АКАДЕМИЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ ПРИ
ГЕНЕРАЛЬНОЙ ПРОКУРАТУРЕ РЕСПУБЛИКИ КАЗАХСТАН

ИНСТИТУТ ПОСЛЕВУЗОВСКОГО ОБРАЗОВАНИЯ

КУЛБАЕВ ЕРБОЛ САРСЕНБЕКОВИЧ

Открытые источники данных как инструмент сбора информации на первоначальном этапе расследования

Проект на соискание степени магистра национальной безопасности и военного дела по образовательной программе 7М12301 «Правоохранительная деятельность» (профильное направление, а также с применением дистанционного обучения)

Научный руководитель:
доцент кафедры
общеюридических дисциплин
Байгалиев А.Б.,
доктор PhD,
младший советник юстиции
_____

г. Косшы, 2025 г.

ТҮЙІНДЕМЕ

Магистрлік жұмыс қылмыстық құқық бұзушылықтарды тергеудің бастапқы кезеңінде ақпарат жинау құралы ретінде ашық дереккөздерді (OSINT) қолдану мәселесіне арналған. Цифрландыру жағдайында дәлелдеудің дәстүрлі тәсілдерін қайта қарау қажеттілігі негізделеді. Автор ашық дереккөздер ұғымы, олардың жіктелуі мен құқықтық реттелуін зерттеп, Қазақстан Республикасының қылмыстық процесінде қолданылуына байланысты проблемаларды анықтайды.

Зерттеу нәтижелері заң шығару, оқу процесі мен тергеу және жедел бөлімшелердің тәжірибелік қызметінде қолданылуы мүмкін.

РЕЗЮМЕ

Магистерский проект посвящен исследованию использования открытых источников данных (OSINT) в уголовно-процессуальном доказывании на первоначальном этапе расследования уголовных правонарушений. Обосновывается актуальность темы в условиях цифровизации, когда традиционные подходы к доказыванию требуют переосмысления. Автор анализирует понятие, классификацию и правовое регулирование открытых источников данных, выявляет существующие проблемы их использования в уголовном процессе Республики Казахстан.

Результаты работы могут быть использованы в правотворчестве, учебном процессе и практике следственных и оперативных подразделений.

SUMMARY

This master’s thesis explores the use of open source intelligence (OSINT) as a tool for information gathering at the initial stage of criminal investigations. It emphasizes the need to reconsider traditional approaches to evidence in light of ongoing digitalization. The author examines the concept, classification, and legal regulation of open sources and identifies problems in their use within the criminal procedure of the Republic of Kazakhstan.

The findings of the research can be applied in legislative activity, legal education, and the practical work of investigators and operational units.

СОДЕРЖАНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

OSINT	(open source intelligence, разведка по открытым источникам) — это сбор и анализ информации из публичных источников
США	Соединённые Штаты Америки
ЮНЕСКО	Организация Объединённых Наций по вопросам образования, науки и культуры
СМИ	средство массовой информации
СИОПСО	системы информационного обмена правоохранительных, специальных государственных и иных органов
УПК РК	Уголовно-процессуальный кодекс Республики Казахстан
УК РК	Уголовный кодекс Республики Казахстан
КНР	Китайская Народная Республика
ДП	Департамент полиции
ГПК РК	Гражданский процессуальный кодекс Республики Казахстан
ОРД	Оперативно-розыскная деятельность
OGP	Open Government Declaration (*Декларация об открытом правительстве*)
ФАТФА	FATF — *Financial Action Task Force* — международная организация, созданная с целью разработки и продвижения стандартов по борьбе **с** отмыванием денег**,** финансированием терроризма и распространением оружия массового уничтожения
SPF	*Sender Policy Framework* – механизм проверки подлинности отправителя электронной почты путём сопоставления IP-адреса с разрешённым перечнем для домена
DKIM	*DomainKeys Identified Mail* – технология цифровой подписи писем, обеспечивающая проверку целостности и аутентичности отправителя
DMARC	*Domain-based Message Authentication, Reporting and Conformance* – политика валидации писем, основанная на проверке SPF и DKIM, с возможностью управления результатами и получения отчётности
ГИС	*Геоинформационная система* – программный комплекс для сбора, анализа и визуализации пространственных (географических) данных
FindFace SDK	Программный модуль для интеграции технологии распознавания лиц, разработанный компанией NtechLab. Используется для идентификации и поиска лиц по фото- или видеоматериалам

ВВЕДЕНИЕ

Актуальность проводимого исследования. Как известно, эффективность стадии предварительного расследования уголовных правонарушений во многом зависит от результатов первоначального этапа этого расследования. Именно на данном этапе бывает возможным раскрытие правонарушения «по горячим следам», в рамках которого уполномоченные лица обнаруживают, фиксируют и изымают следы преступления, а также осуществляется задержание подозреваемых в преступлении лиц. Добытые на первоначальном этапе фактические данные обладает большим доказательственным значением, что обуславливается, к примеру, свежестью восприятия информации потерпевшими и свидетелями, сохранностью от нежелательного воздействия различных фактических данных, имеющих существенного значение для правильного разрешения дела.

Как утверждает Д. А. Влезько, от того, как организована работа в данный период, от правильного выбора, квалифицированного и своевременного выполнения необходимых следственных и иных действий во многом зависит успех дальнейшего расследования и всего производства по уголовному делу [1, с. 362].

На первоначальном этапе осуществляется сбор информации, имеющей какое-либо отношение к расследуемому преступному событию. Однако не всегда получается сразу обнаружить фактические данные, относимые уголовно-процессуальным законом к числу доказательств, которые в соответствии со ст.125 УПК РК должны обладать признаками относимости, допустимости, достоверности. Поэтому на данном этапе расследование немаловажное значение приобретают открытые источники данных, которые используются в качестве инструмента сбора необходимой информации.

В настоящий период уголовно-процессуальная практика зиждется на нормативных правилах доказывания, который сформулирован как минимум более полувека назад. Между тем условия современной жизни обуславливают необходимость переосмысления традиционных постулатов в сфере уголовно-процессуального доказывания. Это в основном связано, как с появлением новых источников, содержащих различные информационные данные, так и с формой их формирования, хранения, передачи и т.д.

Претерпел серьезное изменение и способ формирования, хранения, передачи источников данных. Это связано тем, что современное общество переживает период глобальной цифровизации. Огромные объемы информационных ресурсов, финансовых средств, производственных процессов и прочего приобрели электронную (цифровую) форму.

На необходимость широкого внедрения информационных технологий во все сферы деятельности страны указал и Президент Республики Казахстан в своем Послании народу Казахстана от 1 сентября 2021 года «Единство народа и системные реформы – прочная основа процветания страны»: «В современном

мире одним из главных факторов конкурентоспособности является глубинная цифровизация. Для Казахстана крайне важны трансферт современных цифровых технологий. Мы должны реализовать свой огромный информационно-телекоммуникационный потенциал. В новую цифровую эпоху он будет иметь геополитическое значение» [2].

Актуальность темы нашего исследования обусловлена двумя основными факторами. В первую очередь исследование расширенного перечня открытых источников данных, а затем способы их использования в уголовно-процессуальном доказывании в качестве инструмента сбора информации на первоначальном этапе расследования в условиях всеобщей цифровизации.

До настоящего времени в Республике Казахстан глубоких, комплексных исследований в обозначенной нами сфере не проводилось.

Оценка современного состояния решаемой практической задачи. Научных работ, посвященных исследованию открытых источников данных как инструмента сбора информации на первоначальном этапе расследования, не много. Отдельные аспекты рассматриваемой темы содержатся в работах таких ученых, как: С. А. Машков, С. Овсейко, Н. О. Павленко, Б. В. Рудаков, А. О. Сукманов, М. М. Сарычев, П. А. Фаниев, А. Р. Шарипова, М. О. Янгаева и другие.

Среди казахстанских ученых к рассматриваемой теме обращались А.Т. Коныров, К. К. Сейтенов.

Цель исследования – комплексное исследование вопросов об открытых источниках данных как инструментов сбора информации на первоначальном этапе расследования, определение существующих проблемы выработка предложений по совершенствованию законодательства и правоприменительной практики.

Для достижения этой цели определены следующие задачи исследования:

- изучить вопросы о понятии и классификации открытых источников данных (OSINT);
- проанализировать законодательную регламентацию использования открытых источников данных в уголовно-процессуальном доказывании;
- ознакомиться с правоприменительной практикой по использованию в уголовном процессе открытых источников данных;
- выявить имеющиеся проблемы, связанные с использованием в уголовном процессе открытых источников данных
- предложить пути совершенствования законодательства и правоприменительной практики по использованию в уголовном процессе открытых источников данных.

Объектом исследования выступают общественные отношения, возникающие при применении в уголовном судопроизводстве сведений, полученных из открытых источников.

Предметом исследования служат положения уголовно-процессуального законодательства Республики Казахстан, а также положения международных

нормативных документов, регламентирующих порядок использования открытых данных в рамках уголовного процесса.

Методы и методические основы проведения исследования включает в себя комплекс подходов: общенаучные методы (анализ, синтез, аналогия), частно-научные (статистический, социологический), а также специальные методы юридического познания — сравнительно-правовой и формально-юридический.

Обоснование научной новизны заключается в комплексном анализе возможности использования открытых источников данных (OSINT) в целях уголовно-процессуального доказывания на первоначальном этапе расследования уголовных правонарушений. До настоящего времени в Республике Казахстан данное направление не подвергалось всестороннему научному изучению, а существующие труды затрагивают лишь отдельные аспекты темы.

В работе впервые:

— обоснована необходимость системного подхода к понятию и классификации открытых источников данных применительно к задачам уголовного судопроизводства;

— выявлены пробелы в законодательной регламентации использования OSINT в рамках уголовно-процессуального доказывания;

— предложены конкретные формулировки для внесения в Уголовно-процессуальный кодекс Республики Казахстан, Закон Республики Казахстан «О доступе к информации», Закон Республики Казахстан «Об оперативно-розыскной деятельности» с целью легитимизации использования данных из открытых источников;

— сформулированы предложения по разработке методических рекомендаций и инструкций, регламентирующих применение современных цифровых инструментов и технологий для сбора информации из открытых источников в ходе следственных и оперативно-розыскных мероприятий.

Практические рекомендации:

1. Поскольку Закон Республики Казахстан «О доступе к информации» занимает ключевое положение в сфере регулирования открытых источников данных, представляется обоснованным пересмотреть содержащуюся в нем дефиницию информации с учетом положений Модельного закона об информатизации, информации и защите информации (2005 г.). В этой связи предлагается пункт 1) статьи 1 указанного Закона изложить в следующей редакции: информация — это сведения либо данные, касающиеся лиц, объектов, фактов, событий, явлений или процессов, зафиксированные в любой форме.

2. Целесообразным видится нормативное закрепление термина «компьютерная информация» в статье 7 нового пункта 60) Уголовно-процессуального кодекса Республики Казахстан. В предлагаемой редакции он может быть сформулирован следующим образом: «Компьютерная информация — это полученные в рамках закона сведения о фактических обстоятельствах, имеющих значение для разрешения уголовного дела, воспринимаемые компьютерными средствами и выраженные в виде электрических импульсов,

которые могут храниться, обрабатываться и передаваться с помощью различных электронных носителей данных».

3. В целях совершенствования правовой регламентации, целесообразно внести следующие изменения в Закон Республики Казахстан «Об оперативно-розыскной деятельности»:

— внести дополнение в статью 1, включив определение термина «оперативно-розыскной мониторинг открытых источников информации» в следующей формулировке: *«Оперативно-розыскной мониторинг открытых источников информации представляет собой непрерывный процесс наблюдения за информационно-телекоммуникационными ресурсами с целью выявления, сбора и анализа сведений о потенциально опасных для общества явлениях и процессах, а также об условиях, способствующих их возникновению и развитию, в целях их оперативного предотвращения либо последующего уголовного преследования»;*

— дополнить часть 1 статьи 14-1 следующим положением: *«При необходимости, в процесс использования информационных систем может быть привлечён специалист, обладающий соответствующими знаниями и навыками».*

4. Обоснованным представляется внесение в статью 7 Уголовно-процессуального кодекса Республики Казахстан нового пункта 59), изложенного в следующей редакции: *«Электронный носитель информации – это физический объект, предназначенный для записи, хранения и воспроизведения данных в форме электронного документа, имеющего значение для объективного и законного разрешения уголовного дела».*

5. Полученные в ходе анализа результаты свидетельствуют о необходимости следующих мер:

— подготовка алгоритма, регламентирующего порядок проведения оперативно-розыскного мониторинга открытых источников как в рамках общего наблюдения, так и при целенаправленном поиске конкретных лиц (подозреваемых, обвиняемых) либо утраченного имущества;

— разработка инструктивных положений, регулирующих порядок эксплуатации современных цифровых инструментов, с целью повышения эффективности их применения сотрудниками оперативных подразделений правоохранительных органов.

Апробация и внедрение результатов. Итоги проведённого исследования могут быть использованы в учебной и прикладной деятельности: при подготовке специалистов в сфере уголовного судопроизводства, преподавании курсов по уголовному процессу и криминалистике, а также в рамках повышения квалификации сотрудников правоохранительных органов, прокуроров, судей и адвокатов.

Результаты проведенного исследования были опубликованы в научный статье на тему «К вопросу о нормативном определении понятия «компьютерная информация» в законодательстве республики Казахстан», а также внедрены в

практическую деятельность в форме аналитических записках и рабочих материалов о чем есть соответствующий акт внедрения [Приложение 1].

1. Открытые источники данных как инструменты сбора доказательств в уголовном процессе

1.1 Понятие и классификация открытых источников данных (OSINT)

Для рассмотрения заявленной темы исследования первоначальной задачей является раскрытие самого понятия открытых источников данных, а затем и ознакомление с существующей в настоящее время их классификацией.

Зарождение понятия открытых источников данных исследователи соотносят с идеями об открытых данных, возникшими в 1995 году в научной среде американцев, которые инициировали открытое изложение информации касательно глобальных проблемных вопросов в сфере окружающей среды [3. с.185].

В дальнейшем указанная идея получила повсеместное распространение и получило обозначение как открытые данные, которые постепенно стали востребованными применительно ко всем сферам общественной жизни.

По утверждению ряда исследователей термин «открытые данные» «имеет хождение не столь долгое время…началом к его распространению послужило движение, инициаторами которого были ученые, борющиеся за необходимость обеспечения всеобщего доступа к результатам исследований» [3. с.187].

По словам ряда исследователей, термин «открытые данные» «имеет сравнительно недавнюю историю…в истоках которой находится движение ученого мира за всеобщий доступ к результатам исследований. По мере своего развития понятие, обозначаемое данным термином, стал включать в себя различные значения диапазон, которых начинался от инструмента научных исследований до вопросов вовлечения гражданского общества в дела государства» [3. с.187].

Открытые данные (англ. Open data) – это концепция, отражающая идею о том, что определенные данные должны быть свободно доступны для машиночитаемого использования и дальнейшей републикации без ограничения авторского права, патентов и других механизмов контроля.

«Средством защиты от всеобщего доступа могут выступать свободные лицензии, таких, как, например, лицензий Creative Commons. При наличии определенной защиты информации от свободного доступа или при отсутствии лицензии, которая разрешала бы использовать данные повторно и свободно, информация не подпадает под определение открытых данных, невзирая на наличие его машинописного изложения и размещения в Интернете» [4].

На официальном сайте Международной хартии открытых данных можно обнаружить следующее определение: «Открытые данные» можно определить, как данные и контент, которые могут свободно использоваться и предоставлять кому-либо для любых целей безвозмездно» [5].

С. А. Панюкова под открытыми данными предлагает понимать «информацию о деятельности государственных органов и органов местного

самоуправления, а также данные собранные информационно-аналитическими организациями, размещенные в сети Интернет в виде массивов данных в формате, обеспечивающим их автоматическую обработку для повторного использования без предварительного изменения человеком, и на условиях его свободного (бесплатного) в любых соответствующих закону целях любыми лицами независимо от формы ее размещения» [6. с.25-33].

На основе анализа существующих в настоящее время научных толкований можно вычленить наиболее характерные следующие признаки открытых данных:

- они являются информацией, не имеющей каких-либо запретов или ограничений для доступа к ней и ее последующей републикации;
- они не защищены действием авторского права, лицензий, патентов и иных правовых способов ограничений доступа;
- закон не запрещает их повторное использование;
- они обнародуют деятельность государственных органов и органов местного самоуправления, а также распространяют итоговые сведения по деятельности информационно-аналитических организаций;
- закон не предусматривает внесение платы за пользование ими;
- они размещены в машиночитаемом формате.

Постепенно, по мере большей популяризации повсеместного распространения вопросы об открытых данных переместились в правовое поле, и сфера государственного управления также стала их использовать.

«Стартовой площадкой указанного движения рассматриваемого явления является Меморандум об открытом правительстве (Transparency and Open Government memorandum), совершенный 20 января 2009 года в США. В указанном документе были прописаны основные постулаты открытых данных – это прозрачность деятельности правительства, совместность его работы, а также необходимость сотрудничества правительства с обществом» [7].

Основные постулаты Меморандума были заимствованы и усовершенствованы в Директивах открытого правительства (Open Government Directive) [8].

Положение указанных выше документов были восприняты во многих других государствах.

Организация Объединенных Наций в 2013 году разработало руководство, в котором освещались вопросы участия граждан в сфере открытых правительственных данных (Guidelines on Open Government Data for Citizens Engagement). В Руководстве открытые данные обозначаются в качестве материала, доступного для использования любым человеком по его необходимости. В качестве альтернативы понятию «государственная информация» в Руководстве используется понятие «информация общественного сектора», в качестве которой рассматриваются любые данные, исходящие от Органа общественного сектора [9].

В октябре 2015 года Международный саммит OGP принял Международную хартию открытых данных (Open Government Declaration). Документ предлагал разработанные принципы и методы открытого размещения государственной информации. К данной Хартии приняли для руководства 150 государств.

Хартия нормативно закрепляла следующую дефиницию: «Открытые данные — это цифровые данные, которые предоставляются с техническими и юридическими характеристиками, необходимыми для их свободного использования, повторного использования и распространения любым человеком в любое время и в любом месте» [10].

ЮНЕСКО наиболее приемлемым с правовой позиции следует признать разъяснение этого понятия, исходящее от Фонда открытых знаний, где: «Открытые данные и контент могут свободно использоваться, изменяться и распространяться кем угодно для любых целей» [11].

В Республике Казахстан правовым документом, освещающим сферу открытых данных, в том числе права пользователей, является Закон Республики Казахстан от 16 ноября 2015 года «О доступе к информации».

Кроме указанного нормативного акта вопросы использования открытых данных содержатся также в таких законах, как: Закон Республики Казахстан от 24 ноября 2015 года «Об информатизации», Закон Республики Казахстан от 19 июня 2024 года «О масс-медиа», Закон Республики Казахстан от 10 июля 2023 года «Об онлайн-платформах и онлайн-рекламе».

В приведенном выше нормативном правовом комплексе можно обнаружить нормативные толкования понятий, которым свойственно ключевое значение. К таковым относятся: «информация», «данные», «сообщения», «интернет ресурс», «электронный информационный ресурс».

Так, в Законе Республики Казахстан «О доступе к информации» содержатся следующие определения:

«- информация – сведения о лицах, предметах, фактах, событиях, явлениях, процессах, зафиксированных в любой форме (п.1) ст.1);

- открытые данные – данные, представленные в машиночитаемом виде и предназначенные для дальнейшего использования, повторной публикации в неизменном виде» (п.5) ст.1) [12].

Закон Республики Казахстан «Об информатизации» дает разъяснение следующих определений:

«- интернет-ресурс – информация (в текстовом, графическом, аудиовизуальном или ином виде), размещенная на аппаратно-программном комплексе, имеющем уникальный сетевой адрес и (или) доменное имя и функционирующем в Интернете;

- электронные информационные ресурсы – данные в электронно-цифровой форме, содержащиеся на электронном носителе и в объектах информатизации» [13].

В Законе Республики Казахстан «О масс-медиа» можно обнаружить определение официального сообщение, под которым предлагается понимать «информацию, предоставляемую и (или) распространяемую посредством масс-медиа обладателем информации, установленным в соответствии с Законом Республики Казахстан «О доступе к информации»» [14].

В Законе Республики Казахстан «Об онлайн-платформах и онлайн-рекламе» разъясняется, что «под ложной информацией следует понимать информацию, не соответствующую действительности либо содержащую существенные искажения фактов, создающих ложное представление о лицах, предметах, событиях, явлениях и процессах, зафиксированная в любой форме» [15].

Для всех приведенных выше разъяснений основным термином, используемым для разъяснения соответствующих понятий, выступает слово «информация».

Следует отметить, что термином «информация» апеллирует также Модельным законом государств-участников СНГ от 18 ноября 2005 года «Об информатизации, информации и защите информации». Данный закон разъясняет, что «информация - сведения или данные, порядок использования которых, независимо от способа их представления, хранения или организации, подлежит правовому регулированию в соответствии с настоящим Законом и иными национальными законами» [16].

Получается, что термины «информация» и «открытые данные» имеют свойство взаимозаменяемости, поскольку ими апеллируют при толковании взаимоувязанных понятий. Следует обратить внимание на то, что понятие «информация» представляется более емким по сравнению с понятием «открытые данные». Это связано с тем, что «информация» может складываться из любых сведений, зафиксированных в любой форме. Открытыми данными признаются лишь сведения, зафиксированные в машиночитаемом формате. В результате получается, что открытые данные образуют определенную часть более емкого понятия «информация».

Однако, к сожалению, в Законе Республики Казахстан «О доступе к информации», который признается основным правовым актом по отношению к остальным, регулирующем рассматриваемую нами сферу, установленное нами соотношение используемых ключевых понятий не учтено.

В этой связи следует признать справедливыми слова Э. Г. Минькашева, по мнению которого, «термин «информация» должен получать разъяснение посредством использования родового термина «данные». В данном случае допустимо применение сочинительного союза «или». По отношению к слову «сведения» этот сочинительный союз будет разделительным. Иными словами, термин «информация» означает «данные или сведения», а не «сведения (сообщения, данные)», что соответствует логике Модельного закона об информатизации, информации и защите информации от 2005 года» [17. с. 283–287].

В этой связи справедливо высказывание Л. А. Коврижных, по мнению которой «неточное, размытое разъяснение определенного понятия может привести к возникновению смысловой неточности и, в результате, станет причиной ошибок, допускаемых в правоприменительной деятельности» [18, с. 158].

В связи с тем, что в комплексе нормативных правовых актов, имеющих отношение к открытым данным, Закон Республики Казахстан «О доступе к информации», представляется основным, на наш взгляд, именно содержащееся в нем толкование понятия «информации» должно быть приведено в согласование с логикой Модельного закона об информатизации, информации и защите информации от 2005 года. В этих целях полагаем необходимым п.1) ст.1 Закона Республики Казахстан «О доступе к информации» изложить в следующей редакции:

- информация – сведения *или данные* о лицах, предметах, фактах, событиях, явлениях, процессах, зафиксированных в любой форме.

Данная корректировка, связанная с соотнесением нормативных разъяснений, содержащихся в отечественном законодательном акте и международном документе, обеспечит единообразное понимание и применение государственными органами и гражданами в плане обеспечения их свободного доступа к открытым данным.

Как и при использовании любого правового института применение открытых данных основывается на определенных принципах.

Впервые принципы открытых данных, предоставляемых государственными органами, были сформулированы еще в 2007 году. В настоящее время они распространяются на открытые данные из любых источников. К таковым относятся:

«1. Полнота - предоставление всей информации, не обремененной признаками конфиденциальности, безопасности или привилегий.

2. Первичность – исключение агрегированных либо модифицированных форм

3. Своевременность – обеспечение актуальности ко дню истребования за счет высокой скорости.

4. Доступность – свободная возможность пользования любыми лицами.

5. Машинная обработка – данные достаточно структурированы, чтобы обеспечить автоматизированную обработку.

6. Недискриминационные – предоставление информации без запроса данных о личности потребителя.

7. Отсутствие проприетарности – данные доступны в формате, над которым ни один субъект не имеет исключительного контроля.

8. Отсутствие лицензии – информация не обременена ограничениями на основе патентов, авторских прав, товарных знаков или коммерческой тайны. Допустимы разумные ограничения по конфиденциальности, безопасности и привилегированности данных» [19].

Если обратиться к содержательной стороне открытых данных, то обнаруживается очень большое количество источников информации, которые в настоящее время следует отнести к открытым данным. Сейчас открытые источники данных включают:

- поисковые Интернет-системы;
- базы данных;
- электронные средства массовой информации (Интернет-СМИ);
- различные «социальные сети»;
- сайты информационных агентств;
- различные персональные сайты (к таким относятся сайты отдельных организаций, а также личные сайты физических лиц).

Более полно и детализировано содержание открытых данных представлено в нижеследующей схеме на рисунке 1.

Рисунок 1 – Классификация открытых источников информации по видам и каналам поступления

Примечание: в данную схему включены как традиционные медиа-каналы (периодические издания, телевидение, радио), так и цифровые ресурсы (интернет-сайты, форумы, специализированные базы данных), а также мнения экспертов и справочные материалы официальных структур.

Широкое распространение открытых данных способствовало возникновению определенной деятельности, связанной с их использованием. Так, например, в настоящее время появилась аббревиатура «OSINT», которая расшифровывается как «Open-source intelligence, то есть разведка по открытым

источникам. OSINT представляет собой сбор и анализ информации, полученной из разных общедоступных информационных каналов. По сути, такими источниками может быть что угодно: газеты и журналы, телевидение и радио, данные, публикуемые официальными организациями, научные исследования и доклады на конференциях и так далее» [20].

Ниже, на рисунке 2 показаны этапы развития OSINT.

Рисунок 2 – Этапы развития OSINT (разведки на основе открытых источников) в исторической перспективе

Примечание: временная шкала демонстрирует ключевые этапы эволюции OSINT — от анализа СМИ в начале XX века до интеграции инструментов машинного обучения и их массового использования в кибербезопасности и вооружённых конфликтах в XXI веке.

Действительно, открытые данные представляют собой довольно удобный ресурс не только для оперативно-розыскной, но и уголовно-процессуальной деятельности, поскольку эти данные могут содержать сведения, имеющие существенное значение для оперативно-поисковой или следственной работы.

Одной из бесспорных преимуществ получения информации из открытых источников либо их сбора и анализа является отсутствие необходимости лично встречаться с субъектами, от которых исходит эта информация. OSINT позволяет собирать необходимую информацию удаленно, не покидая своего рабочего места. В этом заключается и оперативность, и экономия, как рабочего времени, так и материальных средств, которые могли бы потребоваться для поездок. Помимо этого, сбор необходимых материалов посредством OSINT обеспечивает определенную конфиденциальность.

Это актуализируется также с учетом того, что в настоящее время некоторые виды преступлений совершаются с использованием информационно телекоммуникационных технологий. К примеру, сбыт и приобретение наркотических средств в условиях современности совершается так называемым бесконтактным способом.

В отчете и исполнительном резюме взаимной оценки Республики Казахстан в рамках второго раунда взаимных оценок ЕАГ, составленном в 2023 году отмечается, что в системе правоохранительных органов республики технология OSINT для поиска необходимой информации не применяется должным образом. Должностные лица органов уголовного преследования продолжают полагаться на традиционные служебные информационные ресурсы, в том числе СИОПСО [21. с. 397].

В данном случае справедливы слова Е. Н. Рахмановой и Е. В. Понамаревой, относительно того, что «взрывной рост технологических инноваций опережает возможности (или готовность) государства понимать, отслеживать и эффективно управлять ими и их негативными последствиями» [22. с. 203].

Применительно к использованию правоохранительными органами Республики Казахстан возможностей OSINT имеет место недооценивание данной технологической инновации.

Для сравнения следует отметить, что в США OSINT стали использовать в период с 2005 по 2009 годы. В этих целях был создан центр по анализу разведывательных материалов из открытых источников информации (Foreign Broadcast Information Service, FBIS).

Как считают западные исследователи, «в настоящее время около восьмидесяти процентов всей разведывательной информации добыто посредством OSINT» [23].

О значении OSINT в правоохранительной деятельности свидетельствует тот факт, что в 2012 году ФАТФ «было рекомендовано использование информации из открытых источников в деле борьбы с легализацией доходов от преступной деятельности» [24. с. 60].

По мнению Б. Д. Еркенова и С. А. Сейлхановой, например, «в процессе противодействия отмыванию (легализации) преступно добытого имущества следует использовать следующие инструменты OSINT:

- ✓ цифровые (онлайн) следы;
- ✓ сканирование мессенджеров;
- ✓ отслеживание транзакций;
- ✓ даркнет-мониторинг;
- ✓ картирование корпоративной сети;
- ✓ инспекция по борьбе с финансированием терроризма;
- ✓ анализ блокчейна» [25. с. 175–183].

К бесспорным преимуществам OSINT следует отнести следующие его свойства:

- полученная информация приближена к реальному времени;

- быстрота доступа к информации;
- возможность легитимного получения сведений;
- ясность источников;
- удобство и простата доступа к информации;
- низкая стоимость.

Таким образом в результате проведенного исследования можно резюмировать, что база открытых данных предоставляет большие возможности по оптимизации не только оперативно-розыскной, но и уголовно-процессуальной деятельности. Использование OSINT в настоящее время представляется не просто одной из возможностей, а настоятельной необходимостью для использования в предотвращении, раскрытии и расследования уголовных правонарушений.

1.2 Законодательная регламентация использования открытых источников данных в уголовно-процессуальном доказывании

Основным законодательным регламентированием использования открытых источников данных в уголовно-процессуальном доказывании является положение части второй ст.111 УПК РК, в котором наряду с иными фактическими данными, имеющими значение для правильного разрешения уголовного дела указываются иные документы.

Согласно ст.120 УПК РК иными документами являются:

- объяснения, акты инвентаризаций, ревизий, справки, акты налоговых проверок, заключения органов налоговой службы, а также материалы, содержащие компьютерную информацию, фото-и киносъемки, звуко- и видеозаписи, полученные, истребованные или представленные в порядке, предусмотренном статьей 122 УПК РК;
- материалы, в которых зафиксированы данные о противоправных действиях, полученные с соблюдением требований законов Республики Казахстан «Об оперативно-розыскной деятельности», «О контрразведывательной деятельности» [26].

Рассмотрим приведенные положения подробнее.

Среди приведенного списка иных документов к открытым данным относится компьютерная информация.

Однако в уголовно-процессуальном, либо в уголовном законодательстве разъяснения того, что понимать под компьютерной информацией нет.

В правовой науке мы обнаружили следующие определения.

В.Е. Пирогов под компьютерной информацией понимает информацию, «представленную в виде кодированных или раскодированных данных, хранящихся на материальных носителях, способных выполнять функции по хранению, обработке, передаче и (или) копировании указанных данных» [27. с. 537-539].

Автор применяет термин «на материальных носителях» не расшифровывая того, что следует под ними понимать.

По мнению Э. Г. Минькашева «компьютерная информация – данные или сведения, находящиеся в памяти компьютерной системы, на любом носителе информации в форме, доступной для обработки посредством компьютерной системы или передачи по информационно-телекоммуникационной сети» [28. с. 283-287].

Указанный автор определяет носитель информации посредством использования обобществленного термина «любой».

Законодательное разъяснение рассматриваемого понятия содержится в Соглашении о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий, совершенном в Душанбе 28 сентября 2018 года, где оно изложено следующим образом: «компьютерная информация - информация, находящаяся в памяти компьютерной системы, на машинных или на иных носителях в форме, доступной восприятию компьютерной системы, или передающаяся по каналам связи» [29].

В данном разъяснении рассматриваемого термина содержится его существенный признак, не освещенный научными дефинициями - это «на машинных или на иных носителях в форме, доступной восприятию компьютерной системы, или передающаяся по каналам связи».

В примечании к ст.272 УК Российской Федерации также закреплено следующее определение: «компьютерная информация – сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи» [30].

Данная дефиниция также не содержит конкретного определения того, в каких непосредственно устройствах может храниться, обрабатываться и передаваться информация.

Е. Р. Россинская и А. И. Усов понятие компьютерной информации разъясняют под уголовно-процессуальным ракурсом: «… это фактические данные, обработанные компьютерной системой и (или) передающиеся по телекоммуникационным каналам, доступные для восприятия человеком, и на основе которых, в определенном законом порядке устанавливаются обстоятельства, имеющие значение для правильного разрешения уголовного или гражданского дела» [31. с.30].

Взгляд с позиции уголовно-процессуального права в данном случае вполне обоснован, поскольку «обстоятельства, подлежащие доказыванию, устанавливаются в определенном законом порядке».

Вместе с тем, в настоящее время, когда наблюдается бурное развитие информационных технологий, информация, именуемая компьютерной, может содержаться не только в самих компьютерах (статичных или переносных). Сегодня на основе двоичной системы комбинации цифр также работают смартфоны (айфоны), которые отлично выполняют функции по хранению,

обработке, копированию и (или) передаче информации. По сути эти устройства представляют собой мини компьютеры.

В этой связи следует признать удачными использование в выше приведенных официальных разъяснениях компьютерной информации такие обороты, как: «на машинных или на иных носителях в форме, доступной восприятию компьютерной системы».

В этой связи справедливы утверждения К. Е. Демина – доцента кафедры оружиеведения и трасологии Московского университета МВД России, которые относят «к источникам компьютерной информации: файлы, листинги (или машинные распечатки), данные на различных электронных накопителях информации («винчестеры», карты систем мобильной идентификации, пластиковые банковские карты, телефонные карты, флеш-карты, элементы памяти в различной социотехнике, миниатюрные персональные электронные инструменты, смартфоны, коммуникаторы и т.д.)» [32. с. 44-47].

С учетом изложенного представляется целесообразным определение компьютерной информации закрепить в ст.7 УПК РК в следующей редакции: «Компьютерная информация – это полученная в установленном законом порядке информация о фактических данных, имеющих существенное значение для правильного разрешения уголовного дела, доступных восприятию компьютерной системой и представленная в форме электрических сигналов, хранящихся, обрабатывающихся и передающихся посредством различных электронных накопителей информации».

Оперативно-розыскная деятельность не является уголовно-процессуальной. Эти два вида деятельности регламентированы самостоятельными законами. Тем не менее, ряд задач оперативно-розыскной деятельности, обозначенных в Законе Республики Казахстан «Об оперативно-розыскной деятельности» от 15 сентября 1994 года, полностью совпадают с задачами уголовно-процессуальной деятельности, закрепленными в ст.8 УПК РК.

Рассмотрение вопроса о законодательной регламентации использования открытых источников данных в уголовно-процессуальном доказывании невозможно без освещения вопросов об использовании в процессе оперативно-розыскной деятельности данных из открытых источников.

Это связано с тем, что материалы, в которых зафиксированы данные о противоправных действиях, полученные с соблюдением требований законов Республики Казахстан «Об оперативно-розыскной деятельности», «О контрразведывательной деятельности» признаются иными документами, то есть доказательствами по уголовному делу.

Добытые таким образом материалы пригодны к использованию не только в уголовно-процессуальном доказывании на различных этапах предварительного расследования.

Они, в соответствии с положениями ст.180 УПК РК могут стать поводом к началу досудебного производства, оформленным в виде рапорта должностного

лица органа уголовного преследования о подготавливаемом, совершаемом или совершенном уголовном правонарушении.

Ввиду того, что оперативно-розыскная деятельность регламентируется самостоятельным законом и, соответственно признается самостоятельным видом правоохранительной деятельности, имеет значение каким образом в Законе Республики Казахстан об ОРД регламентируется использование открытых источников информации.

По большей части оперативно-розыскная деятельность использует негласные методы поиска, обнаружения и фиксации информации, представляющей оперативный интерес. Однако пренебрегать возможностью использования открытых данных было бы нецелесообразно.

Мероприятие по использованию открытых данных ученые предлагают называть «оперативно-розыскным мониторингом».

Например, А. О. Сукманов пишет, что «формой использования открытых источников данных может быть осуществление их оперативно-розыскного мониторинга, что значительным образом повысит эффективность борьбы с преступностью. Оперативно-розыскной мониторинг должен охватывать печатные СМИ и ресурсы глобальной сети Интернет» [33. с. 17-19].

То есть, автор предлагает осуществлять оперативно-розыскной мониторинг открытых данных.

М. М. Сарычев и А. А. Дягилев отмечают, что «в результате оперативно-розыскного мониторинга сети Интернет вполне возможно установление сайтов, которые для взаимосвязи используют преступные группировки. Кроме того, может быть обнаружена криминальная информация, отражающая признаки экстремистской и/или террористической деятельности, а также материалы, относящиеся к распространению наркотиков. Правильно задокументированные результаты оперативно-розыскного мониторинга может быть использованы в уголовно-процессуальном доказывании» [34. с. 151-154].

Представляется, что законодательную регламентацию использования открытых источников данных можно обнаружить в установлении законом Республики Казахстан об ОРД в числе общих оперативно-розыскных мероприятий применение технических средств для получения сведений, не затрагивающих охраняемые законом неприкосновенность частной жизни, жилища, личной и семейной тайны, а также тайну личных вкладов и сбережений, переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений [35].

Отнесение данного мероприятия к использованию открытых данных связано с тем, что они не должны затрагивать охраняемую законами тайны и неприкосновенности.

Закон также содержит разъяснение того, что понимать «под специальными техническими средствами – устройства, аппаратура, приспособления, оборудование, имеющие специальные функции, программное обеспечение и конструктивные особенности для добывания и документирования информации в

ходе проведения оперативно-розыскных мероприятий и негласных следственных действий» [35].

Однако с полной уверенностью можно утверждать, что в данном случае речь не идет о получении только лишь непосредственно компьютерной информации.

В статье 1 закона Республики Казахстан об ОРД, закрепляющей разъяснения основных понятий содержится следующее разъяснение: «Перехват и снятие информации, передаваемой по сетям электрической (телекоммуникационной) связи, - перехват и снятие знаков, сигналов, голосовой информации, письменного текста, изображений, видеоизображений, звуков и другой информации, передающейся по проводной, радио, оптической и другим электромагнитным системам» [35].

Вполне очевидно, что «перехват» не может быть использован для использования информации из открытых источников.

Таким образом получается, что в законе Республики Казахстан об ОРД предусмотрено общее оперативно-розыскное мероприятие по получению данных из открытых источников, но нет регламентации того, каким образом оно должно осуществляться.

Так, например, А. Л. Осипенко считает, что оперативно-розыскной мониторинг информационного пространства есть «комплексной системы наблюдения за состоянием криминальных процессов в сетевой социальной среде, основанной на использовании оперативно-розыскных средств и методов.

В свою очередь, «оперативно-розыскное наблюдение в сетевой социальной среде предполагает сбор, обработку и анализ информации о явлениях криминального плана, которые представляют интерес для оперативно-розыскной деятельности, а также оценку и прогноз изменения состояния оперативной обстановки в сетевом информационном пространстве под воздействием криминогенных факторов» [36. с. 24].

А. О. Сукманов возражая с А. Л. Осипенко, считает, что «в большей степени соответствующим действительности следует определять данное оперативно-розыскное мероприятие в качестве наблюдения за состоянием ресурсов сети Интернет. Это обуславливается тем, что в процессе мониторинга и обнаружения, фиксации информации о криминальных событиях, происходящих в сетевом информационном пространстве, мониторингом должны охватываться все, без исключения, информационные процессы и потоки. Именно при помощи такого мониторинга возможно получение криминалистически значимой информации» [34. с. 17-19].

А. С. Овчинский и К. К. Борзунов подмечают существенный признак оперативно-розыскного мониторинга - «непрерывная обработка потоков фоновой информации о происходящих событиях в целях выявления в них возможного криминального содержания и предпосылок совершения преступлений» [37. с. 182].

Действительно в рамках рассматриваемого оперативно-розыскного мероприятия наблюдение должно быть непрерывным.

Об этом свидетельствует также использование термина «мониторинг», которое, согласно различным словарям, «происходит от лат. monitor - надзирающий, предостерегающий:

1) специально организованное, систематическое наблюдение за состоянием объектов, явлений, процессов с целью их оценки, контроля или прогноза [38];

2) процесс систематического наблюдения, объяснения и предсказания некоторого явления» [39].

С учетом изложенного представляется целесообразным сделать дополнение в статью 1 Закона Республики Казахстан «Об оперативно-розыскной деятельности», в котором изложить разъяснение понятия «оперативно-розыскной мониторинг открытых источников информации» в следующей редакции: «Оперативно-розыскной мониторинг открытых источников информации – это мероприятия по непрерывному наблюдению за информационно-телекоммуникационными сетями и системами в целях обнаружения, сбора и анализа информации об общественно опасных процессах и явлениях, а также за факторами их формирующими и развивающими в целях своевременного пресечения и (или) уголовного преследования».

Таким образом проведенное исследование позволяет заключить, что в настоящее время имеется регламентация использования открытых источников данных, как в уголовно-процессуальном, так и в оперативно-розыскном законодательстве.

Однако состояние указанной выше регламентации имеет некоторые недостатки. Представляется, что восприятие предлагаемых нами путей совершенствования уголовно-процессуального и оперативно-розыскного законодательства положительным образом скажутся на дальнейшем использовании открытых источников данных в уголовно-процессуальном доказывании.

2. Правоприменительная практика по использованию в уголовном процессе открытых источников данных

2.1 Правоприменительная практика по использованию в уголовном процессе открытых источников данных

Использование открытых источников данных, как мы установили ранее, возможно, как в процессе расследования уголовных правонарушений, так и в оперативно-розыскной деятельности.

Причем, на наш взгляд, открытые данные в большей степени применимы в ОРД. Так, на первоначальном этапе эти данные могут привлечь внимание оперативных сотрудников и стать первопричиной выявления преступлений. В последующий период расследования открытые источники данных могут быть использованы для добычи доказательственной информации, устанавливающей причастность привлекаемых к уголовной ответственности лиц к совершению как расследуемых, так и иных преступлений. Кроме того, могут быть установлены и другие лица, являющиеся соучастниками преступлений; может быть установлено преступно нажитое имущество и многие иные обстоятельства, необходимые для правильного разрешения дела.

Законодательную регламентацию использования открытых источников данных можно обнаружить в установлении законом Республики Казахстан об ОРД в числе общих оперативно-розыскных мероприятий посредством применения технических средств для получения сведений, не затрагивающих охраняемые законом неприкосновенность частной жизни, жилища, личной и семейной тайны, а также тайну личных вкладов и сбережений, переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений [35].

Таким образом следует констатировать факт того, что закон Республики Казахстан об ОРД содержит положения о получении данных из открытых источников, которые регламентированы в рамках общих оперативно-розыскных мероприятий.

Для выборки информации, представляющей оперативный интерес, должен осуществляться непрерывный мониторинг таких социальных сетей, как, к примеру, «Вконтакте», «Одноклассники», и других.

Дело в том, что правонарушители, также, как и все их современники, в очень активно используют сети Интернет. При этом они не делают исключений для целей по реализации своих криминальных замыслов. Их деятельность в сети Интернет оставляет соответствующие следы. Поэтому различные социальные сети становится источником открытых данных, которая может представлять оперативный интерес.

Е. В. Битюцкий справедливо замечает, в настоящее время организованные криминальные структуры, «специализирующиеся» на незаконном обороте наркотиков, предпочитают так именуемый «бесконтактный» способ оборота наркотиков. Таковым является использование сети Интернет, а также мобильной

связи, электронных платёжных систем. При этом исключается необходимость личного контакта между участниками незаконного оборота наркотиков [40. 22-26].

В последние годы членами криминальных структур активно используют возможности сети Интернет не только в качестве рекламы и осуществления своей противоправной деятельности, но и для использования взаиморасчетов посредством такого нового финансового инструмента, как криптовалюта.

По причине открытости информации о транзакциях в сети биткойн были разработаны схемы и последовательность действий по привязыванию к определенным кошелькам операций с входными и выходными узлами.

Например, в сети Интернет имеет хождение разработанная последовательность действий, основанная на процессе кластеризации. Посредством такой разработки в результате анализа базы блокчейн объединяется несколько адресов криптовалютных кошельков в единый кластер, принадлежащий одному пользователю [41].

Выполнение указанных функций осуществляется посредство анализа транзакционных сетей в целях нахождения нескольких входов для выполнения одной транзакции. Это способствует решению о едином источнике контроля. Правоохранительные органы и финансовые структуры стали сейчас использовать новый инструмент для изучения биткоин-блокчейна – Crystal, который был разработан компанией Bitfury Group. Инструмент Crystal позволяет подвергать исследованию информационные потоки и транзакции в сети блокчейн на предмет обнаружения подозрительных операций и устанавливать их объекты. В результате использования данного инструмента деанонимизируются отдельные объекты и финансовые взаимоотношения между криминальными личностями [42].

Теперь правоохранительные органы получили возможность в режиме открытого доступа установить конкретное лицо по биткойн-адресу при его любом использовании, как, например, снятие наличных денег, расчет в интернет-магазине, иного использования депозитного счета.

В открытом доступе сети Интернет с применением оперативно-розыскного мониторинга среди огромного массива информации возможно получение сведений о лицах, которые оказываются причастны к противоправной деятельности. Любые сведения полученные таким образом подлежат всесторонней проверке на достоверность.

Количественный объем информации представляется очень важным, поскольку чем больше информации, тем больше фрагментарных элементов данных о событиях или о личности представляемых оперативный интерес можно получить.

К примеру, правоохранителями для проверки информации о причастности подозреваемого лица к конкретному преступлению практикуется проверка email-адреса данного лица посредством следующего ряда действий:

- открывают электронное письмо заподозренного лица, не переходя при этом по вложенным ссылкам;

- для более детального получения информации об этом лице изучают такие параметры, как DMARC, SPF, DKIM [43. с. 5440-5447].

Так, например, видеоролик опубликованный в приложении «Tik-Tok» на своей странице под аккаунтом «666Fast» Гончаровым А.И. с обращением в адрес граждан казахской национальности, в котором публично оскорбил их национальную честь и достоинство стал поводом к возбуждению досудебного производства по признакам преступления, предусмотренного ч.1 ст.174 УК РК.

Указанный ролик был обнаружен сотрудником Управления полиции, который осуществлял мониторинг социальных сетей [44].

Для получения информации, представляющей оперативный интерес, могут быть использованы различные поисковые системы, такие как, например, Яндекс, Google.

Сервис Google предоставляет пользователям возможность своих специальных поисковых систем для осуществления поиска интересующего лица (лиц). Эти поисковые системы предусматривают использование 28 команд. При этом восемь команд из разряда простых, а 16 представляют собой категорию документальных операторов.

Например, можно привести следующие поисковые команды: Site (пример запроса: site:ru.wikipedia.org), Filetype (пример запроса: filetype:pdf), Intext (пример: intext:apple), Allintext (пример запроса: allintext:appleiphone), Related (пример запроса: related:apple.com), Allintitle (пример запроса: allintitle: переклейка фотографии в паспорте; intitle: типографская краска цена 2024), Allintitle.

Тщательный анализ полученной информации, их группировка по отдельным признакам дает возможность выделить данные, имеющие существенное значение для выявления и пресечения противоправной деятельности. Комбинация некоторых значений, сочетание с оператором site некоторых других операторов позволит проверить конкретный ресурс на наличие материалов, представляющих оперативный интерес.

К числу открытых источников данных, которые могут быть использованы для целей раскрытия и расследования преступлений следует также отнести данные информационной системы ГИС. ГИС представляет собой комплекс программ, с помощью которых можно осуществлять сбор и обработку различных изображений, к примеру, участков местности, отдельные сооружения; получать самые точные географические координаты искомого объекта. Причем все эти данные ГИС в режиме реального времени.

«При расследовании преступлений названные технологии могут быть задействованы для отслеживания движения людей и их большого скопления, перемещения транспортных средств, для мониторинга зданий, сооружений и прилегающей территории в режиме реального и прошлого времени. Особая ценность таких разработок заключается в том, что с их помощью возможно

осуществлять сбор информации в любой, даже недоступной точке земли» [45. с. 304-309].

Существенное расширение возможностей правоохранительных органов, связанных с использованием открытых источников данных, обеспечивает утверждение Приказом Председателя Комитета национальной безопасности Республики Казахстан от 27 октября 2020 года «Правил функционирования Национальной системы видеомониторинга», в которых определен порядок функционирования Национальной системы видеомониторинга. Вступление в законную силу данных Правил началось с 1 июля 2021 года.

«Национальная система видеомониторинга - информационная система, представляющая собой совокупность программных и технических средств, осуществляющих сбор, обработку и хранение видеоизображений для решения задач обеспечения национальной безопасности и общественного правопорядка» [46].

Объектами национальной системы видео мониторинга являются:

- системы видеонаблюдения на объектах массового скопления людей;
- внутри дворовые системы видеонаблюдения;
- системы видеонаблюдения на особо важных государственных, стратегических и опасно производственных объектах;
- системы видеонаблюдения дорожной безопасности.

Ожидается, что данные системы видео наблюдений в значительной степени скажутся на продуктивности работы правоохранительных органов, как в плане обеспечения надлежащего общественного порядка, так и в деле раскрытия и расследования уголовных правонарушений.

Информация, снятая системой видео мониторинга, при должно процессуальном оформлении будет служить доказательством по уголовному делу или, как минимум, может быть использована в качестве начальной, ориентирующей информацией для дальнейшего осуществления оперативно-розыскной или уголовно-процессуальной деятельности.

Также ожидаемо, что для налаживания работы указанных систем и получения требуемых результатов, необходимо определенное время.

Основу комплекса указанных систем образуют объекты государственного видеонаблюдения, работу которых будут налаживать соответствующие сотрудники государственных органов. Рассматриваемые системы видео наблюдений будут подключать камеры наблюдений с мест массового скопления людей, особо важных государственных объектов, а также системы видеонаблюдения дорожной безопасности.

На сегодняшний день создана единая информационная платформа видеомониторинга, позволяющая в режиме реального времени управлять системой городского видеонаблюдения, оперативно реагировать на происходящие события, а также реализовать функции распознавания лиц посредством использования современных алгоритмов и нейронных сетей. Функционал межкамерного слежения позволяет следить за передвижением не

только разыскиваемых лиц, а также транспортных средств. В целом, система контролирует дорожное движение, осуществляет поиск "оставленных" предметов, фиксирует нарушения правил парковки и вторжения на охраняемую территорию. Отличительной особенностью является идентификация личности в самых сложных ситуациях. Определяя ключевые признаки лица (пол, возраст), а также наличие различных аксессуаров (очки, борода, маска), данные сопоставляются со списками разыскиваемых лиц, что позволяет оперативно организовать поисковые мероприятия [47].

Таким образом, можно сделать следующий вывод:

- предметом оперативно-розыскного мониторинга открытых источников данных является криминалистически значимая информация;

- оперативно-розыскной мониторинг открытых источников данных осуществляется специально уполномоченными сотрудниками правоохранительных органов;

- оперативно-розыскной мониторинг открытых источников данных следует признать эффективным средством выявления, пресечения и расследования преступлений, который в значительной степени расширяет круг возможностей государственных органов, уполномоченных осуществлять оперативно-розыскную деятельность.

Мониторинг и поиск по открытым источникам данных способствует успешному решению «следующих задач:

– обнаружение определенных лиц и связей между ними, используя в том числе скрытые и удаленные данные, социальные сети;

– поиск различных объектов и событий по географическим координатам;

– мониторинг закрытых преступных сообществ, форумов и маркетплейсов Даркнета;

– анализ контента социальных сетей и веб-страниц;

– анализ операций с криптовалютами» [48. с. 44].

В процессе расследования уголовных дел информация из открытых источников данных извлекается с помощью следственных действий, применяемых при обнаружении, фиксации и изъятии любых иных фактических данных.

Таковыми следственными действиями являются осмотр и выемка.

Выемка в данном случае представляется более сложным процессуальным действием, поскольку требует вынесения следователем постановления в соответствии с требованиями ст.254 УПК РК. Процессуальный порядок выемки электронного носителя зависит от того, у кого производится эта выемка (у провайдера, собственника электронного устройства, с интернет-ресурса и т.д.).

В случаях, когда подлежащие выемке электронные носители содержат информацию о государственных секретах или иную, охраняемую законом тайну, постановление должностного лица органов уголовного преследования должно быть санкционировано следственным судьей.

С. П. Евтеев справедливо полагает, что при проведении выемки электронных носителей информации целесообразно использование помощи специалиста, поскольку в данном случае необходим специализированный объемом знаний в области компьютерной технологии, могущий обеспечить понимание сути проводимого следственного действия [49. с. 42-50].

Данная рекомендация полностью согласуется со следующим нормативным предписанием: «Выемка производится с обязательным применением научно-технических средств хода и результатов, при необходимости могут быть привлечены специалист и переводчик» (ч.4 ст.254 УПК РК).

При обнаружении в сети Интернет информации, представляющей оперативный интерес или которая может быть использована в уголовно-процессуальном доказывании по конкретному уголовному делу производится такое следственное действие, как осмотр. С учетом того, что информация из открытых источников данных, как мы установили ранее, признается документом, то и его осмотр производится по правилам осмотра документа.

Так, например, в приговоре Темиртауского городского суда Карагандинской области от 12 июля 2024 года по делу 3524-24-00-1/87 по обвинению Гончарова А.И. в преступлении, предусмотренном ч.1 ст.174 УК РК основу обвинения помимо прочих составили следующие доказательства, полученные из открытых источников данных:

- протокол осмотра предметов от 8 января 2024 года, в ходе которого обнаружен видеофайл наименованием «2023-12-23-223549867.mp4» от 23 декабря 2023 года, содержимое 41,52 мб 720х1280рх, длительностью 1 минута 9 секунд (л.д. 65-66);

- протокол осмотра видеофайла от 8 января 2024 года, объектом осмотра являлся видеофайл наименованием «2023-12-23-223549867.mp4» от 23 декабря 2023 года, при произведении содержится голосовое видео обращение Гончарова А.И. (л.д. 69) [44].

Указанные данные, полученные из открытых источников были исследованы соответствующими экспертами, которые пришли к следующим выводам:

- заключением эксперта №Э/24/16/1113 от 15 февраля 2024 года, согласно которому в представленном тексте содержатся языковые единицы, выраженные в неприличной форме, крайне негативно характеризующие адресата (адресатов) и носящие оскорбительный характер в отношении чести и достоинства адресата (адресатов), а также содержатся смысловые компоненты «угрозы» в виде причинения вреда здоровью (л.д. 97-106);

- заключением эксперта №Б-188 от 27 марта 2024 года, согласно которому в исследуемом тексте видеоролика содержатся языковые единицы, носящие оскорбительный характер в отношении национальной чести и достоинства (л.д. 88-96);

- заключением эксперта №632 от 2 апреля 2024 года, в выводах которого указано, что голос и речь диктора «М1» с исследуемой фонограммы №1 принадлежат Гончарову А.И. (л.д. 121-124) [44].

По другому уголовному делу, также возбужденному по рапорту оперативного сотрудника, осуществлявшего мониторинг социальных сетей, в отношении гр.Давыдкова Д. Н. по признакам преступлений, предусмотренных частью 1 статьи 174, частью 2 статьи 180 УК РК были проведены осмотры

- протокол от 18 декабря 2023 года дополнительного осмотра предмета, а именно сотового телефона марки «Samsung». Осмотром установлено наличие у Давыдкова Д.Н. аккаунта Дмитрий (@dyaou8zixw1c) в социальной сети «TikTok», имеющего возможность подключения к прямым эфирам других пользователей.

- протокол от 23 января 2024 года осмотра предмета, в ходе которого в браузере «Google Chrome» в ходе осмотра «Google Карты», Давыдков Д.Н. указал место своего расположения 22.08.2023 года в момент подключения к прямому эфиру неизвестного ему пользователя и беседы с ним [50].

В процессе осмотра в следственной практике довольно часто используется скриншоты (англ. screenshot). По своей содержательной составляющей скриншот – это фотографирование объекта. Отличительная особенность скриншота заключается в том, что он осуществляется не самостоятельным техническим устройством в виде фотоаппарата, а самим электронным устройством. Информативностью обладает также тот факт, что не только фиксируется изображение с экрана монитора, но и конкретный момент времени, во время которого совершен скриншот, что, на наш взгляд, повышает его качество в плане достоверности.

Следственной практикой установлено, что «можно выделить несколько видов оформления скриншотов:

1) их нахождение в описательной части протокола осмотра;
2) оформление в качестве фото-таблицы к протоколу осмотра;
3) применение скриншотов как иного приложения к протоколу осмотра» [51. с. 97-101].

Проведение осмотра может также быть обусловлено сложностью изъятия материального носителя информации, содержащей криминальные признаки, в связи с нахождением интернет-ресурса в другом государстве и отсутствием налаженного взаимодействия с правоохранительными органами этих государств.

В таких ситуациях используются возможности информационно-телекоммуникационных сетей и применимые в таких случаях технические средства, которые возможно к ним подключить. Посредством таких технических приспособлений производится копирование выявленной криминалистически значимой информации и сохранение на электронном носителе правоохранительного органа.

В целях сохранения доказательственного значения изымаемой информации требуется строгое соблюдение процессуального порядка

обнаружения, фиксации и изъятия данного материала. «В этих целях осуществляется пошаговое описание последовательности процессуальных действий, а именно:

- фиксирование процесса загрузки операционной системы и браузера;
- технический переход к необходимому адресу;
- переход по ссылкам;
- воспроизведение аудиовизуального материала в онлайн режиме и т.д.

Желательно, чтобы вся указанная процедура сопровождалась видеозаписью» [34. с. 151-154].

По мнению А. Б. Смушкина «методы OSINT пригодны к применению для мониторинга открытой сети или «Телеграм». С помощью этих методов можно обнаружить криминальную информацию относительно первичного поиска клиентов для их вовлечения в криминальный бизнес» [52. с. 103].

«Известен случай, когда был осуществлен поиск в Интернет-сети в связи с жалобой гражданина на размещение в телеграмм-канале клеветнической информации о нем. В целях подтверждения информации, содержащейся в жалобе, произведен осмотр публикаций, находящихся в мессенджере «Telegram» по конкретному адресу сети Интернет. Использовано специальное приложение «Telegram» для перехода по указанной ссылке, где обнаружена Телеграмм-группа с большим количеством участников. При поиске информации под известным названием была указана дата ее создания. Была установлена искомая публикация, которая была размещена пользователем с конкретным ник-нейм с указанием даты размещения. Произведено копирование обнаруженного текста, которая была приложена к акту осмотра с указанием даты» [53. с. 131-136].

В уголовно-процессуальной литературе в настоящее время обсуждается вопрос о проведении обыска с использованием возможностей открытых источников данных. По мнению ряда ученых-процессуалистов, возможность осуществления всех вышеуказанных мероприятия в открытом доступе Интернет-ресурсов предоставляет правоохранителям возможность обойтись без судебного санкционирования обыска или осмотра.

К. Ю. Яковлева полагает, что «такая форма проведения обыска, при которой используются технологии OSINT, не противоречит уголовно-процессуальному законодательству. Метом проведения данного следственного действия будет место нахождение электронной информации. Это обстоятельство значительно повышает эффективность следственного действия так как сужение места обыска четко определяет его цели по поиску материалов, имеющих доказательственное значение, поскольку этот поиск будет сосредоточен непосредственно в Интернет ресурсах» [53. с. 131-136].

При составлении протокола такого обыска, по мнению ученых-процессуалистов, место производства должно соответствовать адресу страницы сайта сети Интернет либо автоматизированному рабочему месту лица, осуществляющего данного следственное действие.

Процедура обыска должна фиксироваться с самого начала до окончания техническими средствами фиксации.

Обыск, проведенный с помощью технология OSINT позволяет установлении связи лица с данными, к примеру, текстовые материалы, аудио-видеороликами, которые это лицо разместило в сети Интернет.

В процессе проведения обыска для ориентирования места размещения интересуемой информации рекомендуется обозначение элементов связи электронной почты, номера телефона пользователя и страниц сети Интернет. Такой обыск может охватить сразу несколько страниц сети Интернет.

Использование открытых источников данных может быть и в целях розыска и задержания подозреваемых и обвиняемых в совершении преступлений. В настоящее время довольно большой объем информации содержится в различных видеозаписывающих устройствах, которыми оснащены подъезды многоквартирных домов, их дворы, квартиры, участки дорог, местности и т.д. Большинство автолюбителей оснащают свои транспортные средства камерами видеонаблюдения. Эти общедоступные ресурсы в отдельных случаях могут предоставить очень ценную информацию о лицах, объявленных в розыск.

Причем распознавание разыскиваемых лиц может быть по признакам внешности, особенностям телосложения, жестов или биометрических данных. Применение указанных технологий помогает вычленить необходимый материал из всего массива, что в значительной степени оптимизирует саму поисковую работы, а также его результаты.

Ю. В. Найденышев и Н. А. Завьялова выделяет повышенное качество фактических данных в виде видеозаписей. По их словам, «в отличие от показаний потерпевших и свидетелей, которые являются наиболее распространенным видом доказательств по уголовным делам, видеозаписи не подвержены видоизменяющему воздействию человеческого сознания, отвечают требованиям объективности при оценке фактических обстоятельств дела» [54. с. 11].

В этом отношении показателен пример использования распознавания лиц по видеоизображению в Китайской Народной Республике.

Как пишут А. П. Перетолчин и А. Ю. Афанасьев, «в Китайской Народной Республике на протяжении длительного времени развиваются системы распознавания граждан с использованием систем видеонаблюдения, установленных в общественных местах (как положительные примеры можно привести случай задержания в 2018 г. мужчины, находившегося в федеральном розыске за тяжкое преступление на концерте среди 70 тыс. зрителей, а так же задержание в 2019 г. 25 разыскиваемых преступников на пивном фестивале в Чиндао, когда камеры уличного видеонаблюдения распознали их лица)» [55. с. 225].

Ученые описывают случай, наблюдавшийся в КНР в 2019 году и хорошо иллюстрирующий вышеуказанное. В городе Шэньчжэнь произошло

исчезновение трехлетней девочки, заявление о котором было сделано ее родителями. В базу данных сразу же была размещена фотография девочки. Для обработки нейросетями имеющихся данных, зафиксированных уличными камерами, потребовалось всего пятнадцать минут. Была осуществлена идентификация ребенка, находящегося в распоряжении у неизвестной женщины. Нейросеть мгновенно идентифицировало личность этой женщины. Сотрудникам правоохранительных органов не составило труда определить место нахождение этой женщины. Было произведено задержание похитительницы. В конечном итоге поиск, обнаружение и возвращение ребенка родителям по времени занял всего 15 часов.

Довольно показательным является пример, когда в 2018 году в Российской Федерации во время проведения чемпионата мира по футболу была использована система FindFace SDK, позволяющая распознавать лица вне зависимости от места их пребывания в условиях скопления большого количества людей. С помощью указанной системы произведено задержание более 180 правонарушителей. В 2019 году в Татарстане с использованием системы FindFace SDK были обнаружены и задержаны 11 лиц, находящихся в розыске [56. с. 62-65].

Не редки случаи, когда уголовное правонарушение оказывается запечатленным камерами видеонаблюдения. Это происходит, когда уголовные правонарушения совершаются в общественных местах, или местах, оснащенных камерами видеонаблюдения. В таких случаях удается установить виновников преступления либо установить круг лиц, причастных к правонарушению (к примеру, когда можно установить определенный круг лиц, посещавших данное место).

Причем такая информация может быть полезна не только в дела розыска скрывшихся подозреваемых или обвиняемых. Розыск может быть связан с расследованием без вести пропавшего лица.

В этой связи в процессе расследования уголовных дел по поиску без вести пропавших лиц (а также и подозреваемых и обвиняемых) возможно налаживание так называемой «обратной связи», при которой органы расследования не только собирают информационный материал по делу, но и привлекают к поиску большее количество граждан и их объединений посредством размещения в открытых источниках данных собственной поисковой информации.

Следует отметить, что правоохранительные органы Республики Казахстан уже оценили по достоинству указанное обстоятельство. МВД республики запустили страницу «ВКонтакте».

Так, по словам официального представителя ДП города Алматы Салтанат Азирбек, «страница будет постоянно обновляться по мере поступления из служб и подразделений Департамента сведений по розыску лиц. Информация предусматривает наличие фотографии человека, набор его анкетных данных, дату, время место и обстоятельства исчезновения. Кроме того, отражаются сведения о внешних отличительных признаках, одежде разыскиваемого лица.

Непременно указываются контакты должностных лиц, в чьем производстве находится розыскное дело и куда граждане могут сообщить имеющуюся у них информацию.

Наши намерения – вовлечь в разыскную работу как можно более широкий круг аудитории. В этих целях использование социальных сетей актуально, так как она представляется довольно популярным и интенсивно используемым средством массовой информации. Социальная сеть позволяет расширить географию поиска без вести пропавших и преступников. Уверены, что людей с активной гражданской позицией в нашем обществе преобладающее большинство, и любую информацию по фактам они будут своевременно нам сообщать» [57].

Таким образом, проведенное исследование позволяет заключить, что использование открытых источников данных и технологии OSINT в значительной степени повышает эффективность, как оперативно-розыскной деятельностью по выявлению, раскрытию и пресечению преступлений, так и по предварительного расследования.

Причем в уголовно-процессуальной деятельности использование открытых источников данных возможно посредством проведения соответствующих следственных действий, акцент в которых должен делаться на описательной и удостоверительной составляющей их процессуального оформления. Полученные данные из открытых источников могут быть исследованы соответствующими экспертами для дачи заключений, как по подлинности (например, принадлежности голоса конкретному лицу), так и по содержанию (например, могущих оказать психологическое воздействие, следует ли текст отнести к пропаганде наркотиков или к экстремистским и т.д.)

С учетом специфики проведения осмотра, выемки, обыска и иных следственных действий целесообразна разработка криминалистической наукой соответствующих алгоритма действий, которые будут способствовать повышению доказательственного значения собираемой информации.

2.2 Проблемные вопросы, связанные с использованием в уголовном процессе открытых источников данных

Как мы установили в предыдущем подразделе информация, полученная из открытых источников данных, может быть признана доказательством по уголовному делу и отнесена к категории документов.

Данная информация может быть получена сотрудниками правоохранительных органов, осуществляющих оперативно-розыскную деятельность для целей уголовного процесса, а также непосредственно в процессе досудебного расследования лицом уполномоченным на ее осуществление.

Информация, имеющая существенное значение для установления обстоятельств совершенного преступления, может быть извлечена из открытых

источников данных с помощью различных следственных действий. Наиболее применимыми в данных случаях являются такие следственные действия, как осмотр, обыск, выемка. По полученным данным может быть назначение и проведение определенной экспертизы для установления различных вопросов, например, наличия или отсутствия следов монтажа, принадлежность голоса определенному лицу и т.д.

В связи с появлением в уголовно-процессуальном доказывании такого нового вида доказательств в виде документов, извлеченных из открытых источников данных, возникают некоторые проблемы, требующие своего разрешения.

Первая проблема не отличается особой уникальностью, поскольку она распространяется на все виды фактических данных, используемых в уголовном процессе в качестве доказательств.

Как известно, любое доказательство должно соответствовать установленным уголовно-процессуальным законом критериям – это допустимость, относимость и достоверность.

Доказательство признается относящимся к делу, если оно представляет собой фактические данные, которые подтверждают, опровергают или ставят под сомнение выводы о существовании обстоятельств, имеющих значение для данного дела (ч.3 ст.125 УПК РК).

Доказательство признается допустимым, если оно получено в порядке, установленном настоящим Кодексом (ч.4 ст.125 УПК РК).

Доказательство признается достоверным, если в результате проверки выясняется, что оно соответствует действительности (ч.5 ст.125 УПК РК).

К примеру, «по одному уголовному делу, лицо, привлекаемое к уголовной ответственности за угрозу убийством, главным подтверждением вины обвиняемого являлся скриншот. Суд первой инстанции отклонил данное доказательство ссылаясь на то, что следователем были допущены процессуальные нарушения. Эти нарушения заключались в том, что не было произведено осмотра источника получения скриншота, а также отсутствует постановление о приобщении к уголовному делу данного осмотра. Однако такое заключение суда первой инстанции было опровергнуто судом апелляционной инстанции. Суд апелляционной инстанции посчитал достаточным указание следователем социальной сети, являющейся активной до настоящего времени. Поэтому нет оснований для исключения скриншота из списка доказательств по делу»[58].

Несмотря на то, что в данном случае апелляционная инстанция признала скриншот имеющим силы доказательства, по нашему мнению, введение в уголовное дело данного документа должно было проведено с соблюдением предписаний уголовно-процессуального законодательства, то есть посредством фиксации факта обнаружения, а затем способа фиксации и изъятия.

По мнению А.А. Наумова и Е.Г. Шихановой «довольно часто в основу обвинительного приговора в числе иных доказательств берутся переписки

«Вконтакте», доказывающие факт приготовления к преступлению. Из этого следует заключить, что скриншоты имеют дальнейшую перспективу на использование их в уголовном дела в качестве доказательств…хотя существует пробел в законодательстве» [51. с. 97-101].

Иными словами, процесс собирания фактических данных, заключенных в открытых источниках данных, также, как и при собирании любых иных доказательств, требует четкого соблюдения установленного уголовно-процессуальным законом порядка.

Однако, если на основании опыта следственной практики, складывающейся на протяжении многих десятков лет, криминалистическая наука вооружила работников следственных подразделений рекомендациями по наиболее эффективным способам обнаружения, фиксации и изъятии фактических данных по самым различным видам преступлений и при самых различных ситуациях их обнаружения, то относительно собирания доказательств, содержащихся в открытых источниках данных, на сегодняшний день рекомендаций нет.

К примеру, такие открытые источники данных, как данные, публикуемые в газетах, журналах, передаваемые радио или телевидением, существуют давно и поэтому выборка необходимой информации не представлял особых сложностей ввиду того, что эта информация содержалась на бумажном носителе (радио и телевидение также могли представить свои данные на бумажном носителе).

В настоящее время подавляющее большинство открытых источников данных содержатся в сети Интернет либо на каких-либо электронных носителях. Современная действительность отличается оцифрованностью информационных ресурсов.

В связи с изложенным разрешение указанной проблемы представляется в разработке рекомендаций в форме алгоритма действий по обнаружению, фиксации и изъятию информации, содержащейся в открытых источниках данных.

Вторая проблема связана с тем, что в уголовно-процессуальном законодательстве действительно имеется пробел в части определения статуса фактических данных, содержащихся на материальных носителях информации, поскольку информация из открытых источников данных содержится в каких-либо электронных носителях информации (компьютер, телефон, флешка, банковская карта и т.д.), обнаруживается и изымается в процессе расследования уголовного дела. Поэтому важно определить процессуальный статус этих носителей.

В уголовно-процессуальной литературе идут дискуссии по поводу отнесения информации на материальных носителях к вещественным доказательствам или к документам.

К примеру, П.С. Пастухов и Л.В. Головко предлагают «электронные носители причислять к одной из разновидностей вещественных доказательств или, как минимум, документов» [59. с.17].

Ряд ученых предлагают разрешить указанную дилемму путем введения в уголовно-процессуальное право понятия «электронные доказательства» [60. с.76].

Мы полностью солидарны с авторами, которые пишут следующее.

Отнесение электронных носителей к числу вещественных доказательств или документов должно быть с учетом качества содержащейся в нем информации, что и должно определять его место в совокупности доказательств по определенному уголовному делу. При условии, когда электронный носитель рассматривается в качестве объекта материального мира, его следует признавать вещественным доказательством [61. с. 154]. В тех случаях, когда ценность заключается в информации, хранящейся в электронном носителе, то его следует относить к «иным документам» [62. с. 196-197].

Следует отметить, что в ГПК РК в отличие от УПК РК имеется нормативное закрепление обсуждаемого понятия.

Так, в ст.99 ГПК РК, именуемой, как «Доказательства на материальных носителях информации», закреплено следующее:

«1. Доказательства могут быть представлены на материальных носителях информации, содержащих: аудио-, видеозаписи, в том числе полученные приборами наблюдения и фиксации, материалы фото- и киносъемки и другие материалы на электронных и цифровых носителях, имеющих значение для дела и отвечающих критериям относимости и допустимости.

2. Лицо, представляющее доказательства на материальных носителях или заявившее ходатайство об оказании содействия в их истребовании, обязано указать, когда, кем, в каких условиях и при каких обстоятельствах осуществлены записи.

Несообщение лицом указанных сведений исключает возможность исследования в судебном заседании таких доказательств» [63].

УПК РК лишь содержит разъяснение понятия электронного документа. Так, согласно п.15) ст.7 УПК РК «электронный документ – документ, в котором информация предоставлена в электронно-цифровой форме и удостоверена посредством электронной цифровой подписи» [26].

Однако данное определение недостаточно для определения правового режима материальных носителей электронной информации.

По этому поводу К. В. Обидин пишет, что «отсутствие законодательного установления понятия «электронные носители информации» приводит к противоречивой практике. К примеру, в рамках одного уголовного дела изымается ноутбук в качестве электронного носителя информации, по другому уголовному делу таковым признается и подлежит выемке только жесткий диск. В последнем случае следователь не копирует информацию, полагая, что

произведено изъятия предмета – ноутбука, а не выемку электронных носителей информации» [64. с.201].

В законе Республики Казахстан «Об информатизации» от 24 ноября 2015 года содержится следующее разъяснение: «электронный носитель – материальный носитель, предназначенный для хранения информации в электронной форме, а также записи или ее воспроизведения с помощью технических средств» [13].

Приведенные нами нормативные определения электронного документа и электронных носителей не отражают значение и сущность этих объектов непосредственно для целей уголовно-процессуального расследования.

Следует отметить, что термины «материальные носители» и «электронные носители» по своей сути идентичны, так как электронный носитель есть материальный объект окружающего мира.

Вместе с тем следует отметить, что электронный носитель сам по себе представляется овеществленным предметом окружающего мира, а в нем может содержаться информация, заключенная в электронном документе.

Представляется целесообразным, использую основу нормативных разъяснений, дополнить статью 7 УПК РК пунктом 59) в следующей редакции: «электронный носитель информации - материальный носитель, предназначенный для записи, воспроизведения и хранения информации в форме электронного документа, имеющего значения для правильного разрешения уголовного дела»

Следующая проблема, связанные с использованием в уголовном процессе открытых источников данных, заключается в способности лиц, уполномоченных на осуществление оперативно-розыскной деятельности и лиц, осуществляющих досудебное производство по уголовным делам, пользоваться имеющимися техническими инструментами и эффективно исследовать открытые источники данных и извлекать из нее необходимую информацию.

В настоящее время буквально все граждане Республики Казахстан являются активными пользователями сети Интернет. Многие граждане создают персональные страницы в социальных сетях и общаются между собой посредством электронной почты, различных мессенджеров, приложений VoIP (интернет-телефонии — Skype, ICQ, Viber, WhatsApp, Telegram и др.).

Например, в Республике Казахстан в ТОР 10 входят такие социальные сети, как ВКонтакте, Одноклассники, Мой мир, Киви, Центр тяжести, Блоггер, Лайвинтернет, Youtube, Facebook, Википедия на платформе которых размещается миллионы самых различных материалов, миллионы людей входят во взаимоотношения между собой, обмениваются определенными символами и т.д.

Для общения в социальных сетях не существует ограничений по времени суток, по государственным границам, ни по возрастной категории, ни в количестве общающихся лиц. Это обстоятельство можно было бы расценить как

показатель всеобщей грамотности в части использования сети Интернет и электронно-технических устройств связи.

Однако это не так. Особенно это оказывается неприятным фактом в отношении сотрудников правоохранительных органов.

«По результатам исследования поиска информации в Интернете, проведенного В. И. Шаровым, в 75,0% случаев необходимые сведения находилась лишь частично. Причины неудач поиска информации опрашиваемые назвали разнообразные, но доминируют все же следующие ответы: «из-за отсутствия доступа к нужным сайтам и базам данных» — 63,6%, «нет методики поиска» - 22,7%, «необходимо использовать специальное программное обеспечение» - 13,6%. Это показывает, что оперативные сотрудники в основном еще с трудом представляют возможности Интернета по получению оперативно значимой информации» [65. с. 113].

Опрос, проведенный среди сотрудников оперативных подразделений Е. В. Буряковым, показал, что большинство из них не до конца понимают даже саму суть получения компьютерной информации [66. с. 29-32].

Поэтому мы солидарны с мнением С. В. Баженова, который пишет, что «для доступа к сведениям необходима помощь специалиста (преодоление технических или программных средств защиты, получение метаданных, пр.), а также использование специальной техники и (или) специальных программ оперативно-техническими подразделениями» [67. с. 32].

В результате следует констатировать факт того, что многие сотрудники правоохранительных органов не имеют возможности в полной мере воспользоваться предоставленными им полномочием по поиску, отысканию и изъятию информации, представляющий оперативный или следственный интерес в открытых источниках данных. Они не могут выбрать необходимый инструментарий для поиска и получения доступа к необходимым сведениям. Все это приводит к тому, что наиболее информативное поле современности остается не использованным для целей уголовного процесса.

Выходом из создавшейся ситуации представляются положения статьи 80 УПК РК, в соответствии с которыми в необходимых случаях следователи вправе использовать помощь лица, обладающего специальными познаниями в определенной области.

Применительно к оперативно-розыскной деятельности аналогичного нормативного положения, к сожалению, нет.

С. А. Давиденко, исследуя данный вопрос, выделяет следующие основные проблемы, которые возникают у оперативных сотрудников по вопросам «информационного обеспечения:

- отсутствие единого программного обеспечения;
- не полное оснащение техникой подразделений и служб;
- отсутствие ежедневного обновления и добавления полученной информации в базы данных» [68. с. 20-22].

Для повышения эффективности оперативно-розыскного мониторинга открытых источников данных, на наш взгляд, требуется разработка инструкции по эксплуатации соответствующего инструментария, который бы могли воспользоваться сотрудники оперативных подразделений. Более того, разработанная инструкция должна быть оснащена техническими устройствами по постоянному обновлению информации. Помимо этого, должен быть налажен контроль за надлежащим использованием и пополнением базы данных.

Это обусловлено тем, что платформа информационных систем очень сложная и требует наличия узкой специализации для эффективного его использования. Кроме того, эта система характеризуется большой динамичностью, обусловленной бурным развитием науки этой отрасли. Все это, безусловно, требует постоянного совершенствования даже для тех лиц, которые специализируются на работе с информационными системами.

В настоящее время большинство людей оставляют свои виртуальные следы в информационных системах. Но есть категория лиц (в основном пожилые или малолетние лица), которые не оставляют виртуальных следов.

Однако современная действительность сводит указанное обстоятельство к минимуму. Это обусловлено тем, что современный окружающий человека мир «нашпигован» всевозможными техническими устройствами, ведущими видеозаписи. В этой связи вне зависимости от воли человека данные об этом лице все получают свои виртуальные следы в виде запечатления в таких, как

- в системе операторов сотовой связи, так как в настоящее время телефоном сотовой связи обладает каждый человек;

- технических базах данных операторов сотовой связи, где фиксируются конкретные телефонные аппараты и определяется место расположение абонента;

- базах видеозаписей камер наружного наблюдения, которые находятся повсюду: на вокзалах, супермаркетах, дворах многоквартирных домов, различных государственных и негосударственных учреждениях и т.д.;

- в базах информационных систем учреждений, оказывающих транспортные услуги - это данные о приобретении конкретным лицом проездных документов на самолет, поезд, автобусы;

- базах информационных систем банка, где отражаются сведения о различных операциях с денежными средствами (получение, вклад, перевод, обмен валют и т.д.);

- базах информационных систем учреждений, оказывающих услуги по вызову такси.

Обнаруженная в указанных источниках открытых данных информация позволит оперативным сотрудникам:

- определить место расположение абонента сотовой связи что, в свою очередь, позволит предположить возможные варианты его дальнейшего маршрута движения, а также предположить о его психологическом состоянии;

- в некоторых ситуациях обнаружить связь между лицом и определенными известными событиями и установлению примерного круга свидетелей этих событий;

- определить круг интересов искомого лица, а также установить круг его общения.

На основании изложенного представляется целесообразным дополнить часть 1 ст.14-1 закона Республики Казахстан «Об оперативно-розыскной деятельности» текстом следующего содержания: «В необходимых случаях использование информационных систем может осуществляться с привлечением специалиста».

Проведенное исследование устанавливает необходимость:

- разработки рекомендаций в форме алгоритма действий по проведению оперативно-розыскного поиска по открытым источникам данных, как в процессе общего мониторинга, так и по поиску конкретных подозреваемых, обвиняемых, либо похищенного имущества;

- разработки инструкции по эксплуатации информационных инструментов в целях эффективного использования современных информационных систем сотрудниками оперативных подразделений правоохранительных органов.

ЗАКЛЮЧЕНИЕ

В результате проведенного исследования вопроса об открытых источниках данных как инструментов сбора информации на первоначальном этапе расследования нами установлено нижеследующее.

1. На основе анализа существующих в настоящее время научных толкований можно вычленить наиболее характерные следующие признаки открытых данных:

- они являются информацией, не имеющей каких-либо запретов или ограничений для доступа к ней и ее последующей републикации;
- они не защищены действием авторского права, лицензий, патентов и иных правовых способов ограничений доступа;
- закон не запрещает их повторное использование;
- они обнародуют деятельность государственных органов и органов местного самоуправления, а также распространяют итоговые сведения по деятельности информационно-аналитических организаций;
- закон не предусматривает внесение платы за пользование ими;
- они размещены в машиночитаемом формате.

В Республике Казахстан сферу открытых данных и права доступа к ним, регулирует целый комплекс нормативных актов, основным из которых является Закон Республики Казахстан от 16 ноября 2015 года «О доступе к информации».

Полное и детализировано содержание открытых данных представлено в предлагаемой нами схеме.

Широкое распространение открытых данных способствовало возникновению определенной деятельности, связанной с их использованием. Так, например, в настоящее время появилась аббревиатура «OSINT», которая расшифровывается как Open-source intelligence, то есть разведка по открытым источникам. OSINT представляет собой сбор и анализ информации, полученной из разных общедоступных информационных каналов.

База открытых данных предоставляет большие возможности по оптимизации не только оперативно-розыскной, но и уголовно-процессуальной деятельности. Использование OSINT в настоящее время представляется не просто одной из возможностей, а настоятельной необходимостью для использования в предотвращении, раскрытии и расследования уголовных правонарушений.

2. Основным законодательным регламентированием использования открытых источников данных в уголовно-процессуальном доказывании является положение части второй ст.111 УПК РК, в котором наряду с иными фактическими данными, имеющими значение для правильного разрешения уголовного дела указываются иные документы.

Среди приведенного списка иных документов в статье 120 УПК РК к открытым данным относится компьютерная информация.

Однако в уголовно-процессуальном, либо в уголовном законодательстве разъяснения того, что понимать под компьютерной информацией нет. Официальное разъяснение рассматриваемого понятия мы обнаружили в Соглашении о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий, совершенном в Душанбе 28 сентября 2018 года. В данном определении имеется существенный признак, отличающий его от существующих теоретических дефиниций – это «на машинных или на иных носителях в форме, доступной восприятию компьютерной системы, или передающаяся по каналам связи».

В настоящее время, когда наблюдается бурное развитие информационных технологий, информация, именуемая компьютерной, может содержаться не только в самих компьютерах (статичных или переносных). Сегодня на основе двоичной системы комбинации цифр также работают смартфоны (айфоны), которые отлично выполняют функции по хранению, обработке, копированию и (или) передаче информации. По сути эти устройства представляют собой мини компьютеры.

Это обстоятельство обуславливает необходимость нормативного определения понятия «компьютерная информация».

Ввиду того, что оперативно-розыскная деятельность регламентируется самостоятельным законом и, соответственно признается самостоятельным видом правоохранительной деятельности, имеет значение каким образом в Законе Республики Казахстан об ОРД регламентируется использование открытых источников информации.

Мероприятие по использованию открытых данных ученые предлагают называть «оперативно-розыскным мониторингом».

Нами установлено, что в законе Республики Казахстан об ОРД предусмотрено общее оперативно-розыскное мероприятие по получению данных из открытых источников, но нет регламентации того, каким образом оно должно осуществляться.

3. В открытых источниках сети Интернет при оперативно-розыскном мониторинге содержащейся в ней информации обнаруживается большое количество данных в отношении лиц, которые могут иметь отношение к совершению преступлений.

Таким образом, можно сделать следующий вывод:

- предметом оперативно-розыскного мониторинга открытых источников данных является криминалистически значимая информация;

- оперативно-розыскной мониторинг открытых источников данных осуществляется специально уполномоченными сотрудниками правоохранительных органов;

- оперативно-розыскной мониторинг открытых источников данных следует признать эффективным средством выявления, пресечения и расследования преступлений, который в значительной степени расширяет круг

возможностей государственных органов, уполномоченных осуществлять оперативно-розыскную деятельность.

В процессе расследования уголовных дел информация из открытых источников данных извлекается с помощью следственных действий, применяемых при обнаружении, фиксации и изъятии любых иных фактических данных. Таковыми следственными действиями, к примеру, являются осмотр, обыск и выемка.

В уголовно-процессуальной деятельности использование открытых источников данных возможно посредством проведения соответствующих следственных действий, акцент в которых должен делаться на описательной и удостоверительной составляющей их процессуального оформления. Полученные данные из открытых источников могут быть исследованы соответствующими экспертами для дачи заключений, как по подлинности (например, принадлежности голоса конкретному лицу), так и по содержанию (например, могущих оказать психологическое воздействие, следует ли текст отнести к пропаганде наркотиков или к экстремистским и т.д.)

4. В связи с появлением в уголовно-процессуальном доказывании такого нового вида доказательств в виде документов, извлеченных из открытых источников данных, возникают некоторые проблемы, требующие своего разрешения.

Так, в уголовно-процессуальном законодательстве имеется пробел в части определения статуса фактических данных, содержащихся на материальных носителях информации, поскольку информация из открытых источников данных содержится в каких-либо электронных носителях информации (компьютер, телефон, флешка, банковская карта и т.д.), обнаруживается и изымается в процессе расследования уголовного дела. Поэтому важно определить процессуальный статус этих носителей.

Вместе с тем следует отметить, что электронный носитель сам по себе представляется овеществленным предметом окружающего мира, а в нем может содержаться информация, заключенная в электронном документе.

Следующая проблема, связанные с использованием в уголовном процессе открытых источников данных, заключается в способности лиц, уполномоченных на осуществление оперативно-розыскной деятельности и лиц, осуществляющих досудебное производство по уголовным делам, пользоваться имеющимися техническими инструментами и эффективно исследовать открытые источники данных и извлекать из нее необходимую информацию.

Следует констатировать факт того, что многие сотрудники правоохранительных органов не имеют возможности в полной мере воспользоваться предоставленными им полномочием по поиску, отысканию и изъятию информации, представляющий оперативный или следственный интерес в открытых источниках данных. Они не могут выбрать необходимый инструментарий для поиска и получения доступа к необходимым сведениям. Все

это приводит к тому, что наиболее информативное поле современности остается не использованным для целей уголовного процесса.

В результате проведенного исследования нами сформулированы следующие выводы:

1. Поскольку Закон Республики Казахстан «О доступе к информации» занимает ключевое положение в сфере регулирования открытых источников данных, представляется обоснованным пересмотреть содержащуюся в нем дефиницию информации с учетом положений Модельного закона об информатизации, информации и защите информации (2005 г.). В этой связи предлагается пункт 1) статьи 1 указанного Закона изложить в следующей редакции: информация — это сведения либо данные, касающиеся лиц, объектов, фактов, событий, явлений или процессов, зафиксированные в любой форме.

2. Целесообразным видится нормативное закрепление термина «компьютерная информация» в статье 7 Уголовно-процессуального кодекса Республики Казахстан. В предлагаемой редакции он может быть сформулирован следующим образом: «Компьютерная информация — это полученные в рамках закона сведения о фактических обстоятельствах, имеющих значение для разрешения уголовного дела, воспринимаемые компьютерными средствами и выраженные в виде электрических импульсов, которые могут храниться, обрабатываться и передаваться с помощью различных электронных носителей данных».

3. В целях совершенствования правовой регламентации, целесообразно внести следующие изменения в Закон Республики Казахстан «Об оперативно-розыскной деятельности»:

— внести дополнение в статью 1, включив определение термина «оперативно-розыскной мониторинг открытых источников информации» в следующей формулировке: *«Оперативно-розыскной мониторинг открытых источников информации представляет собой непрерывный процесс наблюдения за информационно-телекоммуникационными ресурсами с целью выявления, сбора и анализа сведений о потенциально опасных для общества явлениях и процессах, а также об условиях, способствующих их возникновению и развитию, в целях их оперативного предотвращения либо последующего уголовного преследования»;*

— дополнить часть 1 статьи 14-1 следующим положением: *«При необходимости, в процесс использования информационных систем может быть привлечён специалист, обладающий соответствующими знаниями и навыками».*

4. Обоснованным представляется внесение в статью 7 Уголовно-процессуального кодекса Республики Казахстан нового пункта 59), изложенного в следующей редакции: *«Электронный носитель информации – это физический объект, предназначенный для записи, хранения и воспроизведения данных в форме электронного документа, имеющего значение для объективного и законного разрешения уголовного дела».*

5. Полученные в ходе анализа результаты свидетельствуют о необходимости следующих мер:

— подготовка алгоритма, регламентирующего порядок проведения оперативно-розыскного мониторинга открытых источников как в рамках общего наблюдения, так и при целенаправленном поиске конкретных лиц (подозреваемых, обвиняемых) либо утраченного имущества;

— разработка инструктивных положений, регулирующих порядок эксплуатации современных цифровых инструментов, с целью повышения эффективности их применения сотрудниками оперативных подразделений правоохранительных органов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Влезько Д.А. Содержание первоначального этапа расследования преступлений // В сб.: Научное обеспечение агропромышленного комплекса. Сб. статей по материалам 71-й науч.-практ. конф. преподавателей по итогам НИР за 2015 год. Отв. за вып. А. Г. Кощаев. 2016. с. 362–363.
2 Токаев К.-Ж.К. Единство народа и системные реформы – прочная основа процветания страны: Послание народу Казахстана от 1 сентября 2021 года. [Электронный ресурс] - Режим доступа: https://www.akorda.kz/ru/poslanie-glavy-gosudarstva-kasym-zhomarta-tokaeva-narodu-kazahstana-183048 (дата обращения: 15.10.2024).
3 Дарменова А. С., Мамыкова Ж. Д., Андерсен К. Н. Открытые данные: двадцатипятилетняя история развития // Вестник НГУЭУ. 2002. № 2. с. 183–197.
4 Открытые данные, материал из Википедии — свободной энциклопедии [Электронный ресурс] - Режим доступа: https://ru.wikipedia.org/wiki/Открытые_данные (дата обращения: 06.10.2024).
5 Международной хартии открытых данных [Электронный ресурс] - Режим доступа: http://opendatacharter.net (дата обращения: 06.10.2024).
6 Панюкова С.А. Роль открытых данных в развитии журналистики данных // Знак: проблемное поле медиаобразования. 2015. - № 1 (15). - С. 25–33.
7 Transparency and Open Government memorandum. 2009. The White House. [Электронный ресурс] - Режим доступа: https://obamawhitehouse.archives.gov/the-press-office/transparency-and-open-government (дата обращения: 15.10.2024).
8 Open Government Directive. December 8, 2009. [Электронный ресурс] - Режим доступа: https://obamawhitehouse.archives.gov/open/documents/open-government-directive (дата обращения: 15.10.2024).
9 Guidelines on Open Government Data for Citizen Engagement. United Nations, Department of Economic and Social Affairs, Division for Public Administration and Development Management. 2013. [Электронный ресурс] - Режим доступа: https://digitallibrary.un.org/record/3907402/files/OpenGovtData.pdf?ln=en (дата обращения: 15.10.2024).
10 Международной хартии открытых данных [Электронный ресурс] - Режим доступа: http://opendatacharter.net (дата обращения: 06.10.2024).
11 Открытые данные для искусственного интеллекта (ИИ) [Электронный ресурс] - Режим доступа: https://en.unesco.org/open-access/terms-use-ccbysa-en (дата обращения: 7.10.2024).
12 Закон Республики Казахстан от 16 ноября 2015 года «О доступе к информации». [Электронный ресурс] - Режим доступа: https://adilet.zan.kz/rus/docs/Z1500000401 (дата обращения: 06.10.2024).
13 Закон Республики Казахстан от 24 ноября 2015 года «Об информатизации». [Электронный ресурс] - Режим доступа: https://adilet.zan.kz/rus/docs/Z1500000418 (дата обращения: 06.10.2024).

14 Закон Республики Казахстан от 19 июня 2024 года «О масс-медиа». [Электронный ресурс] - Режим доступа: https://online.zakon.kz/Document/?doc_id=38665430 (дата обращения: 06.10.2024).
15 Закон Республики Казахстан от 10 июля 2023 года «Об онлайн-платформах и онлайн-рекламе». [Электронный ресурс] - Режим доступа: https://online.zakon.kz/Document/?doc_id=36356625 (дата обращения: 06.10.2024).
16 Модельный закон государств–участников СНГ от 18 ноября 2005 года «Об информатизации, информации и защите информации». [Электронный ресурс] - Режим доступа: https://online.zakon.kz/Document/?doc_id=30161686 (дата обращения: 06.10.2024).
17 Минькашев Э. Г. Понятие информации и компьютерной информации: правовые аспекты // Молодой ученый. 2021. № 50 (392). с. 283–287.
18 Коврижных Л. А. О подходах к определению понятия «компьютерная информация» // В сб.: Неволинские чтения: Вопросы совершенствования высшего юридического образования. Киров, 2017. с. 158–163.
19 Open Government Data Principles. [Электронный ресурс] - Режим доступа: https://public.resource.org/8_principles.html (accessed: November 10, 2024).
20 Kaspersky daily | Блог Касперского: Что такое OSINT и в чем опасность. [Электронный ресурс] - Режим доступа: https://blog.kaspersky.kz/osint-open-source-intelligence/26709/ (дата обращения: 05.10.2024).
21 Отчет и исполнительное резюме взаимной оценки Республики Казахстан в рамках второго раунда взаимных оценок ЕАГ. – Алматы, 2023. – 423 с
22 Рахманова Е.Н., Пономарева Е.В. Новые технологии и управление: вызовы цифровой эпохи // Уголовное право: стратегия развития в XXI веке. — 2023. — № 3. — С. 202–209.
23 Paulson, T.M. Intelligence Issues & Development / T.M. Paulson. – Nova Publishers, 2008. – 150 p [Электронный ресурс] - Режим доступа: https://books.google.kz/books/about/Intelligence_Issues_and_Developments.html?id=pCOFOqD9TYQC&redir_esc=y (дата обращения: 16.11.2024).
24 Руководство ФАТФ по финансовым расследованиям: оперативные вопросы – Париж: ФАТФ/ОЭСР, 2012. – 66 с.
25 Еркенов Б.Д., Сейлханова С.А. Эффективность применения инструментов OSINT при противодействии преступной легализации (отмыванию) // Вестник Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан. – 2024. – № 2 (32). – С. 175–183.
26 Уголовно-процессуальный кодекс Республики Казахстан от 05 июля 2015 г. [Электронный ресурс] - Режим доступа: https://online.zakon.kz/Document/?doc_id=31575852 (дата обращения: 20.12.2024).
27 Пирогов В.Е. Неправомерный доступ к компьютерной информации: теоретические проблемы толкования понятия «компьютерная информация» // В сб.: Тренды развития современного общества: управленческие, правовые, экономические и социальные аспекты. – Курск, 2024. – С. 537–539.

28 Минькашев Э.Г. Понятие информации и компьютерной информации: правовые аспекты // Молодой ученый. – 2021. – № 50 (392). – С. 283–287.
29 Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий, совершенное в Душанбе 28 сентября 2018 года. [Электронный ресурс] - Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202207180005 (дата обращения: 20.12.2024).
30 Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ [Электронный ресурс] - Режим доступа: https://online.zakon.kz/Document/?doc_id=30397073 (дата обращения: 25.12.2024).
31 Россинская Е.Р., Усов А.И. Судебная компьютерно-техническая экспертиза. – М.: Норма, 2001. – 414 с.
32 Дёмин К.Е. О понятии «компьютерная информация» применительно к процессу доказывания // Вестник Московского университета МВД России. – 2019. – № 1. – С. 44–47.
33 Сукманов А.О. Понятие и сущность оперативно-розыскного мониторинга открытых источников информации // Вестник Калининградского юридического института МВД России. – 2011. – № 1 (23). – С. 17–19.
34 Сарычев М.М. Использование открытых источников в рамках ОРД // Научные исследования XXI века. – 2024. – № 2 (28). – С. 151–154.
35 Закон Республики Казахстан от 15 сентября 1994 года № 154-XIII «Об оперативно-розыскной деятельности» [Электронный ресурс] - Режим доступа: https://online.zakon.kz/Document/?doc_id=1003158 (дата обращения: 25.12.2024).
36 Осипенко А.Л. Оперативно-розыскной мониторинг информационных ресурсов глобальных компьютерных сетей // Оперативник (сыщик). – 2009. – № 3 (20). – С. 29-33.
37 Овчинский А.С., Борзунов К.К. Оперативно-разыскная информация в инициативных аналитических исследованиях // Вестник экономической безопасности. – 2016. – № 2. – С. 180–183.
38 Глоссарий - [Электронный ресурс] - Режим доступа: http://www.glossary.ru/cgi-bin/gl_sch2.cgi?RNghr8klto9 (дата обращения: 20.12.2024).
39 Стратегии бизнеса: аналитический справочник / Под ред. Г.Б. Клейнера. – М.: КОНСЭКО, 1998.
40 Битюцкий Е.В. Проблемы расследования преступлений, связанных со сбытом наркотических средств, совершённых бесконтактным способом // Сборник материалов Всероссийской научно-практической конференции, 15 декабря 2014 г. – М.: НИЦ ФСКН России, 2014. – 400 с.
41 Ermilov D., Panov M., Yanovich Y. Automatic Bitcoin Address Clustering. [Электронный ресурс] - Режим доступа: https://bitfury.com/content/downloads/clustering_whitepaper.pdf (accessed: January 25, 2025).

42 Bitfury выпустила Crystal – блокчейн-инструмент для финансовых расследований. [Электронный ресурс] - Режим доступа:http://cryptowiki.ru/news/bitfury-vypystila-crystal-blokchein-instryment-dlia-finansovyh-rassledovanii.html (дата обращения: 26.01.2025).
43 Смирнова Ю.А. Использование открытых источников сети Интернет для получения криминалистически значимой информации по делам экономической направленности // Научный аспект. – 2024. – Т. 40. – № 5. – С. 5440–5447.
44 Приговор Темиртауского городского суда Карагандинской области от 12 июля 2024 года по делу № 3524-24-00-1/87.
45 Соломатина А.Г. Использование информационных технологий при расследовании преступлений // В сб.: Уголовное судопроизводство России и зарубежных государств: проблемы и перспективы развития. – СПб., 2023. – С. 304–309.
46 Приказ Председателя КНБ РК от 27 октября 2020 года № 69-қе «Об утверждении Правил функционирования Национальной системы видеомониторинга». [Электронный ресурс] - Режим доступа: https://online.zakon.kz/Document/?doc_id=37809149 (дата обращения: 26.01.2025)
47 Распознает лица, предметы, машины: новую систему видеомониторинга внедряют в Алматы. [Электронный ресурс] - Режим доступа: https://www.zakon.kz/obshestvo/6439971-raspoznaet-litsa-predmety-mashiny-novuyu-sistemu-videomonitoringa-vnedryayut-v-almaty.html (дата обращения: 26.01.2025).
48 Бессонов А.А. Использование в раскрытии преступлений информации из открытых источников информации (OSINT) // Актуальные вопросы теории и практики оперативно-разыскной деятельности: Межвед. науч.-практ. конф., 16 сент. 2022 г. – М.: МУ МВД России им. В.Я. Кикотя, 2022. – С. 40–45.
49 Евтеев С.П. Получение компьютерной информации: нерешённые вопросы и возможности использования результатов оперативно-розыскной деятельности в уголовном процессе // Вестник ВИПК МВД России. – 2017. – № 1 (41). – С. 42–50.
50 Приговор Кызылжарского районного суда СКО от 22 мая 2024 года по делу № 5950-24-00-1/4.
51 Наумов А.А., Шиханова Е.Г. Использование социальных сетей в процессе доказывания // Вестник Международного института рынка. – 2019. – № 2. – С. 97–101.
52 Смушкин А.Б. Криминалистические аспекты исследования даркнета в целях расследования преступлений // Актуальные проблемы российского права. – 2022. – № 3. – С. 102–111.
53 Яковлева К.Ю. Использование технологии OSINT в ходе обыска места нахождения электронной информации // Проблемы правовой и технической защиты информации. – 2023. – № 11. – С. 131–136.
54 Найденышев Ю.В., Завьялова Н.А. Использование технических средств видеофиксации с функцией интеллектуального распознавания лиц по

биометрическим данным в криминалистической методике расследования различных видов преступлений // Вестник полиции. – 2019. – № 6 (1). – С. 3–13
55 Перетолчин А.П., Афанасьев А.Ю. Зарубежный опыт в розыске лиц и раскрытии преступлений по биометрическим данным // В сб.: Международный форум молодых ученых. – М., 2020. – С. 222–227.
56 Пучкова Д.В. Возможность использования габитоскопического модуля и иных современных технологий при расследовании преступлений // Тенденции развития науки и образования. – 2020. – № 68–7. – С. 62–65.
57 ДВД Алматы открыл в соцсетях страницу по розыску без вести пропавших. [Электронный ресурс] - Режим доступа: https://www.caravan.kz/news/dvd-almaty-otkryl-v-socsetyakh-stranicu-po-rozysku-bez-vesti-propavshikh-364501/ (дата обращения: 27.01.2025)
58 Апелляционное постановление Курганского областного суда от 03.04.2014 по делу № 22-635/2014.
59 Головко Л.В. Цифровизация в уголовном процессе: локальная оптимизация или глобальная революция? // Вестник экономической безопасности. – 2019. – № 1. – С. 15–25.
60 Воронин М.И. Электронные доказательства в УПК: быть или не быть? // Lex Russica. – 2019. – № 7 (152). – С. 74–84.
61 Оконенко Р.И. Электронные доказательства и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства США и РФ: дис. ... канд. юрид. наук. – М., 2016. – 198 с.
62 Тушев А.А., Назаров Н.А. Информация как основа всех видов доказательств в уголовном процессе // Общество и право. – 2012. – № 3. – С. 196–197.
63 Гражданский процессуальный кодекс Республики Казахстан. https://online.zakon.kz/Document/?doc_id=34329053 (дата обращения: 28.01.2025)
64 Обидин К.В. Электронное доказательство: необходимый этап развития уголовного судопроизводства // Актуальные проблемы российского права. – 2020. – № 11. – с. 198–206.
65 Шаров В.И. Интернет как источник оперативно-розыскной и процессуальной информации // Вестник Нижегородской академии МВД России. – 2016. – № 3. – с. 111–114.
66 Буряков Е.В. Информационные технологии в розыскной деятельности // Научный вестник Омской академии МВД России. – 2018. – № 3 (70). – С. 29–32
67 Баженов С.В. Оперативно-розыскное мероприятие «Получение компьютерной информации» // Научный вестник Омской академии МВД России. – 2017. – № 2 (65).
68 Давиденко С.А. Проблемы информационного обеспечения розыскной деятельности без вести пропавших лиц и пути их разрешения // В сб.: Обеспечение прав и свобод человека в уголовном судопроизводстве: организационные, процессуальные и криминалистические аспекты. – 2018. – С. 20–22.