германии законодательные нормы тщательно регламентируют доступ к данным о трафике, признавая эти данные закрытыми от общего доступа. Серьезные нарушения закона или инциденты, имеющие отношение к использованию телекоммуникационных технологий, могут оправдать запрос такой информации. При этом необходимо строгое соблюдение принципа пропорциональности между важностью дела и объемом запрашиваемой информации, что является ключевым аспектом немецкого уголовно-процессуального законодательства (указано в § 100g KUHAP). Далее, когда речь идет о проведении следственных мероприятий с целью сбора цифровых данных, § 101 Уголовно-процессуального кодекса обязывает правоохранительные органы Германии информировать заинтересованные стороны. К таковым относятся, например, обвиняемые, а также лица, отправляющие и получающие электронную корреспонденцию, и те, кто находится в условиях содержания под стражей.

Уведомление должно быть сделано как можно скорее. Цель расследования, жизнь, физическая неприкосновенность, личная свобода или собственность других лиц не должны подвергаться опасности, включая возможное использование дополнительных тайных следственных действий (§ 101(5) Уголовного кодекса Германии).

Особенность процедуры доказывания по французским уголовным делам заключается в свободе выбора способа получения доказательств. При этом органы расследования вправе делать все, что им заблагорассудится, для установления обстоятельств совершенного преступления. На наш взгляд, эта особенность обусловлена существованием «свободных доказательств», которые не подчиняются процессуальным формулам и не регламентируются законом[16].

Статьи 706-96 Уголовного кодекса Франции разрешают следователям использовать технические средства для доступа к цифровой информации, отправляемой, хранимой и передаваемой по телекоммуникационным сетям. При этом данные средства могут не только управляться дистанционно, но и устанавливаться на компьютеры или другие цифровые устройства подозреваемых без их согласия[72].

Изъятию подлежат не только оригиналы цифровой информации и носителей, но и копии, которые могут быть использованы в качестве доказательств в уголовном процессе (ч. 5 ст. 56 и ч. 3 ст. 97 Уголовно-процессуального кодекса).

Как и во Франции, Уголовно-процессуальный кодекс Бельгии не содержит исчерпывающего перечня доказательств.

Доказательства могут быть представлены любыми способами, не запрещенными законом[43]. Уголовно-процессуальный кодекс Бельгии учитывает специфику процедуры доступа к цифровой информации. В ходе уголовного судопроизводства владелец цифровой информации может быть не только задержан, но и скопирован, а доступ к этой информации может быть ограничен или удален (ст. 36a).

Согласно Уголовно-процессуальному кодексу Бельгии, при необходимости доказать подлинность дела или при наличии риска потери информации может быть проведен обыск не только компьютерной сети, но и других доступных к ней сетей (ст. 88ter)[71]. На наш взгляд, включение подобных положений в национальное уголовно-процессуальное законодательство позволит частично решить проблему правового регулирования доступа к цифровой информации, хранящейся «в облаке».

На основании вышеизложенного приходим к выводу,что даже в странах со схожими правовыми традициями существуют существенные различия в национальном законодательстве и подходах к регулированию использования цифровой информации в уголовном процессе.Если в некоторых странах к

цифровой информации применяются традиционные правила доказывания, то в других странах существуют специальные законы, регулирующие этот вопрос.Если доступ к цифровой информации затрагивает конституционные права и свободы граждан, то для проведения следственных действий требуется разрешение суда. В остальных случаях такого разрешения не требуется.Оригинальная цифровая информация может быть изъята вместе с носителем, либо в качестве доказательства может быть использована копия. В обоих случаях подлинность должна быть доказана.Сбалансированное использование зарубежного опыта внесет существенный вклад в развитие отечественного уголовно-процессуального законодательства в части использования цифровой информации в уголовном процессе, которое в настоящее время игнорируется отечественным законодателем.

1.2 Использование в ходедосудебного расследования информации с систем облачного хранения

В соответствии с Уголовно-процессуальным кодексом Республики Казахстан (далее –УПК Республики Казахстан) допускается использование электронных документов (документы, в которых информация предоставлена в электронно-цифровой форме и удостоверена посредством электронной цифровой подписи, п. 15 ст. 7 УПК Республики Казахстан) в качестве протоколов следственных и процессуальных действий, решений должностных лиц, в том числе приговоров по делу; защитнику предоставляется право с использованием научно-технических средств опрашивать с их согласия лиц, предположительно владеющих информацией, относящейся к уголовному делу, ход такого опроса можно отразить на электронном носителе (п. 5 ч. 3 ст. 122 УПК Республики Казахстан).

Активное использование информационных технологий привело к внедрению в сферу досудебного интереса ряда технологических устройств, содержащих видеоинформацию, связанную с расследуемыми преступлениями.

Например, в настоящее время для обеспечения безопасности граждан, жилья, рабочих мест, учреждений и других объектов широко используются технические средства, и оборудование для видеонаблюдения является важной частью этой деятельности. Зафиксированные таким оборудованием события, объекты и окружающая обстановка могут дать важную криминальную информацию. Следовательно, основной задачей следователей является эффективное обнаружение, фиксация и изъятие такой информации, предотвращение ее утраты (уничтожения) или манипулирования ею, а также соблюдение всех необходимых процессуальных требований и тактических условий.

Поиск оборудования для камер видеонаблюдения часто является неотъемлемой частью начальных этапов практически всех современных уголовных расследований.

Для получения или копирования криминалистически значимой информации при камерном видеонаблюдении необходимо знать местоположение носителя видеозаписи. В таких случаях видеофайлы хранятся на сервере системы видеонаблюдения, а местоположение может соответствовать адресу здания, в котором установлена камера, или находиться гораздо дальше. Хотя на практике доступ к видеозаписям с камер наблюдения не вызывает серьезных проблем, вопрос изъятия цифрового видео и приобщения его к документам уголовного дела в настоящее время является дискуссионным и представляет определенные трудности.

В современной следственной практике записи с камер наблюдения могут быть получены по запросу и зафиксированы в ходе осмотра места происшествия, выемки или дознания. Поэтому при осмотре места происшествия следует обращать внимание не только на наличие камер

наблюдения на месте преступления, но и на наличие камер наблюдения в местах возможного приближения или отхода преступников от места преступления. Обнаружение этих камер и изучение видеозаписей обычно поручается сотрудникам компании. Также устанавливаются и приглашаются к участию в расследовании владельцы камер и сотрудники (техники), непосредственно управляющие системой видеонаблюдения в организации.

Если в результате просмотра видеозаписи обнаруживается информация, имеющая значение для расследования, вещатель готовит отчет. Кроме того, проводится рецензирование изъятого видеоматериала, и в протокол рецензирования включаются только те фрагменты, которые имеют значение для расследования уголовного дела. Необходимые видеофрагменты копируются на функциональные электронные носители информации, из них составляется и распечатывается фототаблица, которая является приложением к протоколу следственного действия. Оригинал задержанной видеозаписи и носитель информации приобщаются к материалам уголовного дела»[25].

Однако, как показывает практика, на ранних стадиях расследования, когда необходимо получить информацию о преступлении, зафиксированном камерой наблюдения, изъятие видеозаписей, как правило, производится непосредственно в ходе осмотра места происшествия, а не путем конфискации. Это происходит по разным причинам:

1.При осмотре места происшествия не всегда удается обнаружить доказательства совершения уголовного преступления, поэтому до досудебного расследования может пройти некоторое время. Поскольку выемка можетбыть произведена только после начала досудебного расследования уголовного дела, необходимые видеоматериалы (и не изъятые вовремя доказательства) могут быть случайно или намеренно уничтожены до принятия следственным судьей решения о проведении данного следственного действия.

2.При осмотре места происшествия сотрудники милиции, как правило, имеют возможность обратиться за непосредственной помощью к техническому

специалисту - сотруднику учреждения, располагающего аппаратурой видеонаблюдения, который может оперативно подготовить и предоставить необходимый видеоматериал. Но тогда могут возникнуть трудности, связанные с тем, что специалиста нет на рабочем месте, поэтому необходимо связаться с руководством учреждения и пригласить сотрудника на работу.

3.В связи с большим количеством находящихся в производстве уголовных дел и появлением новых следственных задач, требующих срочного решения, внимание следователей постоянно отвлекается на другие приоритетные направления работы, и видеозаписи в дальнейшем могут быть не заняты.

Мы считаем целесообразным изымать записи с камер видеонаблюдения в ходе расследования на месте преступления. Одним из наиболее весомых аргументов в пользу такого подхода является то, что при задержке изъятия цифровая видеоинформация может быть утеряна или уничтожена. В этом контексте важно также учитывать, что некоторые системы видеонаблюдения работают особым образом: видеозаписи сохраняются на диске и хранятся там относительно недолго - до полного заполнения накопителя. Затем на тот же накопитель записывается новая информация, а предыдущая удаляется. Таким образом, время хранения видеоинформации, хранящейся на диске, может исчисляться неделями или часами[15].

Следует также учитывать, где должны быть определены границы осмотра оборудования для видеонаблюдения в полевых условиях. Опираясь на традиционное криминалистическое понятие «место преступления»[10]и анализ архитектурных особенностей различных систем видеонаблюдения, можно сделать следующие выводы.

Как уже отмечалось, основой интегрированной системы видеонаблюдения является выделенный сервер, в функции которого входит запись видеопотока с камеры, хранение, кодирование и декодирование информации, а также управление периферийными устройствами. В условиях

ограниченного пространства сервер не может заменить цифровой видеорегистратор, особенно если система видеонаблюдения устанавливается только для просмотра и архивирования видеоданных. Поскольку криминалистически значимая видеоинформация является не чем иным, как цифровым отпечатком преступления, место расположения носителей информации можно официально считать частью места преступления. В свою очередь, эти носители информации могут быть изъяты в ходе обычного осмотра места происшествия в присутствии представителя организации (владельца системы видеонаблюдения) и при поддержке упомянутых выше технических экспертов.

В то же время, учитывая, что некоторые современные авторы считают, что такой подход приводит к несправедливой трактовке термина «место происшествия»[47], мы вынуждены признать, что наша точка зрения является спорной. Предложенный подход также представляется неоднозначным, когда в системах видеонаблюдения используются сетевые хранилища данных (NAS) или облачные сервисы. NetworkAttachedStorage - это дисковый массив (внешнее хранилище) и аппаратная платформа, которая может быть частью глобальной или локальной сети. NAS используется для резервного копирования или архивирования данных с камер видеонаблюдения. Передача данных может осуществляться удаленно. Сервер не связан физически с местом установки системы видеонаблюдения и может находиться в любой точке мира. Облачные системы видеонаблюдения также предполагают хранение файлов на удаленных серверах (облачная инфраструктура), доступ к которым можно получить в любое время через Интернет из любой географической точки. Контроль и управление облачными серверами и каналами связи осуществляет компания, организующая облако (провайдер).

В связи с этим некоторые ученые и практики предлагают, как представляется, действенное решение проблемы, например, включение

задержаний в число допросов и разрешение предъявления задержаний до начала уголовного судопроизводства[13].

Доступ к видеозаписям с камер наблюдения обычно не требует изъятия носителя информации. Для проведения следственных действий достаточно воспроизведения такой информации. Это делается без нарушения работы системы безопасности, без причинения материального ущерба и других неудобств владельцу, что позволяет избежать конфликтных ситуаций[14].

При проведении следственных действий, связанных с контролем, записью и изъятием цифровой видеоинформации, важно заранее иметь технические средства для копирования запрашиваемой информации. Для копирования информации на записанный диск рекомендуется использовать внешние оптические приводы или внешние накопители (жесткие диски и твердотельные накопители). Следует подчеркнуть, что для указанных целей могут использоваться только технические средства правоохранительных органов (специалисты, следственные подразделения). Использование оборудования для личного пользования или оборудования, принадлежащего организации, создает условия для возможной манипуляции или уничтожения скопированной информации. Организационные средства для воспроизведения информации могут быть использованы только в том случае, если явно исключается противоправное воздействие.

Как отмечается в уголовно-процессуальной литературе, изъятие электронных носителей информации в рамках проведения некоторых следственных действий представляет особую сложность, поскольку производство электронных носителей информации зачастую является проблематичным для следственных органов, которые могут не обладать достаточными знаниями в области информационных технологий для доступа, хранения и надлежащего использования цифровой информации[39].

Стремительное развитие информационных и телекоммуникационных технологий радикально изменило жизнь современного общества. В то же время

электронная информация все чаще становится средством подготовки и совершения преступлений. Как отмечают некоторые авторы, сегодня информация электронных СМИ активно используется для предоставления доказательств по уголовным делам[9].

Несмотря на необходимость упоминания об использовании электронных (цифровых) носителей информации для получения доказательств в уголовном процессе, действующее уголовно-процессуальное законодательство Российской Федерации не регулирует данные правоотношения комплексно. Например, отсутствует нормативное правовое определение термина «электронные носители информации», что не позволяет выявить, чем они отличаются от других цифровых устройств.

Правильное понимание содержания электронных носителей информации оказывает непосредственное влияние на решение теоретических и правовых вопросов, связанных с изъятием электронных носителей информации в уголовном процессе. Особенно это актуально для процедуры изъятия электронных носителей информации в ходе досудебного расследования уголовных преступлений в экономической сфере.

В процессуальной литературе обращается внимание на то, что при совершении коммерческих преступлений нередко удается установить нарушение конституционных прав (собственности, пользования и распоряжения) других лиц, не являющихся подозреваемыми или обвиняемыми по уголовному делу, и поэтому при расследовании таких дел возможно изъятие не только оргтехники, документов, но и денег, а также неизбежного ущерба, вызванного изъятием и конфискацией денег. Следует также отметить, что следственные органы могут беспрепятственно и без достаточных оснований изымать важнейшую оргтехнику и документы, что приводит к «параличу»работы компании, поскольку на изъятых компьютерах содержатся важнейшие документы и программы[45]. Когда юридические лица изымают электронные носители информации на неопределенный срок, это часто

приводит к приостановке или полному прекращению деятельности. Владелец электронного носителя информации не может получить информацию о местонахождении изъятого объекта в связи с состоянием дела, передачей следственных материалов и т.д. В результате изъятый объект может быть не возвращен вообще или частично, что нарушает права участников уголовного судопроизводства[24]. Изъятие электронного оборудования и технических средств может привести к прекращению предпринимательской деятельности или ухудшению финансового положения юридического лица[38]. Поэтому изъятие и задержание товаров и документов (в том числе электронных носителей) может быть санкционировано только в том случае, если это необходимо для судебного разбирательства и носит временный характер.

И.С. Исянаманов пишет, что при изъятии изъятых предметов (оргтехники, документов, компьютеров) и принятии их в качестве доказательств требуется особый подход, который может включать полное изъятие документов и оргтехники и их консервацию, что является исключением[22].

Изъятие электронных носителей информации производится в связи с проведением следственных действий с участием экспертов. Однако, как отмечают некоторые авторы, несмотря на это положение, на практике электронные носители информации часто изымаются следственными органами самостоятельно, без привлечения экспертов. Это приводит к изъятию информации, не имеющей отношения к предмету доказывания, а длительные сроки следствия, связанные с проведением некоторых следственных действий (например, экспертизы), оказывают серьезное негативное влияние на владельцев изъятых электронных носителей.

Защита может использовать тот факт, что информация была изъята без участия эксперта, для оспаривания доказательств и указать на то, что носитель информации мог манипулировать и фальсифицировать доказательства в ходе изъятия. Таким образом, законодатель предлагает различать электронные

носители информации, которыми можно манипулировать, и те, которые могут быть изъяты независимо от следственных органов.

Многие авторы утверждают, что при изъятии и копировании информации с электронных носителей важно привлекать не только свидетелей-экспертов, но в идеале и свидетелей, обладающих знаниями в области информационных технологий[29].

В то же время следует отметить, что изъятие карт памяти, CD-RW и т.д. не требует специальных знаний, поскольку эти средства максимально просты в использовании. С другой стороны, изъятие электронных носителей с использованием внешних онлайн – ресурсов «облачного хранения»требует особого внимания. На сегодняшний день особых правовых проблем, связанных с изъятием или копированием информации, хранящейся в «облаке», не существует. Проблема заключается в том, что доступ к такой информации может быть затруднен, поскольку серверы, на которых она хранится, во многих случаях физически расположены в удаленных районах. Для перехвата таких электронных носителей требуется доступ к информации, хранящейся на удаленных серверах. Однако это может оказаться невозможным, поскольку пользователи электронных носителей, имеющие доступ в Интернет, могут легко уничтожить такую инкриминирующую информацию[10].

В облачных учетных записях обычно используется двухфакторная аутентификация - не только логины и пароли, но и SMS-коды, пароли, отправленные на другие почтовые ящики, USB-ключи и даже биометрия. По мнению ИТ-экспертов, аутентификация с помощью сервисов Google широко распространена, поскольку SMS-аутентификация бесполезна в случае кражи мобильного телефона. Например, получив в свое распоряжение устройство, подозреваемый может удаленно войти в свои учетные записи с любого доступного устройства, выйти из всех учетных записей или изменить пароли.

Переводя взор на сферу кибербезопасности и анализируя защиту данных на различных устройствах, отмечается, что криптографические программы

стали неотъемлемой частью как мобильных операционных систем Android и iOS, так и настольных платформ MAC и Windows. Встроенные меры безопасности, такие как FileVault на операционной системе MAC и экстернальное приложение Veracrypt, ставшее выбором для пользователей Windows, играют ключевую роль в шифровании данных. Защищая все файлы путем криптографии, эти механизмы придают устройству статус «цифровой крепости», обычно активируясь автоматически в фоне безопасностных настроек.

Тем не менее, компьютерная утрата с активированным шифрованием, по словам специалистов, трансформируется в обузу для вора, ведь без ключа дешифровки аппарат становится лишь куском бесполезного железа. В свете этого появляется интригующий парадокс: информация, хранящаяся в «облаке», остается недосягаемой, несмотря на тщетные попытки взлома. Лишь перехватывая код восстановления через альтернативный гаджет, можно пытаться совершить подключение к данным, рассчитывая на удачный исход.

Для обхода запретов на прямой доступ к «облачным складам» информации, предпочитают применять методы удаленного подключения через специализированные технические и программные наборы инструментов, акцентируя внимание на копировании сведений, которое выполняется для последующего детального анализа. Такой подход, предложенный знающими людьми в этой области, позволяет эффективно избегать прямой кражи, оберегая исследователя от непредвиденных рисков и правонарушений.

Некоторые исследователи отмечают, что при изъятии электронных носителей необходимо иметь дело с паролями и специальными программами, отвечающими за защиту информации. Например, многократный ввод неправильного пароля уничтожает информацию, поэтому на этом этапе изъятия необходимо использовать специализированных программистов[36].

При изъятии электронного носителя информации допускается его копирование. При невозможности возврата правообладателю электронного

носителя информации, изъятого в связи с проведением оперативно-розыскных мероприятий, копирование информации, содержащейся на изъятом электронном носителе информации, осуществляется по требованию правообладателя изъятого электронного носителя информации или обладателя содержащейся на нем информации. Копирование этой информации на другой электронный носитель, предоставленный правообладателем изъятого электронного носителя информации или обладателем содержащейся в нем информации, осуществляется в присутствии понятых из органа предварительного расследования или суда и с участием правообладателя изъятого электронного носителя информации или обладателя содержащейся в нем информации и/или его представителя и эксперта. При копировании информации необходимо убедиться в том, что она не будет утрачена или изменена в сложившихся условиях. Не допускается копирование информации, если это может помешать расследованию преступления[12].

Эксперт, участвующий в следственных действиях, по просьбе правообладателя изъятого электронного носителя информации или владельца содержащейся на нем информации в присутствии понятых производит копирование информации, содержащейся на изъятом электронном носителе информации. Копирование информации осуществляется на другой электронный носитель информации, предоставленный правообладателем изъятого электронного носителя информации или обладателем содержащейся на нем информации. Электронный носитель информации, содержащий скопированную информацию, выдается правообладателю изъятого электронного носителя информации или владельцу содержащейся на нем информации. Следственные действия, связанные с восстановлением информации, и протокол заседания, на котором электронный носитель информации, содержащий восстановленную информацию, передается правообладателю изъятого электронного носителя информации или владельцу содержащейся на нем информации, протоколируются.

Материально-правовая природа воспроизведения информации на электронных носителях в Уголовно-процессуальном кодексе трактуется по-разному.

Д.В. Овсянников использует копирование электронной информации в качестве доказательства по уголовным делам[35].

Р.И. Оконенко утверждает, что копирование является самостоятельным процессуальным действием, но не следственным действием, поскольку происходит через перехваченные электронные носители информации[37].

По мнению В.А. Семенцова: «Существует потребность в электронном воспроизведении информации в исследовательской практике, и эта новая когнитивная технология отвечает требованиям правового, этического и социального законодательства в развитии общества. Достаточно интегрировать электронное воспроизведение в систему процессуальной деятельности, направленной на сбор доказательств»[42].

Таким образом, можно говорить о том, что уголовно-процессуальные нормы не успевают за условиями информационного общества, в котором совершаются преступления и проводятся следственные действия, поэтому необходимо не только адаптировать следственные действия к современным условиям, но и принять дополнительные меры, необходимые для расследования, выемки, фиксации цифровых данных. Электронные носители, содержащие скопированную информацию, должны быть переданы правообладателю конфискованного электронного носителя или владельцу содержащейся на нем информации. Должны быть составлены протоколы воспроизведения информации и передачи электронных носителей с воспроизведенной информацией правообладателю конфискованного электронного носителя или владельцу содержащейся на нем информации

2Особенности использования облачных систем хранения в уголовном судопроизводстве.

2.1 Методы использования облачных систем хранения в уголовном судопроизводстве

Информатизация судопроизводства в целом и уголовного, в частности, осуществляется по всему миру, в связи, с чем опыт зарубежных государств, в особенности стран, имеющих схожий с российским порядок производства по уголовным делам, представляет теоретический и практический интерес. В частности, в Республике Казахстан в декабре 2017 г. в Уголовно-процессуальный кодекс [1] были внесены изменения[2], позволяющие расследовать уголовные дела в электронном формате. Согласно материалам сайта Верховного Суда Республики Казахстан, первое электронное уголовное дело было рассмотрено уже в январе 2018 г. В Уголовно-процессуальный кодекс Республики Казахстанвведен новый термин: «формат уголовного судопроизводства»(ст. 42-1 УПК РК) и предусмотрено два формата: бумажный и электронный.

Электронная цифровая форма, как определено УПК РК, предоставляется для массива документов, важных в рамках уголовного процесса. К ним относятся различные типы судебных обращений и ходатайств, в числе которых: обвинительное сообщение, заявляющее о факте уголовного проступка (ч. 1 ст. 181УПК РК); иски гражданского характера (ч. 5 ст. 167 УПК РК); протесты относительно протоколов, зафиксированных в ходе судебных дебатов, независимо от их полноты (ст.ст. 348 и 348-1УПК РК);записи о главных разбирательствах в суде (ч. 8 ст. 347УПК РК); предложения прокурора, направленные на восстановление упущенных сроков для предъявления апелляции (ч. 1 ст. 419УПК РК); запросы, цель которых – изъять материалы уголовного дела для возможности внесения новых ходатайств (ст. 486УПК РК);

а также прошения о пересмотре судебных постановлений, которые уже вступили в силу (ч. 1 ст. 488УПК РК). Данные электронные документы удостоверяются с помощью электронной подписи, что делает их юридически значимыми в рамках законодательства Республики Казахстан.

Электронные документы, подтверждающие определенные факты, могут принимать различные формы, в том числе заключения экспертов (ч. 1 ст.283 УПК Республики Казахстан) и специалистов (ст. 117 УПК РК). Субъектами, имеющими полномочия на предоставление подобных сведений для включения в материалы уголовного дела, являются ряд лиц: подозреваемые, обвиняемые, защитники, а также частные обвинители, потерпевшие, гражданские истицы и ответчики, наряду со своими представителями, как-то же самое относится и ко всем гражданам и организациям (ч. 4 ст.122 УПК Республики Казахстан). В равной мере и защитник, и представитель потерпевшего имеют юридическое право на проведение допросов свидетелей, вероятно обладающих релевантной информацией касательно рассматриваемого преступления, с использованием технических устройств. Записи такого допроса, выполненные с помощью вышеупомянутых средств, могут быть зафиксированы на электронных носителях, которые последующим образом прикрепляются к материалам конкретного уголовного дела в качестве доказательственной базы (как указывается в п. 5 ч. 3ст.122 УПК Республики Казахстан)[18].

Первоначальное описание электронного разбирательства дел преступного характера в уголовном процессуальном кодексе Республики Казахстан было крайне обобщенным, лишь устанавливая основы для создания и хранения некоторых видов судебных бумаг и свидетельских показаний в цифровой форме. Отсутствие детализированных инструкций по данным вопросам дополняется предоставлением Генеральному прокурору страны полноты власти по изданию правовых актов с обязательной юридической силой для всех подразделений, преследующих уголовные проступки, что касается использования цифровых технологий и обработки информации в рамках

судопроизводства (ч. 6 ст. 58УПК РК). Однако значительный шаг к упорядочиванию указанных процедур был сделан с введением в действие Инструкции о ведении уголовного судопроизводства в электронном формате (в дальнейшем упоминаемого как «Инструкция»)[5].

В дискурсе о цифровом судопроизводстве Республики Казахстан выделяется информационная система «Единый реестр досудебных расследований»(ИС ЕРДР)[67], обладающая специализированными модулями. Среди ключевых инноваций данной платформы - модуль «Электронное уголовное дело»(е-УД), задача которого заключается в облегчении процесса коммуникации, организации и хранения электронной документации, связанной с уголовными делами. Отличительной особенностью ИС ЕРДР является сервис «SMS-оповещение», который обеспечивает рассылкуоповещений разнообразным участникам уголовного процесса посредством мобильной связи или электронной корреспонденции. Больше того, функция «Публичный сектор»предоставляет уникальную возможность удаленного доступа к судебным материалам, подачи процессуальных документов, жалоб и ходатайств. Напротив, при недоступности удаленного взаимодействия с ИС ЕРДР, вовлеченные стороны могут ознакомиться с материалами уголовного дела непосредственно через воспроизведение документов лицом, курирующим процесс, с последующей возможностью получить их электронные версии (п. 26 Инструкции)[21].

Представителям органов, осуществляющих досудебное расследование, предоставляется возможность пользования электронной информационной системой ЕРДР для ведения дел с уголовно-правовой направленностью. Реализация доступа к модулю электронного документооборота уголовных дел, находящихся в процессе расследования, обеспечивается для каждого участника следственных и оперативных групп. Уполномоченное лицо при обращении к ИС ЕРДР должно пройти этапы подтверждения своей законной идентичности. Данный процесс включает в себя три основных метода: использование

уникальной электронной цифровой подписи, разработанной национальными удостоверяющими структурами Казахстана; применение индивидуального идентификационного номера, выделенного правительственным органом, ответственным за статистические данные в области учетов и правовой статистики; а также привлечение биометрических данных с помощью специализированного устройства считывания. Эти меры прописаны в девятом разделе соответствующей Инструкции и являются неотъемлемой частью авторизации и аутентификации для предоставления надлежащего уровня информационной безопасности и контроля доступа в рамках процедур предварительного следствия (п. 31 Инструкции)[17].

При активации процедуры уголовного производства, средства информационных систем Единого реестра досудебных расследований неминуемо выполняют генерацию первоначальных электронных записей. Среди этого портфеля документов – доклад о регистрации криминального участия (КУИ), отчет о выявлении фактов, указывающих на криминальные действия, а также извещение представителя прокуратуры о том, что досудебное следствие инициировано. Система автоматически интегрирует эти рапорты в состав электронного досье на уголовное дело, предполагая выбор за электронным вариантом ведения, с последовательной регистрацией в каталоге уголовного дела, что упрощает организацию и доступность информации о преступлениях (п. 11 Инструкции). В рамках функционала Информационной Системы Единого Реестра Досудебных Расследований заложена функция автоматической генерации официальных обращений, направляемых в Прокуратуру и органы судебной власти[41].

Лицом, ведущим досудебное расследование, определяется цифровая модальность документооборота уголовного дела, что оформляется в мотивированном распоряжении, согласно ч. 2ст. 42-1 Уголовно-процессуального Кодекса Республики Казахстан. Осведомление о документе, включающее сведения об уголовном деле, в течении суток поступает к

ведущему надзору прокурору через электронную систему записи дел (е-УД). Идентичным образом, законодательно установленный интервал времени отводится для информирования заинтересованных сторон: подозреваемых, защитников, частных обвинителей, обвиняемых, их законных представителей, а также потерпевших и гражданских истцов вместе с их представителями, гражданских ответчиков. Включение уголовных процессов в электронную форму, исключив бумажные аналоги, становится безальтернативным, за исключением обстоятельств, связанных с объединением различных дел (п. 10 Инструкции).

В рамках уголовного процесса лицо, выполняющее процедурные задачи, реализует процесс создания электронных документов, утилизируя предварительно разработанные формы, интегрированные в информационную систему ЕРДР. Процедура аутентификации записей, сформированных в цифровом эквиваленте, довлеет на участниках, что достигается подтверждением подлинности с помощью присвоения электронной подписи с использованием специализированных устройств для фиксации подписей или же электронных механизмов соответствующей сертификации (п. 12 Инструкции).

В ответ на резолюцию о переводе документации уголовного процесса в цифровую сферу, все изначально бумажные акты, относящиеся к делу, подлежат конвертации в цифровые копии формата PDF. Эта операция должна осуществляться без промедления, в течение суток от момента вынесения соответствующего постановления о переходе на электронное судопроизводство. Такие цифровые версии документов интегрируются в структуру электронного уголовного дела, гарантируя их доступность для последующего юридического рассмотрения (п. 11, 14, 16 Инструкции). Документация, первоначально созданная на бумажных носителях и затем трансформированная в цифровой облик, нахождение которой осуществляется в рамках учреждений, отвечающих за преследование правонарушений, подлежит передаче в инстанции государственного обвинения либо предъявлению в

судебные органы, где она становится составной частью электронного уголовного процесса (п. 6 Инструкции). Диспозиция материалов, внедряемая в модуль электронного документооборота для уголовных производств (е-УД), предполагает их интеграцию посредством закрепляющих действий ответственного субъекта, осуществляющего репрессивную деятельность (п. 13 Инструкции). В системе единого реестра дознаний непрерывно происходит процесс заполнения существенных информационных учетных материалов; кроме того, обеспечивается цифровая связность меж профессионалами в области экспертизы, квалифицированными сотрудниками и органами правосудия(п. 5 Инструкции)[41].

В исключительных случаях, когда стремление к управлению процессами судопроизводства в виртуальной среде оказывается невозможным, допускается существенная трансформация Уголовно-процессуального кодекса Республики Казахстан из электронной формы в документацию, исписанную на бумаге (ч. 2 ст. 42-1 УПК РК). В соответствии с двадцать вторым пунктом инструкции, регулирующей детали цифровизированного управления уголовными процессами, устанавливаются условия для временного отклонения от применения электронной системы документооборота. Лишь после истекания суточного промежутка от начала вынужденной или экстремальной ситуации, например, как прерывание энергоснабжения, обрыв связи или невозможность доступа к электронному делопроизводству, предписывается возможность перехода к использованию бумажных документов. Отставляя сторону указанную временную рамку, срочное осуществление действий, описанных следствием или установленных процессуальным порядком по уголовным кейсам, разрешает перевод документации в аналоговый формат без ожидания указанного периода[33].

В некоторых обстоятельствах, определенных государственной Инструкцией, передача содержимого уголовного процесса, зафиксированного в электронных системах, на бумажные носители становится обязательным

условием. Одним из таких случаев является необходимость отправки данных по уголовному делу за пределы данной юрисдикции с целью дальнейшего преследования подозреваемого. Обязательство фиксации информации на бумаге также возникает, когда в деле фигурируют сведения, являющиеся государственной тайной или информацией, охраняемой законом от обнародования. Помимо выше указанных ситуаций, процедура может быть инициирована в случае, когда расследующий орган решает о слиянии нескольких дел в одно по собственному усмотрению, как оговорено в соответствующем разделе упомянутой Инструкции.

В информационной системе «ЕРДР»фиксируется объективное решение о трансформации формата уголовного досье - из цифровой основы в физическую форму записи. Процесс начинается с заполнения специфичной аннотации, аргументирующей переход, и регистрации заявки на смену формата. Следующим этапом является оперативное, но в рамках положенного времени, которое зафиксировано как не более одних суток, преобразование данной цифровой информации в печатные экземпляры судебных материалов. Действующий порядок требует также замены уже интегрированных электронных версий файлов в формате PDF. Они должны быть вытребованы в оригинальной бумажной форме из архивов, где они до этого хранились (п. 23 Инструкции)[19].

В случае резолюции, принимаемой уполномоченным органом касательно объединения нескольких уголовных эпизодов, срочное воплощение данного решения в единый электронный документ в системе е-УД осуществляется в течение временного промежутка, не превышающего одни сутки. Это установление становится актуальным, когда собрание информации происходит в электростатическом формате. В обстоятельствах, когда архивация отдельных компонентов объединяемой информации ранее осуществлялась с использованием бумажных носителей, тот же арбитр, что ведает судопроизводством, в момент принятия упомянутого решения исследует случай

и принимает вердикт относительно предпочтительной формы хранения совмещенных материалов. Согласно директиве, указанной в пункте 17 Инструкции, такое сохранение может обретать как физическую, так и цифровую материализацию[7].

При переходе к цифровому управлению уголовным судопроизводством, при слиянии дел, уже ведущихся в традиционной бумажной манифестации, существует срочное требование по интеграции документации в цифровую систему. Этот процесс включает трансформацию документов в формат PDF для включения в электронное уголовное дело с последующим обновлением базы данных модуля е-УД, отражающим выполненную конвертацию формата. Временной предел для данной операции строго регламентирован и составляет не более 24 часов после ратификации соответствующего постановления. Обратный процесс – возвращение к бумажному ведению после цифрового управления – также требует немедленности в действиях, предписывая окончание трансформации в аналогичный промежуток времени. Переходное управление документацией обеспечивает сохранение законности и последовательности процессуальных действий в рамках судебной практики (п. 17 Инструкции)[46].

Выделение уголовного дела в отдельное производство осуществляется в модуле е-УД путем выделения материалов дела с присвоением отдельного номера ЕРДР (п. 18 Инструкции). В случае прерывания сроков досудебного расследования в порядке ст. 45 УПК РК, в модуле е-УД лицу, ведущему уголовный процесс, ограничивается доступ на совершение процессуальных и иных действий в рамках электронного уголовного дела, кроме тех, которые предусмотрены УПК РК (п. 19 Инструкции). Осуществив изучение принятого процессуального решения по электронному уголовному делу на предмет его законности, прокурор дает добро на следующий этап: архивное хранение дела. Это действие происходит электронным способом, с применением специализированного модуля е-УД, который автоматически сохраняет данные

и присваивает нужный статус закрытому производству. Этот процесс идет последовательно за решением уголовно-процессуального органа о прекращении дальнейшей работы над делом (п. 20 Инструкции). Решение о передаче электронного уголовного дела по подследственности делает недоступным (неактивным) данное уголовное дело для передающего органа (п. 23 Инструкции)[40].

Осуществление контроля за правовой чистотой процессуальных актов, их верификацию, санкционирование, а также пересылку электронных материалов уголовного дела для рассмотрения в судебной инстанции, осуществляет прокурор, находящийся в положении наблюдателя. Реализация этих функций возможна благодаря информационной системе ЕРДР, позволяющей ему получать актуализированные данные о принятых мерах в контексте рассматриваемой криминальной ситуации. Это приводит к обеспечению прозрачности и законности на всех этапах уголовно-правового разбирательства (п. 27–29 Инструкции)[32].

Вопросы, касающиеся процессуальных норм электронного ведения уголовных дел, в судебной практике Республики Казахстан отнюдь не нашли своего исчерпывающего отражения в существующем законодательстве. В ходе анализа данного законодательства выявлены недочеты, связанные с ограниченным обхватом процедурных аспектов. В частности, закон определяет, что при ситуациях, выходящих за рамки стандартного процесса - будь то нештатные обстоятельства или экстренные случаи - предписывается переход от цифровой структуры к традиционному бумажному варианту уголовного досье в течение двадцати четырех часов. Такой перечень мероприятий призван минимизировать преждевременное отступление от использования электронной системы документооборота, исключая ситуации, требующие немедленных действий. Следует отметить, что несмотря на определенные пробелы в регулировании, судебная практика в Казахстане включает в себя расследование и рассмотрение документации, подготовленной в электронном виде.

Рассмотрение аналогичных нормативных решений, которые уже применяются в законодательстве соседних стран, указывает на потенциал для усовершенствования местного законодательства, учитывая зависимость успешной юридической интеграции электронных уголовных дел от полноты охвата процессуальных вопросов (п. 22 Инструкции). Существует законодательное положение, предусматривающее обязательную трансформацию уголовного производства в бумажный вид без права последующих корректировок в ситуациях, когда появляется необходимость проведения следственных операций или действий, связанных с юридическим процессом, и это сопровождается технологическими неполадками[33].

К проведению следственных действий в рамках электронного ведения уголовного дела обозначены определенные игнорируемые проблемы. Отсутствуют четкие инструкции относительно присоединения бумажных доказательственных материалов защитниками и другими участниками производства, несмотря на актуализацию дела в электронной форме. К тому же, всё ещё неясны каноны, касающиеся критериев качества цифровизации документов, таких как разрешение сканированных копий, обязательные атрибуты файлов, а также ограничения размера. Путаница усугубляется неопределённостью в отношении допустимости применения бумажного формата документирования в ситуациях, где технические условия предотвращают ведение электронной регистрации, включая повторный осмотр места дела или допросы на местности. Нормативно не установлено, разрешено ли в этих условиях обходиться без перевода всего процессуального образа ведения дела на бумагу.

Проблематика своевременности следственных и процессуальных операций, а также вопросы, связанные со сроками содержания подозреваемых под стражей в контексте потенциальных проблем с доступностью электронных материалов уголовных дел, вызывает особую озабоченность. В частности, возникают существенные опасения по поводу длительных (более 24 ч) сбоев

информационной системы ЕРДР, а равно и иных чрезвычайных обстоятельств, усложняющих или делающих невозможным получение распечатанных экземпляров документов. Налицо неразрешенная проблема, связанная с продолжительностью предварительного расследования, поддержанием законности задержаний и оформлением необходимых юридических процедур в условиях, когда вся документация по делу находится исключительно в электронном виде и ее физическое воспроизведение ограничено техническими неполадками[23].

Постоянное обновление информационных технологий сопровождается сложностями в долгосрочном хранении уголовных документов в цифровой перспективе. Эволюция носителей цифровых данных, бесспорно, представляет собой двоякий процесс. Старые версии программ и устройств для чтения информации, ушедшие в небытие, не позволяют без дополнительных усилий воссоздать текстовый материал, зарегистрированный на электронных носителях десятилетнюю давность. Спустя два десятилетия, нам необходимы специализированные программы и оборудование, вроде приводов флоппи-дисков, для извлечения данных. Это выдвигает на первый план задачу разработки особых подходов к долговременной архивации результатов уголовных разбирательств, сохраняемых в цифровом эквиваленте.

Введение интеграции электронной документации в области уголовного судопроизводства, включая стадию предварительного расследования, представляет собой вызов, требующий детальной ревизии и расширения действующего законодательного корпуса по уголовному процессу. Рассмотрение уголовных дел в электронном формате подразумевает, в свою очередь, создание методик эффективного получения, систематизации и сохранения электронных доказательств. В контексте электронных уголовных процессов, лица, владеющие электронной цифровой подписью, получат возможность мгновенно оформлять необходимые документы и обмениваться ими с правоохранительными органами, тем самым оптимизируя траты времени

и ресурсов. Однако лицам, лишенным подобной технологии, останется преданность устоявшимся процедурам ведения уголовных процессов. Образец правовых норм и практики ведения дел в электронном качестве, демонстрируемый иностранными юрисдикциями, должен быть принят в расчет при эволюции отечественной законодательной базы, дабы обеспечить прогрессивное и функциональное судопроизводство.

Полагаем, что принципами построения судебного облака для судов должны выступить:

–свободный доступ резидентам облачного хранилища данных;

–гарантия цифровой защиты информации от третьих лиц;

–резервное копирование (backupcopy) данных облака;

–размещение data-центров на территории РеспубликиКазахстан;

–наличие альтернативного программного обеспечения для управления облачной инфраструктурой.

Применительно к форме цифровой информации, хранящейся в электронном виде, полагаем возможным размещать в судебном облаке два вида документов:

– электронный документ (подписанный электронной подписью);

–скан-образ письменного документа.

В контексте управления информационными массивами, особенно в юридической сфере Республики Казахстан, актуально становится применение комплексов автоматизации для судопроизводства. Специально разработанные программно-технические решения облегчают работу судов, упорядочивая и закрепляя результаты процессуальных действий, осуществляемых как самим судом, так и иными участниками, в электронном формате. Эти системы, упрощая документооборот, неизбежно затрагивают и вопросы комплектования архивов. Как результат, архивное хозяйство и пополнение его новыми цифровыми записями требует глубоко продуманной стратегии. Важно заботиться о том, чтобы данные процессы соответствовали множеству

критериев, которые включают в себя регулирование временных рамок хранения документации, оценку их правовой значимости и учет различных уровней доступа к конфиденциальной информации.

Состав электронной информации судебного облака, подлежащей на современном этапе хранению в облаке, по нашему мнению, в зависимости от категории информации должен включать в себя следующее разделы:

1) судебные акты и иныедокументы суда:

–решения;

– определения;

– постановления;

– судебные приказы;

– исполнительные листы;

– письма, ответы и запросы;

2) архив суда по отдельным категория дел и журналы учета движения дел:

– дела, рассматриваемые в порядке упрощенного судопроизводства;

– документы, поступившие в суд в электронном виде;

– аудио- и видеозаписи судебных заседаний;

– журналы учета прохождения жалоб и судебных дел по инстанциям;

3) заявления и жалобы:

– иски (заявления);

– апелляционные жалобы;

– кассационные жалобы;

– кассационные и надзорные жалобы в ВС;

– заявления о пересмотре по вновь открывшимся и новым обстоятельствам;

4) документы по делам:

– отзыв на иск (заявление);

– встречный иск;

– заявление о вступлении в дело;

– заявления и ходатайства;

– заявления на компенсацию;

5) банкротство:

– заявление о признании банкротом;

– заявление о признании физического лица банкротом;

– заявление должника о его банкротстве;

– заявление физического лица о его банкротстве;

– требования кредиторов;

– требования кредиторов к физическому лицу;

– арбитражный управляющий;

– процедуры банкротства;

– иные и произвольные документы.

В целях обеспечения безопасности участников судебного процесса из указанных актов исключают персональные данные:

а) фамилии, имена и отчества участников судебного процесса;

б) дата и место рождения, место жительства или пребывания, номера телефонов, реквизиты паспорта или иного документа, удостоверяющего личность;

в) идентификационные номера налогоплательщиков –физических лиц, индивидуальных предпринимателей, основные государственные регистрационные номера индивидуальных предпринимателей –участников судебного процесса; страховые номера индивидуального лицевого счета;

г) сведения о месте нахождения земельного участка, здания, сооружения, жилого дома, квартиры, транспортного средства, иные сведения об имуществе и о находящихся в банках или иных кредитных организациях денежных средствах участников судебного процесса, если эти сведения относятся к существу дела[31].

Для анонимности участников в судебных документах обращение к инициалам и псевдонимам превалирует над использованием персональных данных, обеспечивая невозможность их идентификации. С целью защиты конфиденциальной информации в процессе формации судебного информационного хранилища рекомендуется выработка строгих параметров в отношении структуры и сущности документов, предназначенных для загрузки. Учитывая, что доступ к хранилищу могут иметь резиденты, семантическая целостность персональных данных находится под угрозой. Введение искусственного интеллекта обозначается как мероприятие повышенной результативности для обеспечения целостности данных в электронном судебном пространстве. Тем не менее, важно подчеркнуть, что жесткие ограничения в доступе к цифровым данным для судей являются невозможными, поскольку нарушают их профессиональные прерогативы. Несмотря на это, судебная практика обуславливает неизменное правило неразглашения информации, принятой к сведению в процессе исполнения служебных обязательств, что представляет собой краеугольный камень судейской этики.

Особенности допуска к информации государственной значимости, засекреченной в рамках судебных электронных ресурсов, обуславливают создание дифференцированного доступа. Интеллектуальные системы обязаны выстраивать различные типы электронных копий документации, соизмеримые с уровнем полномочий запросивших лиц. В соответствии с этим, магистратам предначертан обширный доступ к детализированной информации хранящейся в облаке, в отличие от сокращенной версии, доступной тем, кто занимается административной деятельностью судебного учреждения, где данные, позволяющие установить личность, отсутствуют. Этот процесс должен предохранять конфиденциальные данные от непредвиденного обнародования, обеспечивая надежность их сохранения в соответствии с законодательством. Исключение из правил предоставляется документации, содержащей

государственную тайну; их просмотр магистратами возможен после специальной процедуры допуска.

Проведенный анализ позволяет сделать следующие выводы в отношении принципов создания и организации работы «судебного облака»:

1. Создание судебного облака должно основываться на принципах, обеспечивающих информационную безопасность и цифровой суверенитет страны.

2. Местом хранения информации (data-центры) должна быть территория Республики Казахстан.

3. Доступ cloud-резидентам к судебному облаку должен иметь дифференцированный подход к соответствующей цифровой информации.

2.2 Процессуальный порядок обнаружения, осмотра и изъятия информации с облачных систем и дальнейшее ее использование в ходе досудебного расследования

Сегодняшний день отмечен ростом прецедентов, связанных с нарушениями в областях информационной безопасности и IT. Усиление данной тенденции частично вызвано широким внедрением облачных сервисов для архивации данных. Следствие этого – возникновение новых требований к органам, отвечающим за раскрытие и превенцию подобного рода нарушений. В связи с активным прогрессом в данной сфере, препятствием для эффективного разбирательства инцидентов выступает отсутствие всестороннего научного подхода к сбору релевантной информации. Эксперты сталкиваются с серьезными проблемами при попытке извлечения сведений из облачных систем.

Определяемый как технология обработки данных на удалённых серверах, облачные вычисления предоставляют функциональность компьютерных ресурсов в качестве услуги посредством сетевых протоколов. Важным аспектом

такой модели служб является то, что пользовательский доступ не ограничивается исключительно сетью Интернет; возможности включают в себя и приватное подключение через локальные сети, развертываемые на основе Web-технологий. Следует подчеркнуть, что несмотря на широкое распространение наименования «Интернет-сервис», это определение имеет более широкий контекст и не всегда предполагает прямое использование глобальной сети[49].

Современные тренды в архивации информации указывают на устаревание локального хранения данных на физических накопителях, таковых как жесткие диски компьютера. Практика сложилась таким образом, что перенос информации на флеш-карты и подобные устройства уже не считается наиболее рациональным решением. Вместо этого, наблюдается значительный рост популярности использования дистанционных облачных сервисов, где файлы и документы размещаются в отдельных папках доступных через интернет. Преимущество такой системы заключается в удобстве доступа к информации вне зависимости от местоположения пользователя, что обеспечивается чрез вездесущую связь с глобальной сетью и совместимость с разнообразными устройствами. Это дает возможность для оперативного получения нужных данных без привязки к конкретному носителю, тем самым упрощая процесс работы с информацией и повышая ее мобильность и безопасность.

В эпоху цифровизации, в Казахстане активно внедряются облачные сервисы для хранения данных. Повсеместно применяются такие системы, как GoogleDrive, Dropbox, а также SkyDrive и Яндекс.Диск, выделяющиеся своей популярностью. Обеспечение доступа к данным и управление ими в облачном пространстве демонстрируют прогресс современного информационного общества, причем их масштабное использование свидетельствует о широком спектре функциональных способностей этих платформ[50].

В ходе исследований, связанных с анализом факторов и последствий противоправных деяний, актуализируется нужда в сборе и тщательном

рассмотрении данных, размещенных в Интернет-ресурсах облачного типа. Это обусловлено тем, что такие хранилища зачастую содержат ценную информацию, способную пролить свет на обстоятельства совершения правонарушений. Но при исследовании облачных хранилищспециалисты сталкиваются со следующими трудностями:

1. Имеющиеся на сегодняшний день программные продуктыне способны в полной мере извлекать данные из всех облачных хранилищ.

2. Зачастую преступники, пытаясь скрыть информацию о совершенных ими злодеяниях, удаляют данные из облачных хранилищ.

3. Высокая стоимость специализированных программных комплексов, предназначенных для работы с облачными технологиями, зачастую является препятствием при расследовании инцидентов в сфере информационной безопасности.

В области кибернетической безопасности расследование преступлений, связанных с информационными технологиями, представляет собой задачу высокой сложности. Это объясняется многочисленными методами, которые злоумышленники используют для сокрытия следов своих противоправных действий. Важность таких расследований обусловлена стремительным развитием технологий, предлагающих инструменты для быстрого доступа и анализа важной информации. К таким инструментам относятся, к примеру, возможности анализа данных из облачных сервисов, мобильных устройств, карт памяти и СИМ-карт, связанных с предполагаемыми преступлениями[51].

Проблематика безопасности персональных сведений в контексте облачных сервисов вызывает серьезное беспокойство среди экспертов информационной безопасности. Случаи несанкционированного проникновения в системы хранения данных и последующие утечки конфиденциальной информации подтверждают, что защитные механизмы таких технологий оставляют желать лучшего. При этом остро стоит вопрос личной ответственности пользователей за сохранность их идентификационных данных.

Нередко пользователи подвергают данные риску неведомо, так как мало осведомлены о синхронизации своих устройств с облачными сервисами. Такое недопонимание усугубляется недостаточным пониманием процессов, связанных с обеспечением информационной безопасности облачных хранилищ, и допустимым кругом лиц, имеющих доступ к личным сведениям пользователей[52].

В ведомстве внутренних дел Республики Казахстан функционирует высокоспециализированный аналитический комплекс для анализа действий в сфере облачных технологий. Разработанный ради оперативного выявления и исследований инцидентов в домене информационной защиты, данный инструментарий позволяет экспертам добывать и анализировать данные авторизации пользователей облачных ресурсов. В процессе детекции преступных деяний, совершаемых при использовании виртуальных хранилищ данных, специалисты применяют методы, традиционные для проведения компьютерных судебных экспертиз. Это дает возможность подобрать эффективный подход к каждому конкретному случаю нарушения кибербезопасности[53].

Специализированные познания являются ключевыми для корректного извлечения информационных массивов, расположенных в серверных ресурсах, работающих на принципах облачных технологий. Данные, размещенные в таком типе хранилищ, находятся на значительном удалении от конечного пользователя, привнося дополнительные трудности в процедуру их восстановления для последующего изучения и анализа. Для реализации оперативного разоблачения событий, требующих срочного вмешательства или выяснения фактов, предполагаемых на начальном этапе расследования, актуальным становится оперативный доступ к информации, сконцентрированной в облачных хранилищах. С успехом проведенный процесс анализа информационных облаков может стать краеугольным в верификации иллюзорных предположений или их эффективном опровержении.Доступ к

информации, размещенной в облаке, представляет значительную сложность, ибо требует верификации личности пользователя через ввод идентификационных данных – имени и кода доступа. Далее, для того чтобы добиться передачи содержимого из облачного хранилища, необходимо подтверждение прав на получение информации, что позволяет создать полный клон данных.

Путём использования модуля OxygenForensicExtractorforClouds[79]программа «Мобильный Криминалист»предоставляет возможность подключения к облачным хранилищам. Осуществляется этот процесс посредством авторизационных данных - электронной почты и пароля, принадлежащих учётной записи. Инициируется просмотр информационных массивов сразу после успешной аутентификации. Инструмент высокой эффективности не ограничивается простым добычей сведений, но преобразует их в формат, благоприятный для всестороннего изучения, что существенно повышает оперативность работы аналитических экспертов. Важно подчеркнуть, что без деталей доступа, предоставляемых «Мобильным криминалистом», проникновение в глубины хранимой информации затруднено, ибо даже после входа, значительная часть данных остается неизведанной для неавторизованных лиц[68].

Возможно, не все держатели девайсов с операционной системой Android осведомлены о том, что,инициируя активную сессию в приложениях, принадлежащих корпорации Google, таких как PlayMarket и Gmail, они невольно предоставляют этим сервисам разрешение на сбор своих геолокационных данных. Такая информация, отображающая геопозиционирование пользователя, систематизирована в форме, подходящей для интеграции в географические информационные системы. Сбор геоданных является ключевым элементом для корректной функциональности сервисов Google, способствующим оптимизации процессов поиска в Google Картах и

таргетирования рекламных объявлений, с которыми пользователь сталкивается, взаимодействуя как с продуктами Google, так и с внешними веб-ресурсами.

В эпоху широкого распространения мобильных технологий становится принципиально значимым беспрерывное обновление сведений о положении таких устройств. Действительно, зафиксировать перемещение гаджетов можно как при их непосредственном перемещении пешком, так и в процессе поездок на автомобильном транспорте. Интересно, что частота и актуальность этих обновлений варьируются в зависимости от скоростных характеристик передвижения и от величины заряда батарей устройств.

Интеграция браузера GoogleChrome, предпочтительно используемого на стационарных компьютерах, с облачными сервисами способствует без проблемному доступу к маршрутным данным. Это происходит благодаря синхронизированному соединению, которое упрощает получение как личной информации из аккаунтов Google, так и последовательности записей о перемещениях пользователя. Согласованное хранение локационных деталей в облачных хранилищах, при условии активации синхронизации, формирует комплексный набор данных, анализ которого на первый взгляд кажется затруднительным. Впрочем, инновационные программные решения позволяют не только извлекать такие данные, но и проводить их всестороннюю обработку для дальнейших прикладных задач[54].

В области информационной безопасности наблюдается непрерывное развитие методов исследования данных в облачных хранилищах. Знатоки, стремящиеся к эффективному анализу данных, хранящихся в облаке, вынуждены не только глубоко осмысливать существующие методологии, но и уделять значительные ресурсы времени на непрерывное освоение их сложностей. Соединение проверенных аналитических подходов с инновационными практиками является ключом к тому, чтобы углублять понимание информации в облачных сервисах, что имеет решающее значение для расследования нарушений в информационном пространстве.

Не отстаёт и сам процесс усовершенствования самих способов хранения данных в облаках, требуя от экспертов непрерывно развивать и адаптировать инструменты для извлечения и анализа информации. К сожалению, примечательно отсутствие безвозмездных, специально разработанных инструментов, а имеющиеся требуют регулярного обновления, чтобы отвечать постоянно меняющимся требованиям к безопасности.Параллельно, политическая среда постоянно модифицирует законодательную базу, стараясь сбалансировать права коммерческих структур и обеспечивать соответствие деятельности представителей бизнеса законам. Такой динамичный равновесный процесс вносит свои коррективы в рабочие реалии специалистов информационной безопасности[55].

В рамках уголовного процесса в Казахстане, который формируется на основе континентальной судебной системы, наблюдается проникновение атрибутов англо-саксонской модели, покрывающей как досудебное расследование, так и разбирательство дел в суде. Процедура обыска и изъятия в соответствии с первой частью 254 статьи УПК РК выполняется лицом, отвечающим за досудебные следственные действия, на основании аргументированного решения. Отметим, что в сфере правового регулирования четко установлено, что решение о проведении указанных операций, как и в случае с документами, содержащими секретные государственные материалы или другую юридически охраняемую информацию, обязано получить одобрение судебного следователя. Это предусматривает, на основании явного толкования установленной нормы, одобрение не самого процесса расследования, а именно решения о его проведении. Кроме этого, пункт 39 статьи 7 УПК устанавливает, что санкцией выступает юридическое допущение судебной инстанции, направленное на осуществление процессуальных действий органами уголовного преследования на этапе досудебного разбирательства.

Определение и разрешение на реализацию процедур, включая обыск и выемку, заключается не только в одобрении актов следователя, но и в более широком контексте процессуальных действий. Согласно первый раздел статьи 55 Уголовно-процессуального кодекса Республики Казахстан (УПК РК), роль следственного судьи не ограничивается одобрением, а распространяется на полномасштабную оценку и разрешение по вопросам, касающимся обыска и выемки, а также других сопутствующих проверок. В дополнение к этому, лицо, ведущее предварительное расследование, наделено, как указано в первой части статьи 254 УПК РК, уникальным и независимым от остальных участников уголовного процесса полномочием выносить решения о начале таких процедур как обыск и выемка. Это одобрение процессуальных шагов устанавливает особое разделение полномочий в рамках правовой системы и подчеркивает важность тщательно выверенных и санкционированных действий в рамках судопроизводства[56].

Санкционирование досудебных процедур, таких как осмотр и выемка жилых помещений, представляет собой сложную правовую задачу, пронизанную нюансами и подводными течениями, которые влияют на конституционные права граждан. Осуществляя осмотр жилища, пристальное внимание уделяется положениям п. 13 ст. 220 Уголовно-процессуального кодекса Республики Казахстан. Этот норматив акцентирует, что осмотр опосредуется лишь после получения одобрения от находящихся там совершеннолетних или в результате получения санкции от следственного судьи. Если жильцы несовершеннолетние, страдают психическими заболеваниями или решительно противятся осмотру, требуется решение о принудительности данной процедуры, обязательно подлежащее узакониванию со стороны судебного органа. Отказ в выдаче санкции судьей делает осмотр неосуществимым.

Вопиющая проблематика регламентации срочных судебных постановлений стоит на перекрёстке законности и эффективности

правоохранительной деятельности. Так, при поступлении ходатайства о разрешении на производство вышеупомянутых действий, незамедлительное его рассмотрение обретает приоритетную степень важности. Тем не менее, следственные судьи нередко сталкиваются с коллизиями, когда у них имеются уже назначенные или текущие дела. Процессуальные кодексы предписывают судье в таких ситуациях объявить перерыв в судебном процессе или отложить рассмотрение других дел. Это, без сомнения, влечёт за собой пересмотр установленных порядков в работе суда, создавая тем самым дополнительные барьеры как для уже приступивших к своему заседанию субъектов, так и для тех, кто еще только ожидает вызова на судебное разбирательство[57].

Регламентировать такие моменты следует с оглядкой на защиту индивидуальных свобод каждого участника процесса, и в этом свете требуется поиск баланса между срочностью и справедливостью. Нелегкая, эта задача порождает дилеммы, решение которых предполагает детальное переосмысление традиционных подходов к управлению судебными ресурсами и рассмотрению ходатайств.

В свете недавних модификаций законодательных актов, когда случается инцидент в приватном жилище и неотложность оценки ситуации не допускает промедления, процедура его осмотра может осуществляться по решению лица, занимающегося предварительным расследованием. Данный чиновник обязан в пределах суток отправить соответствующие документы прокурору. Прокурор, в свою очередь, должен без замедлений рассмотреть полученные материалы и направить их на дальнейшее рассмотрение следственному судье, который осуществит тщательную проверку на предмет законности действий. В обстоятельствах, когда выявляется, что инспекция помещения проведена с нарушениями юридических норм, прокурор приостанавливает передачу материалов и издает аргументированное решение об их неправомерности.

Следовательно, с учётом текущего положения законов, введена необходимость верификации законности выполнения осмотров, обысков и

изъятий документов, содержащих сведения, классифицированные как государственная тайна или другие сведения, подлежащие защите по закону, проверяемых надзорным судьёй без предварительного судебного разрешения.

Осуществление осмотра, обыска или изъятия, подвергает себя строгой правовой процедуре. Проверка соблюдения законности данных действий возложена на институт следственного суда. В случаях, когда по результатам детального рассмотрения, имеющиеся действия признаны неправомерными, постановление следственного судьи об их незаконности присоединяется к доказательственной базе уголовного процесса. Указанное постановление исключает возможность использования результатов противоправных действий в качестве улик. Экспертиза законности является обязательным этапом, гарантирующим адекватность и справедливость судопроизводства[58].

Предоставление разрешений на выполнение процедур следствия, которое находится в ведении органов, занимающихся уголовным преследованием, в числе которых и процесс личного обыска, является одним из направлений компетенции представителей судебной инквизиции. В сфере надлежащего проведения личных обысков сегодняшние правоохранительные реалии указывают на отсутствие остроты в проблематике. Порядок его осуществления, выделяющийся своеобразностью среди других процедур расследования, строго определен нормативными положениями, содержащимися в уголовно-процессуальных кодификациях.

Согласно нормативам статьи 255 Уголовно-процессуального кодекса Республики Казахстан, обладатели полномочий на проведение предварительных следственных действий имеют законное право на выполнение персонального обыска субъекта. Это право активируется с целью выявления объектов или бумаг, которые могут быть скрыты на теле, в одежде или среди принадлежностей лица. Данные действия целенаправленно направляются на обнаружение улик, имеющих ключевое значение для расследования.

При обстоятельствах, не терпящих отлагательства, процедура личного обыска может быть инициирована решением офицера дознания или инквизитора, что предъявляется без отсрочки. Неотложность ситуации оправдывает мгновенное начало процесса, в то время как изначальное уведомление следственного магистрата и последующая передача ему дубликата предписания и отчета по результатам обыска остаются обязательными. Это обеспечивает основу для дальнейшей оценки легальности проведенного обыска, а также адекватности применяемых следственных методов и допустимости доказательств, извлеченных в ходе процедуры[59].

Согласно статье 255 части 2 Уголовно-процессуального кодекса РК, личный обыск лица должен осуществляться лишь инспектором того же пола, что и обыскиваемый, и исключительно при наличии свидетелей и экспертов, не расходящихся по половому признаку. С целью уточнения данной нормы, предлагается внести ясность в законодательство: такие мероприятия надлежит проводить при условии, что обыск подразумевает обнажение лица. В сценариях, где осуществляется проверка личных вещей без нарушения интимной сферы, пол исполнителя роли обыскивающего не является критичным аспектом.

Дополнительно рекомендуется закрепить процессуальную процедуру выдачи лицу, подвергаемому обыску, копии решения о проведении данной процедуры, в том числе ордера судьи. Таковая мера позволила бы не только обеспечить защиту конституционных прав человека, но и открыла бы путь к апелляции постановления дознавателя по данной инспекции. Существующие положения УПК, предоставляющие возможность затребовать документы, являются не столько задолженностью следователя, сколько правом обвиняемого. Актуальное положение дел в сфере предоставления доказательственных бумаг сейчас полностью зависит от дискреционных полномочий органа следствия[60].

Объёмы цифровых архивов в планшетах системах увеличиваются. В них отыскиваются не только персональные и бизнес-документы, но также фото, видеозаписи и аудиоматериалы. Упомянутые данные нередко содействуют раскрытию правонарушений, подлежащих уголовному преследованию, облегчая труд следственных органов. Дополнительно, отдельным лицами организациям доступно размещение значительных объёмов информации на мощных серверах облачных сервисов, которые централизованно обрабатывают и хранят цифровые массивы.

Исследование облачных сервисов и анализ данных, которые они содержат, сталкиваются с рядом затруднений. В числе препятствий для эффективного анализа данных, загруженных в облако, стоит выделить несовершенство программного обеспечения, не всегда способного извлекать сведения из разнообразных облачных репозиториев. Дополнительные сложности возникают при фиксации попыток злоумышленников стереть жизненно важные данные с целью скрыть следы неправомерных действий. Эти препятствия усугубляются высокой стоимостью специализированных инструментов, предназначенных для работы с данными, хранящимися в облаке, что, в свою очередь, ограничивает возможности проведения полномасштабных расследований в области кибербезопасности.

Изучение инцидентов, связанных с хранением данных в облаке, требует применения специализированных криминалистических подходов. Анализируя облачные сервисы и мобильные аппараты тех, кто причастен к делу, эксперты могут в ограниченные временные рамки извлекать актуальные данные. Подобные исследования нацелены на оперативное определение нарушений закона с использованием современных технологий хранения информации (онлайн). Экспертная работа, включающая в себя криминалистический инструментарий, находит ключевые сведения, способствующие раскрытию преступлений.

Изощренный инструментарий UFED предлагает специалистам глубинные аналитические возможности, предоставляя им функционал по изъятию и сохранению конфиденциальных данных, расположенных в цифровых социальных пространствах как Instagram, Twitter и Facebook, равно как из облачных хранилищ файлов и иного контента. Гарантируя соответствие своевременности запросам расследования, такой инструмент обеспечивает продуктивное слияние и структурирование обширных масс данных, трансформированных в систематизированный вид, что становится значительным шагом для последующей детальной интерпретации. Дополнительно, UFED способен координировать передачу информации, улучшая целостность данных и облегчая их внедрение в более широкие аналитические процессы[61].

С целью анализа цифровой информации, «Мобильный Криминалист», выступая в качестве технико-криминалистического инструмента, предназначен для экстракции данных из сетевых хранилищ. Находя доступ к облачным сервисам, программа требует аутентификационные данные, изъятые из мобильных аппаратов, а именно пароли или токены. Образцы таковых, сохранённые внутри аппаратов, обнаруживаются и декодируются автономно, благодаря встроенным алгоритмам «Мобильного Криминалиста». Наряду с устройствами на базе Android и iOS, в сферу его действия попадают также те, что функционируют под контролем WindowsPhone.

Следует подчеркнуть, процесс подключения программа инициирует при первом же обнаружении сетевых учётных атрибутов и незамедлительно приступает к загрузке данных. Последующий интерфейсный анализ охватывает: обзор данной учетной записи, коллекций изображений и видеозаписей, геоинформацию, кооперируя данные, представляет их в графических и текстовых форматах – от картографических модулей до графов взаимосвязей, временных последовательностей событий и состава объединенных контактных данных.

Неоспоримо, обширные функциональные возможности «Мобильного Криминалиста»облегчают аспекты технического осмотра цифровых улик, предоставляя экспертам мощный инструментарий для извлечения и последующей обработки информационных массивов с целью расследования преступлений.

Локализованные в серверных парках Google и защищенной облачной среде, данные о местоположениях окутаны покровом неприступности в силу закрытости формата их хранения. Синхронизационные процессы меж устройствами и облачными системами усиливают трудности, возникающие перед аналитиками, стремящимися извлечь эти ценные сведения для дальнейшей экспертизы. Вопреки тому, что доступ к подобному роду информации представляет собой формидабельное испытание, программа, оснащенная нужными функциями, обладает потенциалом для извлечения и детального рассмотрения этих данных.

Совершенствование облачных хранилищ непрерывно модифицирует процедуры технико-криминалистического исследования. Утилиты, такие как UFED и «Мобильный Криминалист», предоставляют экспертам основу для скоростного анализа содержимого онлайн-хранилищ. В данном контексте, проницательность, знание и подготовленность специалиста по технической экспертизе являются необходимым условием для успешного извлечения информационных массивов, что, несомненно, тянет за собой значительные затраты времени.

Главный способ фиксации хода и результатов обыска является протоколирование (ст. 256 УПК РК).

В ходе процедуры изъятия имущества, аккуратно фиксируется детальная информация о каждой единице: от количества и меры до серийных номеров и уникальных идентификаторов. Подробная расписка, первостепенно составленная при конфискации обширного набора вещей, производится при подаче протокола, становясь его краеугольным элементом. Записи,

зафиксированные на листах описи, несут в себе ключевые параметры изымаемых предметов: наименование, величину, массу и другие характеристики, а также время и точную локацию их обнаружения.

Для удовлетворения законодательных требований Республики Казахстан, связанных с уголовно-процессуальными процедурами, протоколы и описи ценностей и документов тщательно оформляются в копии. Каждый экземпляр закрепляются подписями лица, проводившего изъятие, а также тех, кто присутствовал при процедуре, включая собственника имущества или официального представителя исполнительной власти.

Отражение в протоколах обыска материальных элементов и информационных сообщений не сопряжено с необходимостью создания сложного аппаратного обмундирования и обладает стойкостью к внесению изъятий, не содержа под собой избыточных данных. В контексте документального оформления, узаконенные экземпляры данных записей и их детализаций доставляются либо лицу, лишённому активов вследствие аннексии, либо его официально уполномоченным агентам, ратифицировавшим упомянутые бюрократические свитки.

Рассмотрим следующие способы фиксации:

–графическая,

–предметная,

–наглядно-образная.

В современной практике оформления обысков на уголовном следствии, фиксация выявленных фактов осуществляется различными способами. Чтобы документировать процесс на обширных территориях с множеством объектов или в отсутствие конкретного адреса данного здания, применяют графическое представление. Ключевое здесь - создание визуального сопровождения для привязки важных объектов и артефактов, отысканных в процессе, к местности, благодаря чему значительно упрощается процесс доказывания в уголовном судопроизводстве[62].

Обнаруженные в ходе обыска объекты, имеющие значимость для расследования, подлежат изъятию и фиксированию по предметной форме. Эта процедура имеет законодательную основу, а именно, часть 16 статьи 254 УПК РК, и в новейших реалиях обыска допускает использование фото и видеофиксации. Легкость доступа и удобство пользования сделали данные способы гораздо предпочтительнее методов стенографии и киносъемки, которые почти полностью утратили своё применение, поскольку не обладают уникальными функциональными характеристиками для фиксации процедуры обыска.

Касательно применения видеозаписи, оно интегрировано в процесс уголовного следствия не случайно - возможность зафиксировать достоверное положение вещей на месте обыска и поведение участников данного процесса является важным элементом. Такая мера диктует следователям необходимость строжайшего соблюдения законодательных актов, дисциплину при проведении следственных мероприятий и заодно стимулирует к поддержанию высокой степени самоконтроля и критическому взгляду на собственные действия.

Фотоносители, фонодокументы, кинохранилища, изображения на прозрачной основе, магнитные видеоносители, конструкторские графики, технологические схемы, архитектурные проекции, а также инсценировки на других медиаформатах являются приложением к документу осмотра или выемки. Людям, занимающимся этими операциями, обязательно необходимо заверить документ своей подписью. Указано будет в оригинале документа, какому лицу была передана копия акта допроса или изъятия, и эта передача легализируется подписью владельца копии[63].

В контексте онлайн-расследований на расстоянии – наше понимание таково: визуализация процесса данной инспекционной процедуры, включая её результаты, обязана записываться на видеоматериал. Затем это следует архивировать с файлами соответствующего уголовного процесса. Подобный подход имеет решающее значение для последующего анализа убедительности,

актуальности и легитимности этой информации, которую суд выносит в качестве вердикта на основе доказательной базы.

Существует мнение, что повышение результативности проведения обысков могло бы быть достигнуто через активное применение научно обоснованных рекомендаций, а также за счет привлечения к процессу квалифицированных экспертов и осуществления видеозаписи процедур, включая те, что происходят на удаленном расстоянии. Основной механизм за документирования этапов и выводов при обыске представляет собой составление аккуратного протокола. Последний обладает способностью надежно фиксировать объекты материального мира и информационные данные, одним из явных его достоинств является устойчивость к искажениям при отсутствии лишних сведений. К тому же такой метод записи не влечет за собой необходимость в создании сложных технических устройств[64].

Рассмотрены особенности проведения обыска и выемки по уголовным делам в сфере экономической деятельности, в частности по уголовным делам о незаконной банковской деятельности.

Установлено, что цель обыска заключается в обнаружении и изъятии документов и предметов, которые имеют значение для расследования уголовного дела.

Прежде всего это документы, выданные Национальным Банком(свидетельства о государственной регистрации организации, лицензии), и внутренние документы организации (различные регламентирующие и управленческие документы, приказы, распоряжения, должностные инструкции, служебные записки).

Также в ходе обыска обнаруживают различное оборудование, используемое для выполнения банковских операций, а также магнитные носители компьютерной информации.

Выемке подлежат документы, подтверждающие факт осуществления лицом незаконной банковской деятельности.

Большое доказательственное значение имеют не только документы самой организации, но и иные документы, находящиеся в органах государственной власти, органах местного самоуправления, учреждениях и организациях.

Традиционные следственные действия, такие как обыск и выемка, должны быть адаптированы к особенностям электронной (цифровой) информации, что приводит к размышлениям о необходимости разработки специальных видов обыска и выемки, таких как обыск (выемка) электронных (цифровых) носителей информации; выемка электронной (цифровой) информации; распоряжение провайдеру, оператору информационной системы, депозитарию о предоставлении информации об операциях с электронными (цифровыми) активами; предоставление удаленного доступа к базам данных (сбор данных в режиме реального времени)[65].

Для следственных и оперативных работников-изучение персонального компьютера преступников, может осуществляться в рамках статьи 220 «общие правила осмотра», 221 «осмотр и хранение вещественных доказательств», 245 «Негласное снятие информации с компьютеров, серверов и других устройств, предназначенных для сбора, обработки, накопления и хранения информации», 252 «обыск», 253 «выемка», 254 «порядок обыска и изъятия»УПК РК, где ПК может быть изъят и проверен экспертамив части технологического контента.

Мы считаем, наиболее эффективным следственным действием при изучении персональных электронных компьютеров является статья 245 УПК Республики Казахстан «Негласное снятие информации с компьютеров, серверов и других устройств, предназначенных для сбора, обработки, накопления и хранения информации».

Однако, на наш взгляд, эти негласные следственные действия достигают определенных пределов, то есть следственные и операционные подразделения могут копировать информацию, хранящуюся в персональных компьютерах, но они не могут отслеживать специальные децентрализованные онлайн-браузеры,

такие как Tor, которые направляют зашифрованные сообщения через несколько серверов, чтобы скрыть местоположение пользователя.

Следующей проблемой является внешнее хранилище данных, поскольку хранилище данных расположено снаружи, на нескольких серверах, часто в других странах, и, естественно, не может быть найдено и рассмотрено как «захваченное»с персонального компьютера.

Даже если личные данные будут удалены из внешнего хранилища, нет никакой гарантии, что это действие было выполнено с персонального компьютера подозреваемого.

Таким образом, внешнее хранение данных уже может быть проблемой в следственной и оперативной практике.

При изучении облачного онлайн-хранилища и данных, которые оно содержит, возникает ряд технических и тактических проблем:

1. Невозможность программного обеспечения извлекать информационные данные из любого облачного хранилища.

2. Удаление данных из облачного хранилища злоумышленниками с целью сокрытия информации о совершенных преступлениях.

3. Значительная цена специализированных программных систем, предназначенных для работы с облачными технологиями, часто является преградой для расследования инцидентов, связанных с информационными технологиями.

«MobileCriminalist»- это программа технических и криминалистических экспертов, которая позволяет извлекать данные из облачного хранилища. Получение информации из облачного хранилища с помощью этой программы потребует глубоких знаний и опыта от специалиста, а также тщательной подготовки и значительного времени.

2.3 Предложения и рекомендации по совершенствованию законодательства с целью использования информации с облачных систем и синхронизации в электронное уголовное дело

Уголовно-процессуальный кодекс Республики Казахстанпредусматривает необходимость сбора доказательств идопроса свидетелей в рамках досудебного расследования уголовныхдел. Современные технологии, такие как облачные системы, могут одержать важную информацию, необходимую для установленияфактов преступлений. – 1 УПК РК.

В соответствии с нормативными актами Республики Казахстан и основополагающим государственным документом – Конституцией, любое раскрытие информации личного характера подлежит строгой регламентации. Несмотря на отсутствие непосредственных отсылок к облачным сервисам в Уголовно-процессуальном кодексе РК, доступ к данным, хранящимся в облаках, предполагает получение специального разрешения судебной инстанции. Этот процесс инкорпорирует в себя положения, касающиеся защиты персональной информации, что неизменно ведет к необходимости соблюдения конфиденциальности, как одного из фундаментальных принципов современного законодательства в сфере персональных данных.

В Российской Федерации законом, регулирующим персональныеданные, является Федеральный закон от 27 июля 2006 года № 152-ФЗ«О персональных данных»[6]. Данный закон содержит статьи, вкоторых упоминаются облачные системы хранения данных.

В размышлениях по поводу защищенности персональной информации, мы обращаемся к положениям федерального закона, принятого в Российской Федерации 27 июля 2006 года под номером 152-ФЗ. Данный законодательный акт, затрагивающий сферу личных данных, предписывает строгие рамки их обработки, настаивая на трех главных принципах: обоснованности использования, соблюдении справедливости и законности. Когда дело касается

использования инфраструктур облачных вычислений для манипуляций с данными, имеющими персональный характер, лежит непреложное требование к организациям – гарантирование надежной охраны информации от какого-либо неподобающего вмешательства. Ясно, что ответственность за безопасность и конфиденциальность личных данных, подпадающих под ведение и хранение, неизменно висит на плечах организаций, способствующих их циркуляции и анализу.

В соответствии с нормативами статьи 18 закона Российской Федерации от27 июля 2006 года под номером 152-ФЗ, оговаривающего темы персональной информации, уточняется, что передача данной информации сторонним институтам предусматривает обязательное получение одобрения от лица, чьи данные подлежат разглашению, за исключением обстоятельств, при которых трансферт необходим для реализации юридических или договорных обязательств. Компании, выбравшие для распределения информации платформы облачного хранения, обязаны применять данное положение. Параллельно, статья 19 того же закона подчёркивает необходимость обеспечивания каналов доступа владельцев данных к собственной информации. Это требование равносторонне касается организаций, эксплуатирующих технологии облачных сервисов для управления данными.

Таким образом, законодательство Российской Федерацииустанавливает требования к обработке, передаче и доступу кперсональным данным в облачных системах хранения данных,обеспечивая защиту персональных данных и права субъектовперсональных данных.

Несмотря на то, что в Казахстане существует закон «Оперсональных данных и их защите»[3], который регулируетобщественные отношения в сфере персональных данных, данный законне содержит нормативных актов, регулирующих облачные хранилищакак таковые. Это может создавать определенные проблемы дляграждан, которые хранят свои данные в облачных системах.

Для решения этой проблемы необходимо внести поправки взаконодательство, которые бы учитывали современные технологии итребования пользователей. Примером может служить опыт зарубежныхстран, где существуют законы, регулирующие облачные хранилища иобеспечивающие защиту персональных данных в таких системах.

Во многих странах, в том числе, и в Казахстане, взаконодательстве отсутствует четкое регулирование «облаков».Законодательство Казахстана не содержит термина «облачные технологии». Однако, концепция «облака»частично предусмотреназаконодательством Казахстана (платформа e-gov).

В целом, использование облачных технологий может привести к:

–трансграничной передаче данных;

–передаче персональных данных;

–использованию«облачных»решений различными пользователями (государственными, частными).

Принимая во внимание, что пользователь «облака»можетпередавать различные виды данных за пределы Казахстана, следуетучитывать положения местного законодательства.

Использование «облачных»технологий в Казахстане следует рассматривать со следующих точек зрения:

–Неприкосновенность персональных данных;

–Частные и государственные конфиденциальные данные;

–Регулирование доменов;

–Отраслевое регулирование: организации финансового сектора, телекоммуникации и государственный сектор.

В рамках нормативных требований Республики Казахстан, хранение данных, относящихся к личной информации граждан, обязано осуществляться в пределах страны, причем данная обязанность ложится как на владельца такой информации, так и на оператора или доверенное лицо, осуществляющее

действия по поручению одного из них, в рамках специализированной базы данных. Тем не менее, Закон предусматривает возможность передачи данных личного характера за границы государства, но с условием, что принимающая сторона обеспечивает надлежащую защиту такой информации. Отдельно следует подчеркнуть, что законодательство не запрещает использование для этих целей информационного пространства за пределами Казахстана, включая технологии облачных вычислений.

Для сравнения, аналогичный закон в Российской Федерации содержит требование, чтобы «сбор, запись, систематизация,аккумулирование, хранение, исправление (обновления, изменения) ивыборка»таких данных осуществлялась в базах данных,расположенных в Российской Федерации. На территории Республики Казахстан базы данных должны исключительно содержать персональные сведения граждан в рамках национального законодательства. В то время как нормативы Российской Федерации возлагают на «операторов» обязанность обеспечивать выполнение аналогичных предписаний, регламентация в Казахстане предполагает прямое указание на локализацию данных в рамках государственных границ. Следует отметить, что российские и казахстанские законодательные нормы разнятся по степени строгости требований относительно обработки персональных данных, что очевидно из сравнения приказов и положений, прописанных в документах каждой из юрисдикций.

В Законе Республики Казахстан от 24 ноября 2015 года «Обинформатизации»[4]используется термин «электронные информационные ресурсы», что в целом подразумевает«данные». В частности, термин «данные»определен как информация,представленная в электронно-цифровой форме и содержащаяся наэлектронном носителе, в интернет ресурсах и(или) в информационнойсистеме.

Согласно Закону, данные подразделяются на следующие типы:

В зависимости от формы собственности:

–государственные;

–негосударственные.

В зависимости от уровня доступности:

–публичные;

–с ограниченным доступом.

В соответствии с законодательством Республики Казахстан, лицо, владеющее данными, имеет полномочия их эксплуатировать, и делись ими, учитывая при этом определённые законными рамками ограничения. Информация, не обременённая доступом с ограничением, свободно может быть предметом трансграничной передачи. В отличие, передача данных конфиденциального характера за пределы государства испытывает ряд препятствий.

Отдельно стоит отметить, что действия в сфере использования инновационных «облачных» технологий и связанных с ними услуг не испытывают подавляющих ограничений ни со стороны публичного, ни со стороны частного сектора, согласно действующему закону. Более того, текущее законодательство не охватывает специфические положения, касающиеся «облачных» технологий, не устанавливает определения таковых и не включает инструкции относительно сбора, обработки, хранения и перемещения разнообразных типов данных в рамках облачных платформ.

Правила регистрации, пользования и распределения доменныхимен в пространстве казахстанского сегмента Интернета разработаны в соответствии с подпунктом 16) статьи 7-1 ЗаконаРеспублики Казахстан от 24 ноября 2015 года «Об информатизации»иопределяют порядок регистрации, пользования и распределениядоменных имен в пространстве казахстанского сегмента Интернета.Требованием к серверному оборудованию регистранта является егофизическое нахождение на территории Республики Казахстан (далее – «Требование»). В регистрации .KZ Домена должно быть отказано если,среди прочего, серверное оборудование, на котором будетиспользоваться интернет-

ресурс с заявляемым доменным именем,находится за пределами Республики Казахстан. Регистрация .KZДомена может быть приостановлена, по такому же основанию, сдальнейшей отменой регистрации .KZ Домена. Согласно официальнойпозиции уполномоченного органа, Требование к .KZ Домену относится ксерверному оборудованию, на котором осуществляется хостинг .KZДомена и не распространяется на серверное оборудование сервисовсвязанных с KZ. Доменом. Таким образом, за исключением «облачных»сервисов предусматривающих хостинг .KZ Домена, Требование не распространяется на остальные «облачные»сервисы (продукты)[66].

Законодательство Казахстана относительно финансовыхорганизаций (банки, страховые компании и прочее) ителекоммуникационных компаний не содержит каких-либо прямыхограничений для таких финансовых организаций ителекоммуникационных компаний по передаче данных и использованию«облаков». К защите конфиденциальной информации и персональныхданных в сфере банковских и телекоммуникационных услугприменяются общие положения по регулированию, хотя непредусмотрены ограничения на использование «облаков». Непредусмотрены ограничения на передачу данных в других отраслях.

На наш взгляд пришло время рассмотреть вопрос о внесении изменений и дополнений в уголовно-процессуальный кодекс Республики Казахстан, с регламентацией «дистанционного (онлайн) обыска» как следственного действия, проводимого в области обработки и передачи цифровой информации, а тактические приемы полученных данных признать допустимыми в доказывании по уголовным делам.

Значимость «дистанционного (онлайн) обыска» трудно переоценить, так как ежегодно на рынок поступают все новые модели, мобильных и цифровых устройств, в которых хранятся массу данных о пользователях и его действиях, которые могут помочь в расследовании сложных преступлений следственным органам.

В связи с чем считаем необходимым рассмотрение вопроса внедрения нового института, такого, как «Удаленный (онлайн) обыск».

В частности, в разделе некоторых понятий, содержащихся в УПК Республики Казахстан ст.7, добавить определение в следующей редакции: «удаленный (онлайн) обыск – действия, проводимое лицом, осуществляющим досудебное расследование для поиска фактических данных правонарушении через интернет, в режиме онлайн доступа к персональному оборудованию подозреваемого».

ЗАКЛЮЧЕНИЕ

В качестве результатов исследования автор приходит к следующим выводам:

1. Наблюдается значительное отличие в национальных законодательных нормах, которые касаются обработки цифровых данных в рамках уголовных разбирательств, даже между государствами с аналогичными юридическими ориентирами. В то время как одни страны регулируют данные средство доказывания посредством устоявшихся норм, другие разрабатывают и внедряют специализированные законодательные акты, относящиеся именно к цифровой информации. Разрешение судебных инстанций оказывается обязательным в случаях, когда в ходе следственных операций затрагиваются основные гражданские права и свободы, связанные с доступом к цифровым данным. В прочих обстоятельствах судебное согласие для использования такой информации может быть не требуемо. Неотъемлемо, что любые выделяемые цифровые улики, будь то физические носители или их копии, подлежат юридической проверке на предмет достоверности. Следует подчеркнуть, что адаптация зарубежного опыта в контексте применения цифровых свидетельств оказывает влияние на прогресс в этой области законодательства о ведении уголовного процесса на родной страной почве, дескать, ныне данный аспект едва замечен в законотворческой практике.

2. С целью гармонизации уголовно-процессуальных норм с динамично развивающимися условиями информационного общества, где осуществляются киберпреступления и проводятся следственные мероприятия, обозначается неотложная потребность не только в модификации существующих следственных процедур, но и в реализации усиленных механизмов, способных обеспечить эффективное розыскное действие, изъятие и фиксацию данных в цифровой форме. Эскалация этой потребности требует немедленного внимания и решительных действий.

Необходимо разработать и ввести в действие протоколы для аккуратного воспроизведения информации из электронных устройств, на которых она была зафиксирована, и последующей передачи этих данных, уже на физических носителях, лицу, обладающему соответствующими правами на изначально конфискованный электронный носитель или располагающему информацией, принадлежащей ему. Важно, чтобы такие действия исполнялись с полным уважением к интеллектуальной собственности и конфиденциальности данных.

Так, копирование информации на электронные носители, как процесс, не может быть свободным от обязательной цедировки данных владельцам, которых необходимо уведомить о перемещении их информации. Новый порядок перехода данных должен также включать меры защиты от неавторизированного доступа в процессе их воспроизведения и передачи. Это обязует к созданию строгих протоколов и мер безопасности, гарантирующих целостность и конфиденциальность переносимой информации на каждом этапе процедуры.

3. Количество информации, складируемой как в персональных электронных устройствах вроде планшетов и компьютеров, так и на централизованных облачных серверах юридических и физических лиц, неизбежно растёт. Данные хранилища заполнены не только критично важными частными и корпоративными файлами, но и могут включать материалы, несущие значимость для установления истины в уголовном судопроизводстве, например, в разыскании злодеяний. Файлы различных форматов – фотографические, видеозаписи и звуковые дорожки, архивированные в облачных системах, уже не раз проливали свет на ход криминальных процессов.

Тем не менее, исследование данных, содержащихся в облачных хранилищах, сталкивается с набором технико-тактических препятствий, а именно: с ограничениями программного взаимодействия, не позволяющими полноценно экстрагировать информационный поток из всех разновидностей

облачных систем; с деятельностью злоумышленников, стремящихся ликвидировать электронные следы содеянных злодеяний путём удаления данных; и, кроме того, с экономической стороны – высоко стоимостноеспециализированное ПОдля эффективной работы с облачными технологиями оказывает весомое давление на бюджеты расследований, затрудняя тем самым раскрытие IT-инцидентов.

4. Исследователи применяют передовые криминалистические технологии для добывания данных из социальных платформ, таких как Facebook, Instagram, Twitter. Такие системы, например, UFED, оснащены возможностями по извлечению и анализу личной информации пользователей, включая контент, размещенный в облачных хранилищах. Развертывание методик, традиционно применяемых для детального осмотра в рамках криминалистического расследования, в сфере облачных технологий, позволяет оперативно получать обширные массивы информации, ключевые для идентификации преступных действий, реализуемых с применением мобильных устройств участников события.

С программой UFED правоохранительные и специальные органы смогут:

- Осуществлять мгновенное извлечение персональных данных пользователя;

- Консолидация и организация разных данных в одной форме;

- Передача и интеграция данных для последующего анализа.

Стоит также отметить мобильный комплекс «мобильный криминалист». «MobileCriminalist»- это программа технических и криминалистических экспертов, которая позволяет извлекать данные из облачного хранилища.

Для подключения к облачной службе программа МК должна использовать пароли или токены, извлеченные с мобильных устройств. После импорта данных из облака их можно просматривать и анализировать в программном интерфейсе МС, включая аналитические разделы:

1. Модуль Карты;

2. Подключение графика;

3. Поток Событий;

4. Контакты комбинированные.

Синхронизацией между мобильным аппаратом и облачной системой хранения данных задается частный формат, в котором локационные сведения обосновываются на серверных мощностях Google. Проблематичность и почти неосуществимость поиска необходимой информации в облачных архивах неукоснительно повышаются ввиду затрудненного извлечения данных. При этом, программы типа UFED и MK, помогающие в обработке онлайн-хранилищ облака и анализе их содержимого, способствуют оперативному проведению криминалистических экспертиз. Важно отметить, что такие операции предполагают не только использование улучшений в инфраструктуре облачных хранилищ, но и потребуют экспертных знаний со стороны исполнителя, тщательной методической подготовки и, возможно, длительного времени для эффективного извлечения и обработки информации.

В заключении можно отметить, что доступ к онлайн-обыску можно провести и в рамках конфискации. Тем не менее, сбор доказательств могут натолкнуться на ограничения, требующие оперативного исследования, например:

- содержимые анонимных записей в онлайн-форумах или чат-сообщениях, как правило, они не такие деревянные, если копии хранятся на сервере системы;

- данные, сохраненные в целевой системе и вновь удаленные лишь на короткое время, восстановлению подлежит при изъятии только в том случае, если удаление произошло «поверхностно»с использованием функций удаления операционной системы;

- если данные из целевой системы передаются и хранятся на внешних серверах и доступ к ним возможен только при наличии сведений о внешней системе и данных доступа;

- если данные передаются по зашифрованным соединениям, традиционные методы обнаружения не позволяют прослушивать учетные данные;

- на мобильных системах, сохраненные данные могут быть лишены изъятию в случае повреждений (например, воде, огне) или, в некоторых устройствах (смартфоны или ПК), при запуске мгновенного удаления;

- при злоупотреблении чужой DSL-соединения или незащищенного беспроводного Интернет-доступа третьих лиц;

5. Инновационная методика – дистанционный обыск – обеспечивает неприкосновенность документов и техники предприятия, что в свою очередь является залогом бесперебойного функционирования организации и гарантией уважения её прав и интересов. Принципиально, применение данной технологии способствует защите законных интересов предпринимателей при рассмотрении экономических споров. В то же время, процедурный контроль прокурора над делами, затрагивающими профессиональную сферу предпринимателя, становится ещё одной стратегией, направленной на обеспечение прозрачности и соблюдение законодательных норм в процессе уголовных расследований.

Данное новшество может найти своё отражение в Инструкции Генерального прокурора об организации надзора за уголовным преследованием в разделе №11 о процессуальном прокуроре.

В сфере кибербезопасности процветание информационной преступности является серьезной угрозой. Данные, официально зафиксированные в регистрах преступлений, не отражают полной картины, поскольку масса инцидентов остается за кадром, ускользая от заметки правоохранительными структурами. Противостояние этому вызову требует от силовиков и спецслужб четкой координации и беспрерывного обмена оперативной информацией, включая международное партнерство, затрагивающее коллег за пределами государства. Текущий уровень правового регулирования деятельности, направленной против информационных правонарушений, отличается несогласованностью и

обрывочностью, часто свидетельствуя о невысокой эффективности и противоречиях нормативных актов. Аналогичное положение дел заметно и в контексте законодательного процесса, где замечена разрозненность в инициативах, направленных на усовершенствование и развитие. Плюс к этому стоит прибавить проблемы в системе правовой статистики, что сказывается на точности отображения реального положения дел.

В сфере регулирования информационных процессов неотложной задачей становится разработка специализированных нормативных актов для охраны критической информационной структуры. Учитывая технологическое развитие, необходимо акцентировать внимание на кардинальное обновление подходов к защите персональных данных, предотвращение информационных нарушений, меняющихся до уголовного преследования. Параллельно, выявляется потребность в глубокой модернизации международных правовых доктрин в домене информационной безопасности и охраны секретности государства для гармонизации с приоритетами национальной безопасности Республики Казахстан. Определение информационного права как собственной юридической отрасли обеспечит последовательное развитие законодательных механизмов в контексте углубляющейся цифровизации общества.

Исследование информационной безопасности и проблематика, связывающая её с уголовной ответственностью в контексте законодательства Республики Казахстан, указывает на актуальность модификации и дополнения существующих уголовных норм. Выявленное отсутствие фундаментальных нормативно-правовых актов, регламентирующих информационные отношения на территории Казахстана, подчёркивает данную юридическую проблему.

6. В следствии вышеизложенного автор исследования считает необходимым внести следующие изменения в действующее законодательство Республики Казахстан:

1. В свете неуклонного расширения сферы цифровых технологий возникает необходимость реформирования уголовно-процессуального кодекса

Республики Казахстан. Соответственно предлагается интегрировать в нормативную базу положения, касающиеся «дистанционного (онлайн) обыска», признавая его законным следственным действием в контексте обработки и передачи цифровой информации. В дополнение к этому, предварительно изученные тактики обработки захваченных цифровых сведений следует утвердить как надежный источник доказательств в уголовном судопроизводстве. Учитывая современные реалии, подобное нововведение является ответной мерой на эволюцию информационной среды и призвано обеспечить эффективность правоприменительной практики.

В связи с чем считаем необходимым рассмотрение вопроса внедрения нового института, такого, как «Удаленный (онлайн) обыск».

В частности, в разделе некоторых понятий, содержащихся в УПК Республики Казахстан ст.3, добавить определение в следующей редакции: «удаленный (онлайн) обыск – действия, проводимое лицом, осуществляющим досудебное расследование для поиска фактических данных правонарушении через интернет, в режиме онлайн доступа к персональному оборудованию подозреваемого».

2. Несмотря на то, что в Казахстане существует закон «О персональных данных и их защите», который регулирует общественные отношения в сфере персональных данных, данный закон не содержит норм права, регулирующих облачные хранилища как таковые. Это может создавать определенные проблемы для граждан, которые хранят свои данные в облачных системах.

В связи с этим автор настоящего исследования считает необходимым ввести в действие Закон «Об облачных хранилищах».

3. В законодательстве Республики Казахстан отсутствует определение термина «Облачное хранилище». Данное определение необходимо внести в указанный выше закон «Об облачных хранилищах» и определить его следующим образом: «Облачное хранилище данных – это модель онлайн-

хранилища, данные в котором хранятся на множественных серверах, распределённых в сети».

4. Также следует говорить о том, что на сегодня в действующем законодательстве Республики Казахстан отсутствуют ограниченияи рекомендациипо использованию «облачных» сервисов и технологий, как на государственном, так и на частном уровне. В связи с этим в предлагаемом нами законе необходимо обозначить ряд ограничений и рекомендация использования облачных хранилищ, таких как:

– запрет распространения ограниченной информации, являющейся государственной или коммерческой тайной;

– регулярное сканирование системы на выявление уязвимостей, а также проведение необходимых работ по повышению безопасности;

– провайдер обязан использовать специальные инструменты для защиты входа и постоянного мониторинга системы;

– обязательным является применение многофакторной аутентификации, а также дополнительных средств защиты облачных сервисов.

Таким образом, внесение указанных изменений в действующее законодательство позволит усовершенствовать правовое регулирование облачных хранилищ в уголовном процессе в Республике Казахстан.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V // [Электронный ресурс] – Режим доступа: https://online.zakon.kz/Document/?doc_id=31575852 (дата обращения: 20.10.2023).

2. Закон Республики Казахстан от 21 декабря 2017 года № 118-VI «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам модернизации процессуальных основ правоохранительной деятельности» // [Электронный ресурс] – Режим доступа: https://online.zakon.kz/Document/?doc_id=35167041 (дата обращения: 20.10.2023).

3. Закон Республики Казахстан от 21 мая 2013 года N 94-V «О персональных данных и их защите» // [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/Z1300000094 (дата обращения: 20.02.2024).

4. Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации» // [Электронный ресурс] – Режим доступа: https://online.zakon.kz/Document/?doc_id=33885902 (дата обращения: 10.02.2024).

5. Приказ Генерального прокурора Республики Казахстан от 3 января 2018 года № 2 «Об утверждении Инструкции о ведении уголовного судопроизводства в электронном формате» // [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/V1800016268 (дата обращения: 20.02.2024).

6. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 06.02.2023) «О персональных данных» // Российская газета. – 29.07.2006. – № 165. – С. 24-25

7. Абдулвалиев А. Ф. Цифровые технологии в уголовном судопроизводстве: настоящее и будущее // Новеллы законодательства криминального цикла и их отражение в уголовно-правовых науках. – 2023. – С. 5-16.

8. Афанасьева С.И., Добровлянина О.В. О Внедрении, развитии, усовершенствовании способов собирания доказательственной информации по уголовным делам // Вестник Пермского университета. Юридические науки. – 2023. – №. 2 (60). – С. 349-377.

9. Воробей С.Н. Проблемы правовой регламентации процессуального порядка изъятия электронных носителей и копирования содержащейся на них информации // Закон и право. – 2020. – № 1. – С. 112- 114.

10. Белкин Р.С., Лифшиц Е.М. Тактика следственных действий. – М.: Новый Юристъ, – 1997. –176 с.

11. Бернам У. Правовая система США. – М.: Новая юстиция, – 2006. – 1216 с.

12. Вехов В.Б. Электронные доказательства: проблемы теории и практики // Правопорядок: история, теория, практика. – 2016. – № 4. – С. 46-50.

13. Гаврилов Б.Я. Роль уголовно-процессуального законодательства в повышении эффективности экспертно-криминалистической деятельности // Криминалистика: наука, практика, опыт: Всероссийская научно-практическая конференция, 23 июня 2022 г.: сборник научных трудов / [сост. И.В. Тишутина]. – М.: Московский университет МВД России имени В.Я. Кикотя– 2022. – С. 25-30.

14. Головчанский А.В. К вопросу о тактике изъятия записей камер видеонаблюдения при расследовании уголовных дел // Вестник Воронежского института МВД России. – 2021. – № 2. – С. 333-339.

15. Дмитриев Е.Г. Котенков А.В. О некоторых вопросах использования информации систем видеонаблюдения в ходе расследования преступлений // Российский следователь. – М.: ООО Издательская группа Юрист, ВНИИ МВД РФ, Московская академия Следственного комитета Российской Федерации. – 2013. – № 1. – С. 5-9.

16. Дудоров Т. Д., Карташов И. И. Дознание как сокращенная форма предварительного расследования: теория и практика. – Воронеж, 2017. – 130 с.

17. Евдокимова В.А. Актуальные проблемы использования современных носителей информации в доказывании // Юридическая наука. – 2020. – №. 9. – С. 76-78.

18. Задорожная В. А. Производство по уголовному делу в электронном формате по законодательству Республики Казахстан // Правопорядок: история, теория, практика. – 2018. – №. 4 (19). – С. 70-75.

19. Зазулин А.И. Использование цифровой информации в доказывании по уголовным делам. Зазулин А.И. М.: Юрлитинформ, – 2019. –168с.

20. Зайцев О.А. Особенности использования электронной информации в качестве доказательств по уголовному делу: сравнительно-правовой анализ зарубежного законодательства // Журнал зарубежного законодательства и сравнительного правоведения. – 2019. – №. 4. – С. 42-57.

21. Исмагилов Р.А., Галимов Э.Э. Информационные технологии, используемые для собирания, проверки и оценки доказательств в уголовном судопроизводстве // Актуальные проблемы государства и общества в области обеспечения прав и свобод человека и гражданина. – 2020. – №. 1. – С. 285-290.

22. Исянаманов И.С. Изъятие и удержание вещественных доказательств по уголовным делам о преступлениях в сфере экономической деятельности должны быть исключены // [Электронный ресурс] – Режим доступа: https://pravorub.ru/articles/80784.html. (дата обращения: 15.10.2023).

23. Казиева А., Шалбаева Ш., Кадырова К. Цифровая трансформация как процесс изменения системы государственного управления в Казахстане // «МЕМЛЕКЕТТІК АУДИТ–ГОСУДАРСТВЕННЫЙ АУДИТ». – 2022. – Т. 56. – №. 3. – С. 47-57.

24. Калугин А.Г. К вопросу о процессуальной форме изъятия предметов и документов в стадии возбуждения уголовного дела // Вестник сибирского юридического института МВД России. – 2017. – № 3 (28). – С. 15-21.

25. Кардашевская М.В. Тактические особенности изъятия криминалистически значимой информации с электронныхносителей // Теория и практика расследования преступлений: материалы X Международной научно-практической конференции 14 апреля 2022 г. – Краснодар: Краснодарский университет МВД России. – 2022. – С. 26-28.

26. Карташов И.И., Лесников О.А. Особенности получения и использования цифровой информации в уголовном судопроизводстве некоторых зарубежных стран // Вестник Воронежского института МВД России. – 2020. – №. 4. – С. 184-191.

27. Количенко А.А. Электронные носители информации как источник получения электронных доказательств в уголовном процессе // Вестник Казанского юридического института МВД России. – 2022. – Т. 13. – №. 1 (47). – С. 114-121.

28. Костяная Ю.С. Информация как объект международно-правовой защиты // Вестник Института законодательства и правовой информации Республики Казахстан. – 2020. – №. 3 (61). – С. 215-227.

29. Кузнецов А.Н. Незаконное изъятие и удержание денежных средств в качестве вещественных доказательств: вопросы возмещения убытков // Судебная власть и уголовный процесс. – 2018. – № 2. – С. 216-221.

30. Кулапов В. Л., Малько А. В. Теория государства и права : учебник. – М., 2009. –776 с.

31. Лаптев В. А., Соловяненко Н. И. «Судебное облако»: правовые вопросы структурирования и защиты данных // Актуальные проблемы российского права. – 2019. – №. 6 (103). – С. 195-204.

32. Лебедева А. А. Цифровые технологии в финансовой сфере (на примере криптовалют): монография. – М.: Проспект, – 2019. – 120 с.

33. Можаева И. П., Шульгин Е. П. О Понимании доказательств в правоохранительной деятельности в эпоху цифровых преобразований // Юристъ-Правоведъ. – 2022. – №. 4 (103). – С. 162-167.

34. Мустафина А.Х. Нормативное регулирование хранения электронных документов в Казахстане // «Генеральный регламент»: 300 лет на службе России: от коллежского делопроизводства до цифровой трансформации управления документами. – 2021. – С. 133-142.

35. Овсянников Д.В. Копирование электронной информации как средство уголовно-процессуального доказывания: авторефдис. … канд. юрид. наук. Екатеринбург, – 2015. – 21 с.

36. Овсянников Д.В. Электронное копирование информации в системах средств уголовно-процессуального доказывания // Правопорядок: история, теория, практика. – 2014. – № 2 (3). – С. 130-135.

37. Оконенко Р. И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации :дис. … канд. юрид. наук. – М., 2016. – 158с.

38. Осипенко А.Л. Особенности расследования сетевых компьютерных преступлений // Российский юридический журнал. – 2010. – № 2 (71).– С. 121-126.

39. Панфилов П.О. О совершенствовании порядка изъятия и приобщения в качестве доказательств предметов и документов по уголовным делам о преступлениях в сфере экономической и предпринимательской деятельности // Общество и право. – 2018. – №2 (64). – С. 105-110.

40. Раджабова У. О. Цифровые доказательства в уголовном судопроизводстве Российской Федерации и зарубежных стран // Правовая грамотность как основа развития гражданского общества. – 2022. – С. 68-75.

41. Рамалданов Х.Х. Понятие и сущность цифровизации доказательств и доказывания в уголовном судопроизводстве // Вестник Волгоградской академии МВД России. – 2022. – №. 1 (60). – С. 121-128.

42. Семенцов В.А. Следственные действия в досудебном производстве: монография. М., – 2017. – 254 с.

43. Стойко Н. Г., Шагинян А. С. Уголовный процесс Англии и Уэльса, Бельгии и Дании: сравнительно-правовой аспект. – Красноярск, – 1997. – 83 с.

44. Телевицкая Ю.А. Правоввое регулирование изъятия электронных носителей информации в уголовном процессе государств-участников СНГ // Проблемы борьбы с преступностью в условиях цифровизации. – 2021. – С. 449 – 452.

45. Фонова Т.П. Гарантии прав гражданина при производстве обыска // Научная перспектива. – 2016. – № 1. – С. 44-46.

46. Цифровое право: учебник (под общ.ред. В.В. Блажеева, М.А. Егоровой). – М.: "Проспект", – 2020. – 640 с.

47. Шошин А.А. Некоторые проблемы определения понятия «Место происшествия» // Сибирские уголовно-процессуальные и криминалистические чтения: материалы Международной научно-практической интернет конференции 16-30 апреля 2012 г. – Иркутск: Байкальский государственный университет. – 2012. – № 1 – С. 157-162.

48. Яковлева К.Ю. Соотношение электронной информации с некоторыми видами доказательств в уголовном процессе // Теория и практика общественного развития. – 2023. – №. 2 (180). – С. 153-156.

49. Меркулова М. В. О некоторых проблемах получения материалов записи устройств видеонаблюдения в ходе расследования преступлений // Устойчивое развитие: геополитическая трансформация и национальные приоритеты. – 2023. – С. 1088-1095.

50. Тлеубаев Д. К., Карымсаков Р. Ш. Электронныйучет посетителей в правоохранительных органах в РеспубликеКазахстан //Актуальные научные исследования в современном мире. – 2021. – №. 4-6. – С. 166-170.

51. Зарубин М. Ю., Зарубина В. Р. Актуальность создания облачной ERP-системы для малого бизнеса Республики Казахстан // Актуальные проблемы теории и практики управления. – 2017. – С. 70-76.

52. Трущенков Т. А., Трущенков И. В. Некоторые аспекты осмотра, обыска и выемки в целях обнаружения, фиксации и изъятия компьютерной информации для производства судебной компьютерной экспертизы // Теория и практика судебной экспертизы: международный опыт, проблемы, перспективы. – 2017. – С. 27-33.

53. Титов А. А. Некоторые вопросы обнаружения и исследования компьютерной информации при раскрытии и расследовании преступлений // Сибирские уголовно-процессуальные и криминалистические чтения. – 2022. – №. 3 (37). – С. 39-48.

54. Дедковский А. А. Проблемы обнаружения, фиксации и изъятия цифровой информации по уголовным делам // Цифровая экономика-образованию и науке Союзного государства Беларуси и России. – 2020. – С. 17-21.

55. Гурдин С. В., Саморока В. А. Процессуальные аспекты получения информации из облачного хранилища // Рецензенты: начальник 5-го отдела Следственного управления УВД по ЦАО ГУ МВД России по г. Москве ВА Богдан; следователь 1-го отдела Следственного управления УВД по ЮВАО ГУ МВД России по г. Москве АВ Акимов. – 2020. – С. 85 – 90.

56. Гурдин С. В., Саморока В. А., Абдрахманова Л. Р. К вопросу о получении информации из «Облачного» хранилища при производстве по уголовному делу // Уголовное судопроизводство России: проблемы и перспективы развития. – 2020. – С. 58-62.

57. Степанова Т. Ю., Пихтерев С. Г., Сергеев Е. И. Обеспечение безопасности облачных хранилищ // Лучшая студенческая статья 2018. – 2018. – С. 169-171.

58. Кодолов П. А. Облачное хранилище данных // Наука, техника и образование. – 2016. – №. 4 (22). – С. 51-53.

59. Шефер В. Ю. Основные принципы исследования криминалистически значимой информации в «Облачных сервисах» // Экспертные чтения на Енисее. – 2020. – С. 73-75.

60. Афанасьев Н. С. Проблемы безопасности хранения данных в облачных хранилищах // Актуальные научные исследования в современном мире. – 2021. – №. 7-2. – С. 97-102.

61. Рогова И. А., Бурцева Е. Практика применения UFED–универсального устройства для криминалистического исследования мобильных устройств // Евразийский союз ученых. – 2015. – №. 7-5 (16). – С. 97-100.

62. Афанасьев Н. С. Исследование технологии облачного хранилища // Актуальные научные исследования в современном мире. – 2021. – №. 7-2. – С. 91-96.

63. Баженов С. В. Оперативно-розыскное мероприятие «получение компьютерной информации» // Научный вестник Омской академии МВД России. – 2017. – №. 2 (65). – С. 31-33.

64. Федотов Е. А., Трошкин А. П., Люкутан С. В. Обеспечение единого доступа к облачным хранилищам информации // Ученый XXI века. – 2017. – №. 1-1 (26). – С. 11-13.

65. Екимцев С. В. Особенности проведения оперативно-розыскного мероприятия «получение компьютерной информации» // Научный вестник Орловского юридического института МВД России имени В.В Лукьянова. – 2019. – №. 2. – С. 27-30.

66. Мирошниченко М. А., Абдуллаева А. А., Дементьев М. А. Облачные технологии-направление развития современных информационных систем компании в цифровой экономике // Естественно-гуманитарные исследования. – 2023. – №. 45 (1). – С. 164-171.

67. Единый реестр досудебных расследований // [Электронный ресурс] – Режим доступа: https://erdr-public.kgp.kz (дата обращения: 20.02.2024).

68. Мобильный Криминалист // [Электронный ресурс] – Режим доступа: https://mko-systems.ru/mobile-expert (дата обращения: 20.02.2024).

69. Brenner S. W., Frederiksen B. A. Computer Searches and Seizures: Some Unresolved Issues // 8 MICH. TELECOMM. &TECH. L. REV. 39, 82 (2002).

70. CanadaEvidenceAct, RSC– 1985.– P. 5. – [Электронный ресурс] – Режим доступа: http://www.canlii.ca/t/541b5 (датаобращения: 20.10.2023).

71. Coded‘InstructionCriminelle [C.I.CR.]. – [Электронный ресурс] – Режим доступа: http://www.droitbelge.be/codes.asp#ins (датаобращения: 21.04.2020).

72. CodeofCriminalProcedure. – [Электронныйресурс] – Режимдоступа: http://www.legifrance.gouv.fr/content/location (датаобращения: 20.10.2023).

73. CriminalcodeofCanada. – [Электронный ресурс] – Режим доступа: http://www.laws-lois.justice.gc.ca/eng/acts/C-46/ (датаобращения: 20.10.2023).

74. FederalRulesofEvidence. – [Электронный ресурс] – Режим доступа: http://www.rulesofevidence.org/ (датаобращения: 20.10.2023).

75. General principles for the interpretation and application of the Charter. Section 8 – Searchandseizure. – [Электронный ресурс] – Режим доступа: https://www.justice.gc.ca/eng/csjsjc/rfc-dlc/ccrf-ccdl/check/art8.html (датаобращения: 20.10.2023).

76. Kerr O. S. Search warrants in an era of digital evidence // Mississippi Law Journal. – 2005. – December. – P. 87–88.

77. MifsudBonnici J. P., Tudorica M., Cannataci J. A. The European Legal Framework on Electronic Evidence: Complex and in Need of Reform // Handling and Exchanging Electronic Evidence Across Europe (Law, Governance and Technology Series; Vol. 39). – 2018. – P. 189–235.

78. Orin S. Kerr. Digital Evidence and the New Criminal Procedure // 105 COLUM. L. REV. – 2005. – P. 279, 308.

79. Oxygen Forensic Extractor for Clouds // [Электронный ресурс] – Режим доступа:https://www.securitywizardry.com/index.php/products/forensic-

solutions/forensic-tools/oxygen-forensic-extractor-for-clouds (датаобращения: 20.02.2024).

80. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. U. S. DepartmentofJustice. – [Электронный ресурс] – Режим доступа: http://www.ustice.gov/sites/files/legacy/2015/01/14/ssmanual2009 (датаобращения: 20.10.2023).

81. The German Code of Criminal Procedure. StPO. – [Электронный ресурс] – Режим доступа: http://www.gesetze-im-internet.de/ englisch_stpo/ (датаобращения: 20.10.2023).

82. United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Criminal Laws and Procedures. – U.S. Government Printing Office, 1978. – P. 10730.

Приложение 1

СРАВНИТЕЛЬНАЯ ТАБЛИЦА

предложений по внесению изменений и дополнений в некоторые правовые акты Республики Казахстан, выработанных по результатам диссертационных исследований Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан

№	Структурный элемент	Действующая редакция	Предлагаемая редакция	Обоснование
Уголовно-процессуальный кодекс Республики Казахстан				
1	Новый подпункт 59) статьи 7	Подпункт 59 статьи 7 отсутствует	Статья 7. Разъяснение некоторых понятий, содержащихся в настоящем Кодексе «удаленный (онлайн) обыск – действия, проводимое лицом, осуществляющим досудебное расследование для поиска фактических данных правонарушении через интернет, в режиме онлайн доступа к персональному оборудованию обыскиваемого лица»	Предполагаемая редакция позволит: 1. Соответствие современным реалиям: В условиях развития информационных технологий и активного использования интернета для совершения преступлений, включая различные виды мошенничества, террористическую пропаганду, детскую порнографию и другие правонарушения, необходимо внедрение новых методов и инструментов для проведения досудебного расследования. 2. Эффективность и оперативность: Проведение удаленного (онлайн) обыска позволит оперативно получать необходимую информацию о фактических данных правонарушении через интернет, минимизируя временные затраты на сбор доказательств и ускоряя процесс досудебного

				расследования. 3. Соблюдение законности: Введение данного положения в УПК РК обеспечит соответствие процессуальных действий законодательству, а также международным стандартам в области прав человека и обеспечения справедливого судопроизводства. 4. Защита прав граждан: Удаленный (онлайн) обыск будет проводиться с соблюдением всех прав и законных интересов граждан, обеспечивая при этом конфиденциальность и сохранность информации. 5. Прозрачность и контроль: Введение данного положения обеспечит более высокий уровень прозрачности и контроля за процессом досудебного расследования, так как все действия будут фиксироваться в реальном времени. 6. Минимизация рисков: Удаленный обыск снизит риск воздействия на обыскиваемое лицо, так как не требует его физического присутствия и минимизирует вмешательство в его частную жизнь. Таким образом, добавление положения о проведении удаленного (онлайн) обыска в УПК РК не только оптимизирует процесс сбора доказательств и досудебного расследования, но и обеспечивает соблюдение прав граждан и законных интересов, соответствуя современным требованиям правового государства.
2	Новая статья 221-1	Статья 221-1 отсутствует	Статья 221-1. «Осмотр облачных хранилищ» 1. Осмотр информации из облачных хранилищ осуществляется с санкции следственной судьи. 2. При необходимости производства	Предполагаемая редакция позволит: 1. Регулирование процесса осмотра информации из облачных хранилищ: Добавление статьи 221-1 в УПК РК позволит законодательно установить порядок осмотра информации, хранящейся в облачных хранилищах данных, что обеспечит

			принудительного осмотра информации из облачных хранилищ, осуществляющее досудебное расследование, выносит постановление о производстве осмотра и направляет его следственному судье. 3. При возникновении необходимости в осмотре информации, хранящейся в облачных хранилищах, осмотр должен быть произведен безотлагательно с целью обеспечения правопорядка и соблюдения законности, но с последующим направлением материалов следственному судье в суточный срок. 4. Осмотр информации из облачных хранилищ проводится с использованием современных научно-технических средств для фиксации хода и результатов осмотра. При необходимости могут быть привлечены специалисты для анализа полученной информации. При осмотре информации из облачных хранилищ может быть предусмотрено участие подозреваемого, потерпевшего, свидетеля или специалиста по решению лица, ответственного за производство осмотра, с соблюдением их прав и законных интересов. 5. Осмотр информации из облачных хранилищ должен осуществляться в соответствии с законодательством о защите персональных данных, обеспечивая конфиденциальность и сохранность	правовую ясность и прозрачность в проведении таких действий правоохранительными органами. 2. Защита персональных данных: Введение данной статьи обеспечит соблюдение законодательства о защите персональных данных при осмотре информации из облачных хранилищ, что является важным аспектом для защиты прав и законных интересов граждан. 3. Эффективность расследования преступлений в сфере информационных технологий: Проведение осмотра информации из облачных хранилищ является неотъемлемой частью расследования преступлений, связанных с использованием современных информационных технологий. Введение соответствующей статьи в УПК РК обеспечит эффективность и оперативность таких расследований. 4. Ответственность и контроль: Добавление статьи 221-1 позволит установить ответственность за соблюдение прав и законных интересов участников процесса при проведении осмотра информации из облачных хранилищ, а также обеспечит контроль за сохранностью и корректностью осмотренной информации. Таким образом, введение статьи 221-1 "Осмотр облачных хранилищ" в УПК РК не только обеспечит законность и прозрачность в досудебном расследовании, но и содействует эффективному борьбе с преступлениями в сфере информационных технологий, сохраняя при этом права и законные интересы граждан.

			информации, за исключением случаев, предусмотренных законом. 6. Лица, производящие осмотр информации из облачных хранилищ, несут ответственность за соблюдение прав и законных интересов участников процесса, а также за сохранность и корректность осмотренной информации. 7. Полученная в результате осмотра информация из облачных хранилищ подлежит документированию и использованию в соответствии с уголовно-процессуальным законодательством. 8. Изъятая информация, вместе с протоколом приобщается к материалам уголовного дела и хранится до окончательногоразрешения уголовного дела.	
Закон Республики Казахстан «О персональных данных и их защите»				
3	Новый пункт 14-1 статьи 1	Пункт 14-1 статьи 1 отсутствует	Статья 1. Основные понятия, используемые в настоящем Законе «Облачное хранилище данных – это модель онлайн - хранилища, данные в котором хранятся на множественных серверах, распределённых в сети»	Предполагаемая редакция позволит: 1. Соответствие современным технологиям: Облачные хранилища данных стали широко распространенным инструментом для хранения и обработки информации. Введение определения "Облачное хранилище данных" позволит законодателю четко определить особенности обработки и хранения данных в облачных системах. 2. Защита персональных данных: Определение "Облачное хранилище данных" позволит законодателю разработать соответствующие механизмы регулирования доступа к персональным данным, хранящимся в облаке, что способствует

				повышению уровня их защиты. 3. Разработка порядка осмотра информации из облачных хранилищ: Введение определения "Облачное хранилище данных" позволит в рамках УПК РК разработать соответствующий порядок осмотра информации из таких хранилищ, что обеспечит правовую основу для осуществления таких действий правоохранительными органами. Таким образом, введение данной нормы обеспечит защиту конституционных прав и свобод граждан, включая право на конфиденциальность и защиту их персональных данных в облачных хранилищах.