



ҚЫЛМЫСТЫҚ ПРОЦЕСС, КРИМИНАЛИСТИКА, СОТ-САРАПТАМА ҚЫЗМЕТІ / УГОЛОВНЫЙ ПРОЦЕСС, КРИМИНАЛИСТИКА, СУДЕБНО-ЭКСПЕРТНАЯ ДЕЯТЕЛЬНОСТЬ / CRIMINAL PROCEDURE, CRIMINALISTICS, FORENSIC EXPERTISE

УДК 343.14
МРНТИ 10.79.35

Б.Д. Еркенов, С.А. Сейлханова

*Алматинская академия Министерства внутренних дел Республики Казахстан имени М. Есбулатова,
г. Алматы, Республика Казахстан*

ЭФФЕКТИВНОСТЬ ПРИМЕНЕНИЯ ИНСТРУМЕНТОВ OSINT ПРИ ПРОТИВОДЕЙСТВИИ ПРЕСТУПНОЙ ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЮ)

Аннотация. В статье рассмотрены вопросы сбора, анализа и использования оперативно значимой информации из открытых источников, в сети Интернет, в целях решения задач при проведении параллельных финансовых расследований. Освещены передовые международные практики поиска информации, представляющей оперативный интерес. Авторами обозначен ряд проблем организационного характера в деятельности отечественных правоохранительных органов, устранение которых предлагается рассматривать направлением совершенствования информационно-аналитического обеспечения следственно-оперативной деятельности, а также обучения сотрудников различным методикам и техникам анализа информации, полученной из открытых источников. С учетом огромного потенциала повсеместного внедрения и использования технологий разведки по открытым источникам авторами обосновывается необходимость придания им приоритетного значения при поиске и установлении легализованного имущества и доходов, проведении научных исследований, подготовке специалистов данного направления.

Ключевые слова: противодействие; преступность; разведка; поиск; открытый источник; информация; параллельное финансовое расследование.

Б.Д. Еркенов, С.А. Сейлханова

*Қазақстан Республикасы Ішкі істер министрлігінің М. Есболатов атындағы Алматы академиясы,
Алматы қ., Қазақстан Республикасы*

ҚЫЛМЫСТЫҚ ЗАҢДАСТЫРУҒА (ЖЫЛЫСТАТУҒА) ҚАРСЫ ІС-ҚИМЫЛ КЕЗІНДЕ OSINT ҚҰРАЛДАРЫН ҚОЛДАНУДЫҢ ТИІМДІЛІГІ

Аннотация. Мақалада қатарлас қаржылық тергеп-тексеру жүргізу кезінде мәселелерді шешу мақсатында ашық көздерден, Интернет желісінен жедел маңызды ақпаратты жинау, талдау және пайдалану мәселелері қарастырылды. Жедел қызығушылық тудыратын ақпаратты іздеудің озық тәжірибелері қамтылды. Авторлар отандық құқық қорғау органдарының қызметіндегі ұйымдастырушылық сипаттағы бірқатар проблемаларды белгіледі, оларды жоюды тергеу-жедел қызметті ақпараттық-талдамалық қамтамасыз етуді жетілдіру бағытында, сондай-ақ қызметкерлерді ашық көздерден алынған ақпаратты талдаудың әртүрлі әдістері мен тәсілдеріне үйрету арқылы қарастыру ұсынылады. Ашық көздер бойынша барлау технологияларын кеңінен енгізу мен пайдаланудың орасан зор әлеуетін ескере отырып, авторлар заңдастырылған мүлік пен кірістерді іздеу және белгілеу, ғылыми зерттеулер жүргізу, осы бағыттағы мамандарды даярлау кезінде оларға басымдық беру қажеттілігін негіздейді.

Түйінді сөздер: қарсылық; қылмыс; барлау; іздеу; ашық көз; ақпарат; қатарлас қаржылық тергеп-тексеру.



B.D. Yerkenov, S.A. Seyilkhanova

*The Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after M. Esbulatov,
Almaty c., the Republic of Kazakhstan*

THE EFFICIENCY OF USING OSINT TOOLS IN COUNTERING CRIMINAL LEGALIZATION (LAUNDERING)

Abstract. The article considers the issues of collection, analysis and application of operationally relevant information from open sources, on the Internet, in order with the purpose of solving tasks in conducting parallel financial investigations. The leading practices of searching for information of operational interest are highlighted. The authors have identified a number of organizational problems in the activities of domestic law enforcement agencies, the elimination of which it is proposed to consider the direction of improving the information and analytical support of investigative and operational activities, as well as training officers to various methods and techniques of analysis of information obtained from open sources. Taking into account the huge potential of the widespread implementation and application of open source intelligence technologies, the authors substantiate the necessity of giving them a priority in the search and identification of legalized property and income, conducting scientific research, training of specialists in this area.

Keywords: countering; crime; intelligence; search; open source; information; parallel financial investigation.

DOI: 10.52425/25187252_2024_32_175

Введение. Развитие Интернета и растущая цифровизация платежных процессов произвели революцию в способах легализации (отмывания) доходов от преступной деятельности. Новые технологические достижения, в т.ч. в социальных сетях, онлайн-платформах и онлайн-играх, мобильных платежах, переводах, цифровых и криптовалют, программного обеспечения для анонимизации, снизили риски и затраты для профессиональных «отмывателей», связанные с их преступной деятельностью¹.

С учетом низкого уровня финансовой прозрачности, в большей части постсоветских стран, такие технологии позволяют преступникам обходить проверки средств, поступающих в законную экономику, и использовать пробелы в законодательстве, подрывая меры по противодействию легализации (отмыванию) преступных доходов и позволяя отмывому имуществу и доходам избегать обнаружения.

При этом, по оценкам УНП ООН, ежегодная доля глобального отмывания денег составляет примерно 2,7% мирового ВВП².

Задачи и цели. Основная цель публикации – исследование международного опыта в использовании инструментов OSINT в противодействии преступной легализации доходов, в т.ч. при проведении параллельных финансовых расследований. Основной задачей статьи является рекомендации в использовании разведки из открытых источников в противодействии легализации (отмыванию) преступных доходов.

Материалы и методы исследования. Настоящее исследование осуществлено путем применения комплекса методов, традиционно применяемых в правовой науке, а именно: общенаучного, историко-правового, сравнительно-правового, формально-логического, системно-структурного методов. Наравне с указанными методами использованы частные методики, отвечающие целям и задачам тематики исследования: анализ и оценка нормативных источников, международно-правовых актов, ратифицированных Республикой Казахстан, рекомендаций международных организаций, имеющих отношение к рассматриваемым проблемам.

¹ Профессиональное отмывание денег // Отчет ФАТФ // Июль 2018 г. [Электронный ресурс] – Режим доступа: <http://www.fatf-gafi.org/publications/methodandtrends/documents/professional-money-laundering.html> (дата обращения: 16.03.2024).

² Отмывание доходов от незаконного оборота синтетических наркотиков // Инструментарий Организации Объединенных Наций по синтетическим наркотикам [Электронный ресурс] – Режим доступа: <https://syntheticdrugs.unodc.org/syntheticdrugs/ru/cybercrime/laundryproceeds/index.html> (дата обращения: 21.03.2024).



Изучение вопросов использования сети Интернет в поисках оперативно значимой информации являлось предметом исследований ряда отечественных ученых таких, как С.Ю. Алесковский, В.И. Гинзбург, А.Я. Григорьев, Е.Е. Каймулдинов, С.В. Паташков, Т.Е. Сулейменов, М.П. Сысалов, Ж.М. Чекин и др.

Среди ученых стран ближнего зарубежья следует отметить научные труды В.Ю. Батоева, Г.Ф. Вильдяйкина, В.И. Иванова, В. Минченко, М.О. Качалова, Н.О. Павленко, В.Б. Шарова, М.О. Янгаевой и др.

Исследование проблем в данной области явилось предметом изысканий ученых стран дальнего зарубежья таких, как Ар. Гхилони, Т.М. Полсон, Эм. Таддэо, Эл. Флориди и др.

Результаты/обсуждение. Сегодня профессиональные «отмыватели» в своих преступных целях все чаще используют информационно-телекоммуникационные технологии. Информацию о личности преступника и, в целом, о преступлении часто можно найти в открытом доступе в сетях Интернет. Несмотря на то, что процедура поиска необходимой информации из открытых источников довольно сложный процесс, требующий обладания определенными навыками, полученные результаты могут внести значимый вклад в деятельность по противодействию преступной легализации (отмыванию). На это обращает внимание и автор статьи «Поиск и анализ оперативно-розыскной информации в интернете» В.И. Шаров, по мнению которого, использование информационных ресурсов интернет является резервом оперативно-розыскной деятельности в современных условиях и существенно повышает ее возможности по борьбе с преступностью [1, 411 стр.]. Здесь следует согласиться с мнением В.Ю. Иванова, что ряд преступных деяний практически полностью перешел в сегмент информационно-телекоммуникационных технологий, например, незаконный сбыт наркотических средств в подавляющем большинстве случаев совершается бесконтактным способом [2].

К числу эффективных, однако, недооцененных в отечественном сегменте, инструментов поиска и обнаружения информации в сети Интернет, однако недооцененных в отечественном сегменте, следует отнести программные решения по проведению разведывательно-поисковых мероприятий по открытым источникам, иными словами использование технологии «OSINT» (Open Source Intelligence) [3].

OSINT – это разведывательная дисциплина, включающая в себя поиск, выбор, сбор разведывательной информации из общедоступных источников, а также ее анализ. Источники OSINT отличаются от других форм разведки, поскольку они должны быть легально доступны общественности без нарушения каких-либо законов или конфиденциальности [4].

В системе правоохранительных органов Казахстана данная технология поиска информации не нашла своего должного развития, при этом сотрудники правоохранительных органов в большинстве своем используют служебные информационные ресурсы для поиска необходимых сведений, в первую очередь Систему информационного обмена правоохранительных и специальных органов (СИОПСО)³, и зачастую в недостаточной степени владеют навыками поиска информации в открытых источниках в недостаточной степени ввиду сложности их дальнейшего приобщения в качестве доказательств.

К сожалению, и в отечественной науке вопросы, посвященные разведке из открытых источников не исследованы в полном объеме, отсутствуют также регламентированные нормативные акты, в т.ч. методические рекомендации по их проведению. Тогда как в западных странах история разведки из открытых источников начинается с создания в декабре 1941 года Службы мониторинга зарубежных трансляций (Foreign Broadcast Monitoring Service, FBMS) в США, с целью перехвата и анализа иностранных трансляций. Сотрудники службы записывали коротковолновые передачи, после чего

³ Отчет и исполнительное резюме взаимной оценки Республики Казахстан в рамках второго раунда взаимных оценок ЕАГ // Алматы, 2023. – 423 с.



отдельные материалы переписывались и переводились, а затем отправлялись в военные ведомства и подавались в формате еженедельных докладов. Классическим примером работы FBMS является получение информации об успешности проведения бомбардировок на вражеские мосты путем получения и анализа изменения цен на апельсины в Париже.

Второй этап развития OSINT пришелся на период 2005-2009 гг., когда в США был создан центр по анализу разведывательных материалов из открытых источников информации (Foreign Broadcast Information Service, FBIS). В этот период интернет только начинал входить в жизнь обывателей, стали создаваться социальные сети, получившие широкую популярность. В связи с этим количество информации, публикуемой в интернете, увеличивалось ежемесячно в геометрической прогрессии [5].

По мнению ряда западных ученых, сегодня, результаты OSINT составляют около восьмидесяти процентов всех разведывательных материалов, используемых правоохранительными органами. В последнее время произошли достаточно эффективные случаи использования результатов OSINT в качестве ценной разведывательной информации правоохранительными органами. К примеру, в 2018 году группа OSINT-аналитиков определила место казни, показанное в одном из самых известных пропагандистских видеороликов «Исламского государства». Это было достигнуто путем сравнения характеристик местности, растительности и зданий, показанных на видео кадрах, со спутниковыми изображениями из Google Earth [6].

Сегодня методы разведки из открытых источников (OSINT) становятся мощным инструментом в противодействии легализации (отмыванию) преступных доходов, предлагая гибкость и эффективность, а также обеспечивая совместный итеративный подход к сбору и анализу разведывательной информации. Хотя ни один инструмент или метод не может полностью положить конец

легализации (отмыванию) денег и доходов от преступной деятельности, интеграция OSINT с традиционными методами расследования открывает возможность к более активному подходу в обеспечении проведения качественного параллельного финансового расследования [7].

Следует отметить, что еще в 2012 году экспертами ФАТФ в своем Отчете рекомендовано использование информации из открытых источников в целях противодействия легализации (доходов) от преступной деятельности⁴.

Анализ информации, содержащейся в социальных сетях и на иных сайтах, хранящих персональные данные, открывает большие возможности для поиска и установления следов легализованного (отмытого) имущества и доходов от преступной деятельности.

По нашему мнению, в поиске сведений по установлению легализованного (отмытого) имущества и доходов с использованием инструментов OSINT, необходимо обращать внимание на следующие данные, содержащиеся в открытых источниках.

1. Цифровые (онлайн) следы.

Технологии OSINT могут идентифицировать связи между учетными записями в социальных сетях, тегированными данными геолокации и списками друзей и знакомых по именам, адресам электронной почты, номерам телефонов и другим открытым данным. Эти фрагменты информации позволяют правоохранителям создать подробный профиль действий субъекта, связанный с противоправной деятельностью.

2. Сканирование мессенджеров.

Преступники, участвующие в схемах отмывания денег, часто используют такие мессенджеры, как Telegram, из-за его предполагаемой анонимности. Однако аналитические решения с открытым исходным кодом позволяют сканировать контент платформы, и открывают возможность для более широкого поиска информации. Этого можно добиться посредством поиска по определенным

⁴ Руководство ФАТФ по финансовым расследованиям: оперативные вопросы // Париж, ФАТФ/ОЭСР. – 2012. – 66 с.



ключевым словам, псевдониму, номеру телефона или идентификатору Telegram; обнаружения ссылок на закрытые группы; анализа деятельности администраторов; или доступа к удаленному контенту.

3. Отслеживание транзакций.

Разведывательные данные из открытых источников позволяют правоохранителям отслеживать документы и движение счетов, используя перекрестные ссылки на публичные записи, финансовые веб-сайты и внутренние записи организаций. Кроме того, OSINT может сыграть важную роль в выявлении отрывочных переводов финансовых средств и связанных с ними нарушений, а также в визуализации ключевой информации, которая может выявить неочевидные связи между преступными учетными записями и отдельными лицами.

4. Даркнет-мониторинг.

Аналитические решения с открытым исходным кодом позволяют правоохранителям отслеживать схемы отмывания денег через «даркнет» путем сканирования источников данных, подпольных рынков и форумов для сбора важной информации против злоумышленников. Кроме того, можно деанонимизировать скрытые профили путем перекрестных ссылок на информацию из Surface Web и публикаций в «даркнете» (в т.ч. удаленных) и проводить поиск на основе имен пользователей и адресов криптокошельков, что создает возможности для получения практической информации.

5. Картирование корпоративной сети.

OSINT позволяет следователям визуализировать организационную структуру компаний путем сканирования корпоративных реестров. Инструменты разведки с открытым исходным кодом предоставляют с базы данных сведения о возможных теневых связях у субъектов исследования, что значительно повышает качество собираемой информации.

6. Инспекция по борьбе с финансированием терроризма.

Террористические организации, как

правило, распределяют свои финансовые ресурсы по отдельным странам, что позволяет им использовать слабости регулирования в системах противодействия отмыванию доходов. Однако, собирая данные из официальных источников, таких как финансовые отчеты и реестры, OSINT становится очень ценным при расследовании активов террористических группировок. Такие возможности могут сыграть ключевую роль в ликвидации схем отмывания денег. Кроме того, разведывательные решения с открытым исходным кодом могут еще больше обогатить данные за счет проведения поиска в социальных сетях и онлайн-форумах, что может связать подозреваемых с известными террористическими группировками.

7. Анализ блокчейна.

Несмотря на то, что технология блокчейна обеспечивает определенную степень прозрачности через общедоступные реестры, попытка ориентироваться в этих данных может оказаться затруднительной. Инструменты OSINT могут устранить разрыв и идентифицировать вредоносные криптокошельки путем перекрестных ссылок на транзакции и связи между адресами. Благодаря расширенным функциям, таким как обнаружение децентрализованных групп через общие ссылки и отслеживание денежных переводов по сетям, имеется возможность установления более прозрачной схемы отмывания доходов⁵.

Рассмотрим наиболее популярные инструменты OSINT и кратко проанализируем их возможности, предварительно классифицировав их по функционалу поиска:

1. *Операторы расширенного поиска Google* – играют важную роль в совершенствовании результатов поиска, позволяя аналитикам эффективно находить конкретную информацию. Такие операторы, как «site:», «filetype:» и «intitle:», позволяют точно получать искомые данные, обеспечивая качественную основу для последующего анализа.

2. *Мальтего* – программное обеспечение,

⁵ Most Common Anti-Money Laundering (AML) Challenges // Blog / Social Links / Data-driven investigations [Electronic resource] – Access mode: <https://blog.sociallinks.io/osint-in-anti-money-laundering-aml-investigations-unmasking-financial-shadows/#5most> (Access data: 16.03.2024).



представляющее мощный инструмент визуализации данных, который облегчает анализ ссылок и сбор информации. Позволяет аналитикам визуализировать связь между объектами, помогая установить скрытые отношения в финансовых транзакциях. Является эффективным инструментом для разведки в отношении финансовых компаний, лиц, представляющих интерес, веб-сайтов, профилей в социальных сетях, источников новостей и даже транзакций с криптовалютой.

3. *Платформы социальных сетей.* Такие инструменты, как Twitter Advance Search, Facebook ID и Picuki для Instagram, позволяют аналитикам отслеживать общедоступные профили и отслеживать взаимодействия пользователей, а также их связи между собой.

4. *Shodan* – специализированная поисковая система, которая сканирует и индексирует подключенные к Интернету устройства. Позволяет выявить уязвимость систем и потенциальные каналы для незаконной деятельности, такие как операции по добыче криптовалюты (майнинг).

5. *Исследование блокчейна.* В расследованиях, связанных с криптовалютами, исследователи блокчейнов, такие, как BitcoinWhoisWho, WalletExplorer и Etherscan, предлагают информацию о транзакциях, адресах кошельков и связанных с ними метаданных.

6. *Механизм обратного пути (Wayback Machine)* – ресурс для доступа к архивным веб-страницам. Используется для отслеживания исторической эволюции веб-сайтов, предоставляя информацию о происхождении и развитии потенциально незаконной деятельности.

7. *Базы данных публичных записей* – доступ к публичным базам данных записей, таким как сведения о собственности, реестры предприятий, санкционные списки и судебные документы. Предоставляют информацию о физических и юридических лицах, участвующих в финансовых операциях. Такие веб-сайты, как PACER и OpenCorporates, предоставляют обширные хранилища юридических и финансовых

данных. OpenSanctions представляет собой обширное хранилище данных о всемирных санкциях и списках наблюдаемых политических партий, подвергшихся санкциям, политически значимых лицах (ПДЛ) и других субъектов повышенного риска.

8. *Google Планета Земля.* Аналитики могут исследовать физические местоположения, связанные с подозрительными компаниями или транзакциями благодаря Google Earth, Street View и DualMap. Эти инструменты могут помочь проверить адреса и обнаружить скрытые активы.

9. *Базы данных регистрации доменных имен.* Такие инструменты, как Who.is и WhoisDomainTools, позволяют получить сведения о владельце и деталях регистрации интернет-доменов. Позволяет использовать информацию для выявления связей между организациями, подставными компаниями и отслеживания происхождения подозрительных веб-сайтов.

10. *Поисковые системы даркнета.* Специализированные поисковые системы, такие как Ahmia, облегчают доступ к области Интернета, не индексируемой традиционными поисковыми системами. Используются эти инструменты для мониторинга подпольных рынков, форумов и незаконной деятельности в поисках потенциальных клиентов с помощью браузера TOR.

11. *Инструменты языкового перевода.* Учитывая глобальный характер финансовых преступлений, такие инструменты языкового перевода, такие как Google Translate или DeepL, незаменимы для аналитиков, работающих с неанглоязычными источниками. Они облегчают извлечение важной информации из документов или сообщений на иностранных языках.

12. *Поиск судов и самолетов.* Vessel Finder, Marine Traffic и FlightRadar24 предлагают возможности динамического отслеживания в реальном времени как морских, так и воздушных судов, в т.ч. сведения о полетных данных. Инструменты позволяют собирать важную информацию для оценки потенциального участия в незаконной



торговле, контрабандной деятельности или нарушениях санкций.

13. *База данных офшорных утечек ICIJ* (International Consortium of Investigative Journalists – Международный консорциум журналистов-расследователей). Служат хранилищем документов, собранных ICIJ, об офшорных структурах, связанных с отмыванием денег. База данных содержит информацию о бенефициарных собственниках, а также их связях с офшорными организациями.

14. *Панель расследований OCCRP* (Organised Crime and Corruption Reporting Project – Центр по исследованию коррупции и организованной преступности). Предлагает специалистам доступ к комплексному набору инструментов и данных для параллельных финансовых расследований, которые содержат отчеты компаний, общедоступные документы и новостные статьи. Этот инструмент позволяет аналитикам принимать обоснованные решения и оценивать потенциальные риски, связанные с различными организациями в рамках их деятельности.

15. *Агрегатор новостей. NewsNow* предлагает информационный ресурс, предоставляет доступ к обширному массиву статей, позволяя внимательно отслеживать ключевые слова, относящиеся к конкретной организации или событию. Пользователи имеют возможность настроить эту платформу в соответствии со своими индивидуальными требованиями и целями. Такая адаптивность гарантирует аналитикам получение наиболее актуальной и своевременной информации, что позволяет им быть в курсе важнейших событий в выбранных областях⁶.

Заключение. Отметим, что интеграция деятельности OSINT в усилия по противодействию легализации (отмыванию) доходов – это не просто выбор, а необходимость в постоянно меняющейся сфере профилактики криминальной легализации. Динамичный характер незаконной финансовой деятельности требует профилактического подхода, а

OSINT обеспечивает решающее преимущество в борьбе с возникающими рисками и угрозами.

Используя богатую информацию, доступную в открытых источниках, правоохранители могут выявлять скрытые связи, отслеживать подозрительные транзакции и, в итоге, вносить значительный вклад в смягчение последствий криминальной легализации.

Более того, крайне важно обучать сотрудников правоохранительных органов эффективному использованию открытых источников. Это дает им навыки и знания, необходимые для навигации в сложном мире открытых источников, позволяя им проводить более надежную комплексную проверку, выявлять потенциальные риски и повышать устойчивость следственно-оперативных подразделений к широко распространенным угрозам отмывания денег и финансирования терроризма.

Вместе с тем разработка методических рекомендаций поможет установить стандарты и процедуры для использования инструментов OSINT в борьбе с отмыванием доходов. Это позволит унифицировать подход к анализу и использованию информации, что в свою очередь повысит качество работы правоохранительных органов в этой области.

Разработка методических рекомендаций по использованию инструментов OSINT в противодействии легализации (отмыванию) доходов представляет собой важную задачу, которая поможет улучшить эффективность борьбы с этим видом преступности. Правильная подготовка специалистов и установление стандартов использования инструментов OSINT сыграют ключевую роль в противодействии отмыванию доходов и обеспечении экономической безопасности государства.

Основные компоненты методических рекомендаций должны включать в себя обучение сотрудников различным методикам и техникам анализа информации, полученной из открытых источников.

⁶ Open Source Intelligence (OSINT) and AML/CFT: 15 Useful Tools / Special Eurasia [Electronic resource] – Access mode: <https://www.specialeurasia.com/2023/10/03/osint-and-aml-cft-15-tools/> (Access data: 23.03.2024).



Это включает в себя умение работать с социальными сетями, общедоступными базами данных, онлайн-платформами для анализа финансовых транзакций и другими инструментами OSINT. Кроме того, не менее важно обучение сотрудников правильной интерпретации и анализу полученной информации с целью выявления потенциальных схем отмывания денег.

Список использованной литературы:

1. Шаров, В.И. Поиск и анализ оперативно-розыскной информации в интернете / В.И. Шаров // Юридическая техника. – 2024. – № 18. – С. 411-416.
2. Иванов, В.Ю. Использование OSINT в раскрытии и расследовании преступлений / В.Ю. Иванов // Вестник Уральского юридического института МВД России. – 2023. – № 1 (37). – С. 62-66. – EDN VPIMWC.
3. Батоев, В.Б. О технологии поиска по открытым источникам «OSINT» в оперативно-розыскной деятельности / В.Б. Батоев // Вестник Уфимского юридического института МВД России. – 2023. – № 2 (100). – С. 66-71. – EDN HTHORH.
4. Янгаева, М.О. OSINT. Получение криминалистически значимой информации из сети Интернет / М.О. Янгаева, Н.О. Павленко // Алтайский юридический вестник. – 2022. – № 2. – С. 131-135.
5. Качалов, А.Г. Подготовка специалистов по работе с открытыми данными в сети интернет (OSINT) в гражданских и ведомственных вузах / А.Г. Качалов, М.М. Лантаев // Юридическая наука: история и современность. – 2021. – № 9. – С. 98-106. – EDN MXKJOE.
6. Paulson, T.M. Intelligence Issues & Developm [Electronic resource] / T.M. Paulson. – Nova Publishers, 2008. – 150 p. – Access mode: https://books.google.kz/books/about/Intelligence_Issues_and_Developments.html?id=pCOFOqD9TYQC&redir_esc=y (Access data: 16.03.2024).
7. R. Ghiloni, M. Taddeo, L. Floridi. Open Source Intelligence (OSINT) and AI: The Informational Pivot of Intelligence Analysis / 17 Feb 2023 [Electronic resource] – Access mode: <https://www.oii.ox.ac.uk/news-events/open-source-intelligence-osint-and-ai-the-informational-pivot-of-intelligence-analysis/> (Access data: 26.03.2024).

References:

1. Sharov, V.I. Poisk i analiz operativno-rozysknoj informacii v internete / V.I. Sharov // Juridicheskaja tehnika. – 2024. – № 18. – S. 411-416.
2. Ivanov, V.Ju. Ispol'zovanie OSINT v raskrytii i rassledovanii prestuplenij / V.Ju. Ivanov // Vestnik Ural'skogo juridicheskogo instituta MVD Rossii. – 2023. – № 1 (37). – S. 62-66. – EDN VPIMWC.
3. Batoev, V.B. O tehnologii poiska po otkryтым istochnikam «OSINT» v operativno-rozysknoj dejatel'nosti / V.B. Batoev // Vestnik Ufimskogo juridicheskogo instituta MVD Rossii. – 2023. – № 2 (100). – S. 66-71. – EDN HTHORH.
4. Jangaeva, M.O. OSINT. Poluchenie kriminalisticheski znachimoj informacii iz seti Internet / M.O. Jangaeva, N.O. Pavlenko // Altajskij juridicheskij vestnik. – 2022. – № 2. – S. 131-135.
5. Kachalov, A.G. Podgotovka specialistov po rabote s otkryтымi dannymi v seti internet (OSINT) v grazhdanskix i vedomstvennyh vuzah / A.G. Kachalov, M.M. Lantaev // Juridicheskaja nauka: istorija i sovremennost'. – 2021. – № 9. – S. 98-106. – EDN MXKJOE.
6. Paulson, T.M. Intelligence Issues & Developm [Electronic resource] / T.M. Paulson. – Nova Publishers, 2008. – 150 p. – Access mode: https://books.google.kz/books/about/Intelligence_Issues_and_Developments.html?id=pCOFOqD9TYQC&redir_esc=y (Access data: 16.03.2024).
7. R. Ghiloni, M. Taddeo, L. Floridi. Open Source Intelligence (OSINT) and AI: The Informational Pivot of Intelligence Analysis / 17 Feb 2023 [Electronic resource] – Access mode: <https://www.oii.ox.ac.uk/news-events/open-source-intelligence-osint-and-ai-the-informational-pivot-of-intelligence-analysis/>



intelligence-analysis/ (Access data: 26.03.2024).

АВТОРЛАР ТУРАЛЫ МӘЛІМЕТТЕР / СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

Болат Досжанұлы Еркенов – Қазақстан Республикасы Ішкі істер министрлігінің М. Есболатов атындағы Алматы академиясының докторанты, ұлттық қауіпсіздік және әскери іс магистрі, e-mail: bolat_erkenov@mail.ru.

Еркенов Болат Досжанович – докторант Алматинской академии Министерства внутренних дел Республики Казахстан имени М. Есбулатова, магистр национальной безопасности и военного дела, e-mail: bolat_erkenov@mail.ru.

Yerkenov Bolat Doszhanovic – Doctoral Student of the Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after M. Esbulatov, Master of National Security and Military Case, e-mail: bolat_erkenov@mail.ru.

Саида Айдарбекқызы Сейлханова – Қазақстан Республикасы Ішкі істер министрлігінің М. Есболатов атындағы Алматы академиясының қылмыстық құқық және криминология кафедрасының меңгерушісі, М. Есбулатова, заң ғылымдарының кандидаты, e-mail: saida_7878@mail.ru.

Сейлханова Саида Айдарбековна – начальник кафедры уголовного права и криминологии Алматинской академии Министерства внутренних дел Республики Казахстан имени М. Есбулатова, кандидат юридических наук, e-mail: saida_7878@mail.ru.

Seyilkhanova Saida Aidarbekovna – Head of the Department of Criminal Law and Criminology of the Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after M. Esbulatov, Candidate of Law, e-mail: saida_7878@mail.ru.