УДК 343.14
МРНТИ 10.79.35

М.Е. Тулеуова
Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, г. Косшы, Республика Казахстан

ПРИМЕНЕНИЕ ОТКРЫТЫХ ИСТОЧНИКОВ ДАННЫХ (OSINT) В УГОЛОВНО-ПРОЦЕССУАЛЬНОМ ДОКАЗЫВАНИИ

Аннотация. Эффективность предварительного расследования зависит от качества сбора информации на его первоначальном этапе, особенно при раскрытии преступлений «по горячим следам». В статье анализируются правовые основы использования открытых данных (OSINT) в уголовном процессе Республики Казахстан. Рассматриваются законодательные нормы, регулирующие применение информации из открытых источников в качестве доказательств, а также трактовки понятия «компьютерная информация» в различных нормативных актах и международных соглашениях. Особое внимание уделено внедрению OSINT в деятельность казахстанских правоохранительных органов, его потенциалу и правовым пробелам. Приводится международный опыт США и ЕС, включая анализ цифровых следов, мониторинг соцсетей, отслеживание финансовых транзакций и блокчейн-данных. Автор делает вывод о необходимости совершенствования правового регулирования и расширения возможностей правоохранительных органов в использовании OSINT.

Ключевые слова: уголовное правонарушение; доказательство; открытый источник данных; OSINT; компьютерная информация; сбор информации; оперативно-розыскная деятельность; цифровой след.

М.Е. Тулеуова
Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясы, Қосшы қ., Қазақстан Республикасы

ҚЫЛМЫСТЫҚ ІС ЖҮРГІЗУДІ ДӘЛЕЛДЕУДЕ АШЫҚ ДЕРЕКТЕР КӨЗДЕРІН (OSINT) ҚОЛДАНУ

Аннотация. Алдын ала тергеудің тиімділігі оның бастапқы кезеңінде ақпарат жинау сапасына байланысты, әсіресе қылмыстарды «ізбе із» ашқан кезде. Мақалада Қазақстан Республикасының Қылмыстық процесінде ашық деректерді (OSINT) пайдаланудың құқықтық негіздері талданады. Ашық көздерден алынған ақпаратты дәлел ретінде қолдануды реттейтін заңнамалық нормалар, сондай-ақ әртүрлі нормативтік актілер мен халықаралық келісімдерде «компьютерлік ақпарат» ұғымын түсіндіру қарастырылады. OSINT-ті қазақстандық құқық қорғау органдарының қызметіне енгізуге, оның әлеуеті мен құқықтық олқылықтарына ерекше назар аударылды. Цифрлық іздерді талдау, әлеуметтік медиа мониторингі, қаржылық транзакцияларды қадағалау және блокчейн деректерін қоса алғанда, АҚШ пен ЕО-ның халықаралық тәжірибесі келтірілген. Авторлар OSINT-ті қолдануда құқықтық реттеуді жетілдіру және құқық қорғау органдарының мүмкіндіктерін кеңейту қажеттілігі туралы қорытынды жасайды.

Түйінді сөздер: қылмыстық құқық бұзушылық; дәлелдеме; ашық дерек көздері; OSINT; компьютерлік ақпарат; ақпарат жинау; жедел-іздестіру қызметі; цифрлық із.

M.Ye. Tuleuova
The Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, Kosshy, the Republic of Kazakhstan

THE USE OF OPEN DATA SOURCES (OSINT) IN CRIMINAL PROCEDURAL EVIDENCE

Abstract. The effectiveness of a preliminary investigation depends on the quality of information collection at its initial stage, especially when solving crimes "in hot pursuit". The article analyzes the legal basis for the use of

open data (OSINT) in the criminal process of the Republic of Kazakhstan. The article considers the legislative norms governing the use of information from open sources as evidence, as well as the interpretation of the concept of “computer information” in various regulations and international agreements. Special attention is paid to the implementation of OSINT in the activities of Kazakhstani law enforcement agencies, its potential and legal gaps. The international experience of the USA and the EU is presented, including the analysis of digital footprints, monitoring of social networks, tracking of financial transactions and blockchain data. The author concludes that it is necessary to improve legal regulation and expand the capabilities of law enforcement agencies in using OSINT.

Keywords: criminal offense; evidence; open data source; OSINT; computer information; information collection; operational investigative activities; digital trace.

DOI: 10.52425/25187252_2025_38_207

Введение. Актуальность исследования обусловлена стремительным развитием информационных технологий и расширением их применения в уголовно-процессуальной сфере. В современных условиях возникает необходимость в систематическом подходе к идентификации, сбору, проверке и процессуальному закреплению цифровой информации.

Несмотря на очевидный потенциал OSINT, в национальном уголовно-процессуальном законодательстве Республики Казахстан до сих пор отсутствуют нормы, четко регламентирующие порядок сбора, фиксации и использования данных из открытых источников. Не урегулирован и вопрос их соотношения с другими видами доказательств. Это создает правовую неопределенность и снижает эффективность применения цифровых технологий в расследовании преступлений.

Международный опыт показывает, что многие страны уже выработали правовые и организационные стандарты, направленные на интеграцию OSINT в уголовный процесс. Этот опыт демонстрирует, что при наличии правового регулирования OSINT может стать эффективным инструментом не только оперативно-розыскной деятельности, но и полноценным элементом процессуального доказывания.

Исследование направлено на выявление проблем и пробелов в действующем законодательстве Республики Казахстан, касающемся использования OSINT, и разработку предложений по его совершенствованию с учетом положительного международного опыта. Практическая значимость работы заключается в том, что ее результаты могут быть использованы для модернизации правовых механизмов, обеспечивающих эффективность и законность применения открытых источников данных в уголовно-процессуальной деятельности.

Материалы и методы. Методологическую основу исследования составили сравнительно-правовой, формально-юридический и системный методы. В данной работе использованы труды Д.А. Влезько, Е.Р. Россинской, А.И. Усова, Э.Г. Минькашева, зарубежные публикации – Т.М. Паулсон, рекомендации FATF, сведения Open Data Charter и др. Проведен анализ норм Уголовно-процессуального кодекса Республики Казахстан (далее – УПК РК) (ст.ст. 111, 120, 125), Уголовного кодекса Российской Федерации (далее – УК РФ) (ст. 272), законов РК («О доступе к информации», «Об информатизации», «О масс-медиа», «Об онлайн-платформах и онлайн-рекламе»), международных актов (Соглашение СНГ о киберпреступлениях 2018 г., Меморандум об открытом правительстве США 2009 г., Руководство ООН по открытым данным 2013 г.), также отчетов ЕАГ 2023 года о взаимной оценке РК, данные о применении OSINT в США (80% разведданных).

Результаты, обсуждение. В национальном уголовно-процессуальном законодательстве отсутствует четкая дефиниция понятия «компьютерная информация», что затрудняет ее использование в следственной и судебной практике. Анализ показал, что законодательные подходы Казахстана не учитывают специфику современных цифровых носителей и технологий. Международный опыт (США, ЕС)

демонстрирует широкое применение OSINT, в частности: мониторинг социальных сетей, анализ цифровых следов, отслеживание финансовых транзакций, исследование данных блокчейна. В то же время в РК наблюдается недооценка потенциала OSINT: правоохранительные органы в основном полагаются на внутренние базы данных. При этом использование OSINT имеет ряд преимуществ – доступность, легальность, оперативность, возможность применения без прямого контакта с источниками.

В.Е. Пирогов определяет компьютерную информацию как данные, закодированные или раскодированные, которые хранятся на материальных носителях с возможностью их хранения, обработки, передачи и (или) копирования [1, 537 стр.]. Автор использует фразу «на материальных носителях», не раскрывая их содержание.

По мнению Э.Г. Минькашева, «компьютерная информация – это данные, хранящиеся в памяти или на любом устройстве компьютера. Эти данные представлены в формате, который может быть обработан компьютером или передан по сети» [2, 283 стр.]. Это определение включает в себя все типы носителей информации, обобщенных как «любые».

Согласно Соглашению о сотрудничестве в борьбе с киберпреступлениями в рамках Содружества Независимых Государств (Душанбе, 28 сентября 2018 г.), компьютерная информация определяется как информация, находящаяся в памяти компьютерной системы, на машинных или иных носителях в форме, доступной восприятию компьютерной системы, или передающаяся по каналам связи[1]. Этот ключевой признак отличает данное определение от теоретических дефиниций, приведенных ранее.

Согласно части 2 статьи 111 УПК РК, открытые данные могут быть использованы в качестве доказательств наряду с другими документами, содержащими сведения, значимые для объективного рассмотрения уголовного дела. При этом в статье 120 УПК РК указано, что к таким документам могут относиться компьютерная информация, аудио- и видеозаписи, а также данные, полученные в рамках оперативно-розыскной деятельности.

В примечании к статье 272 УК РФ также содержится определение понятия «компьютерная информация» как сведений (сообщений, данных), представленных в виде электрических сигналов, способных храниться, обрабатываться и передаваться с помощью различных устройств[2]. Однако в данном определении не указано, на каких конкретно устройствах может происходить хранение, обработка и передача информации.

Е.Р. Россинская и А.И. Усов предлагают рассматривать компьютерную информацию в контексте уголовно-процессуального доказывания как фактические данные, обработанные компьютером или передаваемые по телекоммуникационным каналам. Эти данные доступны для восприятия человеком и используются для установления обстоятельств, имеющих значение для разрешения уголовных или гражданских дел [3, 30 стр.]. Авторы отмечают важность соответствия установленного законом порядка при получении такой информации в процессуальных целях.

В отчете и резюме о взаимной оценке РК в рамках второго раунда обзоров ЕАГ, завершенных в 2023 году, отмечается отставание в развитии технологий поиска информации в системе правоохранительных органов страны[3]. Сотрудники правоохранительных органов обычно полагаются на служебные информационные ресурсы, главным образом на Систему информационного обмена правоохранительных и специальных органов (СИОПСО) для получения необходимых данных.

---

[1] О ратификации Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий: закон Республики Казахстан от 9 дек. 2019 г. № 277-VI ЗРК [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/Z1900000277#z6 (дата обращения: 04.02.2025).

[2] Уголовный кодекс Российской Федерации: от 13 июня 1996 г. № 63-ФЗ (ред. от 28.02.2025 г.) [Электронный ресурс] – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 04.03.2025).

[3] Mutual evaluation report of the Republic of Kazakhstan. – 2023 [Электронный ресурс] – Режим доступа: https://eurasiangroup.org/files/uploads/files/ME_(2023)_1_eng_rev1_1.pdf (дата обращения: 16.09.2025).

Казахстанские правоохранительные органы недооценивают потенциал OSINT, тогда как в США она широко применялась с 2005 по 2009 гг. С целью централизованного анализа доступной разведывательной информации в публичном доступе был учрежден Центр мониторинга иностранных трансляций (Foreign Broadcast Information Service, FBIS). Согласно данным западных экспертов, около 80% разведывательной информации в настоящее время собирается с помощью OSINT [4]. В условиях трансформации преступности в информационную эпоху использование открытых источников данных становится необходимым элементом расследования, позволяющим выявлять цифровые следы и анализировать поведение субъектов в сети. Как отмечают Т. Рид и М. Хекер, современные конфликты и преступные практики все чаще переносятся в киберпространство, что требует от правоохранительных органов активного применения OSINT-технологий для установления обстоятельств уголовных дел [5].

Важность OSINT в правоохранительной деятельности подчеркивается рекомендациями Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ) от 2012 года, призывающими использовать информацию из открытых источников для противодействия отмыванию доходов от преступной деятельности[4].

К примеру, отечественные ученые Б.Д. Еркенов и С.А. Сейлханова в борьбе с отмыванием преступных доходов предлагают использовать инструменты Open Source Intelligence (OSINT), такие как:

- анализ цифровых следов (онлайн-активность);
- сканирование сообщений в мессенджерах;
- отслеживание финансовых транзакций;
- мониторинг даркнета;
- картирование корпоративных сетей;
- выявление финансирования терроризма;
- анализ данных блокчейна [6, 180 стр.].

Концепция открытых данных возникла в 1995 году в американском научном сообществе как часть инициативы по обеспечению открытого обмена данными, касающимися глобальных экологических проблем [7, 185 стр.]. В наши дни концепция открытых данных получила широкое распространение во всех аспектах общественной жизни. Сегодня ученые используют открытые данные как инструмент академического исследования и вовлекают общественность в процесс принятия государственных решений [7, 185 стр.].

Открытые данные предполагают, что определенные массивы данных предоставляются без каких-либо ограничений, что позволяет свободно их использовать, читать машинами и повторно публиковать. Для освобождения данных от авторских прав могут применяться некоммерческие лицензии, например, Creative Commons. Согласно определению, представленному на официальном сайте Международной хартии открытых данных, «открытые данные» – это данные и контент, доступные для свободного использования и обмена без каких-либо ограничений и финансовых обязательств[5].

С.А. Панюкова определяет открытые данные как массивы данных в цифровом формате, размещенные в Интернете, которые содержат информацию о деятельности органов власти и местного самоуправления, а также как данные, собранные информационно-аналитическими организациями. При этом эти данные доступны для автоматической обработки и повторного использования без предварительного вмешательства человека. Любое лицо может использовать их бесплатно и в законных целях независимо от способа публикации [8, 27 стр.].

Таким образом, открытые данные характеризуются следующими ключевыми признаками: свободный доступ к просмотру и повторному использованию; отсутствие ограничений авторского права, лицензий или патентов; возможность многократного использования в законных целях; охват данных государственных и местных органов, а также организаций, проводящих

[4] Operational Issues – Financial Investigations Guidance // Paris, FATF/OECD, 2012. – 66 p. [Электронный ресурс] – Режим доступа: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Operationalissues-financialinvestigationsguidance.html (дата обращения: 16.09.2025).

[5] Open data charter [Электронный ресурс] – Режим доступа: https://opendatacharter.org/ (дата обращения: 16.02.2025).

исследования в различных отраслях; безвозмездное (бесплатное) использование; представление в машиночитаемом формате.

В рамках Меморандума об открытом правительстве, выпущенного в США 20 января 2009 года, были провозглашены три принципа открытости: «прозрачность правительства», «совместная работа правительства» и «сотрудничество правительства»[6]. Меморандум стал основополагающим для Директивы об открытом правительстве (Open Government Directive)[7].

В 2013 году Организация Объединенных Наций выпустила Руководство по открытым государственным данным для участия граждан. Согласно этому руководству, открытые данные – это информация, которую любой может свободно использовать в любых целях, не сталкиваясь с какими-либо ограничениями[8].

Согласно содержанию Модельного закона государств-участников СНГ от 18 ноября 2005 года «Об информатизации, информации и защите информации», «информация» – это любые сведения или данные, которые подлежат правовому регулированию вне зависимости от формы их представления, хранения или организации[9].

В Казахстане такие понятия, как «информация», «данные», «сообщения», «интернет-ресурс», «электронный информационный ресурс», определяются Законами РК «О доступе к информации» от 16 ноября 2015 года, «Об информатизации» от 24 ноября 2015 года, «О масс-медиа» от 19 июня 2024 года, «Об онлайн-платформах и онлайн-рекламе» от 10 июля 2023 года. Кроме того, эти законы устанавливают правовую основу для работы со свободными данными и получения к ним доступа.

Так, в Законе РК «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)[10].

Закон РК «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[11].

В Законе РК «О масс-медиа» можно обнаружить определение официального сообщения, под которым предлагается понимать информацию, предоставляемую и (или) распространяемую посредством масс-медиа обладателем информации, установленным в соответствии с Законом РК «О доступе к информации»[12].

В Законе РК «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,

---

[6] Transparency and Open Government / Memorandum for the heads of executive departments and agencies, 2009 // The White House [Электронный ресурс] – Режим доступа: https://obamawhitehouse.archives.gov/the-press-office/transparency-and-open-government (дата обращения: 15.03.2025).

[7] Open Government Directive / Memorandum for the heads of executive departments and agencies, 2009 // The White House [Электронный ресурс] – Режим доступа: https://obamawhitehouse.archives.gov/open/documents/open-government-directive (дата обращения: 15.03.2025).

[8] Guidelines on Open Government Data for Citizen Engagement [Электронный ресурс] – Режим доступа: http://workspace.unpan.org/sites/Internet/Documents/Guidenlines%20on%20OGDCE%20May17%202013.pdf (дата обращения: 11.09.2025).

[9] Модельный закон «Об информатизации, информации и защите информации»: принят на двадцать шестом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ постановлением № 26-7 от 18 нояб. 2005 г. [Электронный ресурс] – Режим доступа: https://online.zakon.kz/Document/?doc_id=30161686 (дата обращения: 11.09.2025).

[10] О доступе к информации: закон Республики Казахстан от 16 нояб. 2015 г. № 401-V ЗРК [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/Z1500000401 (дата обращения: 08.03.2025).

[11] Об информатизации: закон Республики Казахстан от 24 нояб. 2015 г. № 418-V ЗРК [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/Z1500000418 (дата обращения: 08.03.2025).

[12] О масс-медиа: закон Республики Казахстан от 19 июня 2024 г. № 93-VIII ЗРК [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/Z2400000093 (дата обращения: 08.03.2025).

предметах, событиях, явлениях и процессах, зафиксированная в любой форме[13].

Как видим из нормативных актов, понятия «информация» и «открытые данные» взаимосвязаны, но различны по объему. «Информация» – более широкое понятие, включающее все данные в любой форме, в то время как «открытые данные» относятся к данным, доступным в машиночитаемом формате. Несмотря на это, Закон РК «О доступе к информации» не определяет иерархические отношения между этими понятиями, что может создавать неясность в их интерпретации.

Мы присоединяемся к мнению Э.Г. Минькашева, полагающего, что информация должна быть определена через термин «данные», соединенный разделительным союзом «или» со словом «сведения» [2, 287 стр.]. Таким образом, информация представляет собой либо данные, либо сведения, а не объединение сведений, сообщений и данных. Такое определение соответствует логике Модельного закона об информатизации, информации и защите информации 2005 года[14].

Поскольку Закон РК «О доступе к информации» является фундаментальным в указанном нормативно-правовом комплексе, необходимо привести определение информации, содержащееся в нем, в соответствие с Модельным законом об информатизации, информации и защите информации от 2005 года. Это позволит обеспечить согласованность в использовании понятия «информация» во всех нормативных актах, связанных с реализацией права граждан на доступ к информации, включая открытые данные. Такое изменение повысит качество применения этих документов.

Открытые данные охватывают множество разнообразных источников, которые можно классифицировать следующим образом:

- поисковые системы, такие как Google и Bing, которые предоставляют доступ к обширным объемам информации, включая веб-страницы, изображения и видео;
- базы данных, содержащие структурированную информацию по конкретным темам, такую как научные исследования, статистические данные и каталоги;
- электронные новости и новостные агентства, предоставляющие актуальную информацию по различным темам;
- платформы социальных сетей, такие как Facebook и Twitter, которые генерируют большие объемы пользовательского контента, что в свою очередь может быть использовано для анализа общественных настроений и тенденций;
- сайты информационных агентств, публикующих новости, аналитику и информацию на своих веб-сайтах;
- личные сайты, принадлежащие организациям или физическим лицам.

Основные преимущества OSINT:

- информация доступна в режиме близком к реальному времени;
- данные доступны быстро и легко;
- информация получена законно;
- источники информации легко идентифицировать;
- пользователи могут легко получить доступ к данным;
- доступ к информации в основном бесплатный или недорогой.

Таким образом, OSINT выступает не просто как дополнительная возможность, а как неотъемлемая часть предотвращения, раскрытия и расследования преступлений, поскольку открытые источники данных позволяют оперативно получать достоверную информацию при минимальных затратах. Как подчеркивает М. Баззелл, эффективный специалист в сфере OSINT должен обладать собственными инструментами и навыками поиска, что обеспечивает независимость и надежность результатов расследования [9].

Как отмечает М.М. Лоувенталь, современная разведывательная деятельность в зна-

[13] Об онлайн-платформах и онлайн-рекламе: закон Республики Казахстан от 10 июля 2023 г. № 18-VIII ЗРК [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/Z2300000018 (дата обращения: 08.03.2025).

[14] Модельный закон «Об информатизации, информации и защите информации»: принят на двадцать шестом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ постановлением № 26-7 от 18 нояб. 2005 г. [Электронный ресурс] – Режим доступа: https://online.zakon.kz/Document/?doc_id=30161686 (дата обращения: 08.02.2025).

чительной степени опирается на открытые данные, что делает их применение в уголовно-процессуальном доказывании объективно востребованным и эффективным [10]. Учитывая, что доказательствами в уголовном деле могут служить материалы, полученные из открытых источников в соответствии с законами об оперативно-розыскной и контрразведывательной деятельности, необходимо рассмотреть вопрос об использовании открытых источников в оперативно-розыскной деятельности.

Помимо использования в расследовании уголовных дел, эти материалы также могут выступать в качестве повода для начала досудебного производства.

Хотя оперативно-розыскная деятельность регулируется отдельным законом, важно отметить, как Закон об оперативно-розыскной деятельности устанавливает порядок использования открытых источников информации.

Основным методом получения информации в оперативно-розыскной деятельности являются негласные методы, но использование открытых данных также может быть эффективным. По мнению А.О. Сукманова, одним из ключевых применений является оперативно-розыскной мониторинг печатных и интернет-источников. Это позволяет правоохранительным органам отслеживать преступную активность и реагировать на нее [11, 18 стр.].

М.М. Сарычев и А.А. Дягилев подчеркивают, что оперативно-розыскной мониторинг в Интернете может выявить сайты преступных группировок и незаконный контент, включая пропаганду экстремизма, терроризма и наркотиков. С помощью компьютерных данных, полученных в результате такого мониторинга, можно укреплять доказательную базу в уголовных процессах [12, 151 стр.].

Закон предусматривает использование технических средств для сбора информации в рамках оперативно-розыскных мероприятий. При этом не должны нарушаться охраняемая законом тайна частной жизни, неприкосновенность жилища, личной и семейной тайны, а также тайна вкладов, сообщений и переписки. Определение «специальных технических средств» в законе включает устройства, аппаратуру, приспособления и программное обеспечение, предназначенные для получения и документирования информации в ходе оперативно-розыскных мероприятий или негласных следственных действий.

Однако использование таких средств не ограничивается исключительно компьютерной информацией[15].

В Законе отсутствуют конкретные указания о правомерных способах получения информации из открытых источников. В статье 1 Закона определение «перехват информации» охватывает широкий спектр данных, включая сигналы, текст, изображения и звуки, передаваемые по электромагнитным системам. Однако это определение не делает различий между перехватом информации из закрытых и открытых источников[16].

А.Л. Осипенко определяет оперативно-розыскной мониторинг информационного пространства как комплексную систему наблюдения за криминальными процессами в сетевых социальных средах. Эта система основана на применении оперативно-розыскных мер и методов. В частности, оперативно-розыскное наблюдение предполагает сбор, анализ и оценку информации о криминальных явлениях в Интернете. С его помощью можно анализировать оперативную обстановку в сети и прогнозировать ее изменения под влиянием криминогенных факторов [13, 29 стр.].

В отличие от этого, А.О. Сукманов предлагает сосредоточиться на наблюдении за ресурсами сети, поскольку они могут содержать не только непосредственно криминальные данные, но и информацию о любых процессах, которая может иметь криминалистическую ценность [11, 19 стр.].

А.С. Овчинский и К.К. Борзунов выделяют важную характеристику оперативно-розыскного мониторинга: он включает в

[15] Об оперативно-розыскной деятельности: закон Республики Казахстан от 15 сент. 1994 г. № 154-XIII [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/Z940004000_ (дата обращения: 11.03.2025).

[16] Там же.

себя непрерывную обработку фоновых информационных потоков о текущих событиях. Это позволяет выявлять признаки криминальной активности и предпосылки совершения преступлений в сети Интернет [14, 182 стр.].

Заключение. Результаты исследования свидетельствуют о необходимости совершенствования правового регулирования применения открытых источников данных в уголовном процессе и оперативно-розыскной деятельности. Представляется целесообразным закрепить в статье 7 УПК РК понятие «компьютерная информация» в следующей редакции: «Компьютерная информация – полученные в соответствии с законодательством сведения о фактических обстоятельствах, имеющих значение для правильного разрешения дела, которые хранятся, обрабатываются или передаются электронными устройствами в виде электрических сигналов».

В статью 1 Закона РК «Об оперативно-розыскной деятельности» предлагается ввести определение понятия «оперативно-розыскной мониторинг открытых источников информации» в следующей редакции: «Оперативно-розыскной мониторинг открытых источников информации – это систематическое наблюдение за информационно-телекоммуникационными сетями и системами для своевременного выявления, сбора и анализа сведений о социально опасных явлениях, а также о факторах, которые их обусловливают, с целью предотвращения или расследования преступлений».

Применение рекомендаций из исследования по совершенствованию уголовно-процессуального и оперативно-розыскного законодательства поможет эффективно использовать открытые источники данных для доказательства в уголовных делах и позволит повысить эффективность раскрытия и расследования преступлений.

Список использованной литературы:

1. Пирогов, В.Е. Неправомерный доступ к компьютерной информации: теоретические проблемы толкования понятия компьютерной информации / В.Е. Пирогов // Тренды развития современного общества: управленческие, правовые, экономические и социальные аспекты: сб. науч. ст. 14-й Всерос. науч.-практ. конф. – Курск, 2024. – С. 537-539.
2. Минькашев, Э.Г. Понятие информации и компьютерной информации: правовые аспекты / Э.Г. Минькашев // Молодой ученый. – 2021. – № 50 (392). – С. 283-287.
3. Россинская, Е.Р. Судебная компьютерно-техническая экспертиза / Е.Р. Россинская, А.И. Усов. – М.: Право и закон, 2001. – 414 с.
4. Paulson, T.M. Intelligence Issues & Developm / T.M. Paulson. – Nova Publishers, 2008. – 177 p.
5. Rid, T. War 2.0: Irregular Warfare in the Information Age / T. Rid, M. Hecker. – Praeger, 2009. – 278 p.
6. Еркенов, Б.Д. Эффективность применения инструментов OSINT при противодействии преступной легализации (отмыванию) / Б.Д. Еркенов, С.А. Сейлханова // Құқық қорғау органдары академиясының Жаршысы. – 2024. – № 2 (32). – С. 175-183.
7. Дарменова, А.С. Открытые данные: двадцатипятилетняя история развития / А.С. Дарменова, Ж.Д. Мамыкова, К.Н. Андерсен // Вестник НГУЭУ. – 2020. – № 2. – С. 183-197.
8. Панюкова, С.А. Роль открытых данных в развитии журналистики данных/ С.А. Панюкова // Знак: проблемное поле медиаобразования. – 2015. – № 1 (15). – С. 25-33.
9. Bazzell, M. Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information. – 9th ed. / M. Bazzell. – Independently Published, 2021. – 666 p.
10. Lowenthal, M.M. Intelligence: From Secrets to Policy. – 7th ed. / M.M. Lowenthal. – CQ Press, 2017. – 593 p.
11. Сукманов, А.О. Понятие и сущность оперативно-розыскного мониторинга открытых источников информации / А.О. Сукманов // Вестник Калининградского юридического института МВД России. – 2011. – № 1 (23). – С. 17-19.

12. Сарычев, М.М. Использование открытых источников в раках ОРД / М.М. Сарычев // Научные исследования XXI века. – 2024. – № 2 (28). – С. 151-154.
13. Осипенко, А.Л. Оперативно-розыскной мониторинг информационных ресурсов глобальных компьютерных сетей / А.Л. Осипенко // Оперативник (сыщик). – 2009. – № 3 (20). – С. 28-32.
14. Овчинский, А.С. Оперативно-розыскная информация в инициативных аналитических исследованиях / А.С. Овчинский, К.К. Борзунов // Вестник экономической безопасности. – 2016. – № 2. – С. 180-183.

References:

1. Pirogov, V.E. Nepravomernyj dostup k komp'juternoj informacii: teoreticheskie problemy tolkovanija ponjatija komp'juternoj informacii / V.E. Pirogov // Trendy razvitija sovremennogo obshhestva: upravlencheskie, pravovye, jekonomicheskie i social'nye aspekty: sb. nauch. st. 14-j Vseros. nauch.-prakt. konf. – Kursk, 2024. – S. 537-539.
2. Min'kashev, Je.G. Ponjatie informacii i komp'juternoj informacii: pravovye aspekty / Je.G. Min'kashev // Molodoj uchenyj. – 2021. – № 50 (392). – S. 283-287.
3. Rossinskaja, E.R. Sudebnaja komp'juterno-tehnicheskaja jekspertiza / E.R. Rossinskaja, A.I. Usov. – M.: Pravo i zakon, 2001. – 414 s.
4. Paulson, T.M. Intelligence Issues & Developm / T.M. Paulson. – Nova Publishers, 2008. – 177 p.
5. Rid, T. War 2.0: Irregular Warfare in the Information Age / T. Rid, M. Hecker. – Praeger, 2009. – 278 p.
6. Erkenov, B.D. Jeffektivnost' primenenija instrumentov OSINT pri protivodejstvii prestupnoj legalizacii (otmyvaniju) / B.D. Erkenov, S.A. Sejlhanova // Құқық қорғау organdary akademijasynyң Zharshysy. – 2024. – № 2 (32). – S. 175-183.
7. Darmenova, A.S. Otkrytye dannye: dvadcatipjatiletnjaja istorija razvitija / A.S. Darmenova, Zh.D. Mamykova, K.N. Andersen // Vestnik NGUJeU. – 2020. – № 2. – S. 183-197.
8. Panjukova, S.A. Rol' otkrytyh dannyh v razvitii zhurnalistiki dannyh/ S.A. Panjukova // Znak: problemnoe pole mediaobrazovanija. – 2015. – № 1 (15). – S. 25-33.
9. Bazzell, M. Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information. – 9th ed. / M. Bazzell. – Independently Published, 2021. – 666 p.
10. Lowenthal, M.M. Intelligence: From Secrets to Policy. – 7th ed. / M.M. Lowenthal. – CQ Press, 2017. – 593 p.
11. Sukmanov, A.O. Ponjatie i sushhnost' operativno-rozysknogo monitoringa otkrytyh istochnikov informacii / A.O. Sukmanov // Vestnik Kaliningradskogo juridicheskogo instituta MVD Rossii. – 2011. – № 1 (23). – S. 17-19.
12. Sarychev, M.M. Ispol'zovanie otkrytyh istochnikov v rakah ORD / M.M. Sarychev // Nauchnye issledovanija XXI veka. – 2024. – № 2 (28). – S. 151-154.
13. Osipenko, A.L. Operativno-rozysknoj monitoring informacionnyh resursov global'nyh komp'juternyh setej / A.L. Osipenko // Operativnik (syshhik). – 2009. – № 3 (20). – S. 28-32.
14. Ovchinskij, A.S. Operativno-rozysknaja informacija v iniciativnyh analiticheskih issledovanijah / A.S. Ovchinskij, K.K. Borzunov // Vestnik jekonomicheskoj bezopasnosti. – 2016. – № 2. – S. 180-183.

АВТОРЛАР ТУРАЛЫ МӘЛІМЕТТЕР / СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

Мульдир Ерлановна Тулеуова – Қазақстан Республикасы Бас прокуратурасы жанындағы Құқық қорғау органдары академиясының Жоғары оқу орнынан кейінгі білім беру институтының арнайы заң пәндері кафедрасының аға оқытушысы, құқықтану магистрі, e-mail: bdykva@mail.ru.

Тулеуова Мулдир Ерлановна – старший преподаватель кафедры специальных юридических дисциплин Института послевузовского образования Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, магистр юриспруденции, e-mail: bdykva@mail.ru.

Tuleuova Muldir Yerlanovna – Senior lecturer at the Department of Special Legal Disciplines of the Institute of Postgraduate Education of the Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, Master of Law Sciences, e-mail: bdykva@mail.ru.