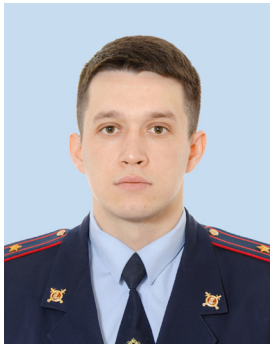
Научная статья
УДК 343.985.5
https://doi.org/10.36511/2078-5356-2024-1-79-86



# К вопросу о получении оперативно значимой информации из открытых источников информации сети «Интернет»

***Васюков Виталий Федорович*[1, 2], *Афанасьев Алексей Юрьевич*[3, 4]**

[1]Московский государственный университет международных отношений МИД России (МГИМО), Москва, Россия

[2]Научный центр безопасности дорожного движения МВД России, Москва, Россия

[3]Нижегородская академия МВД России, Нижний Новгород, Россия

[4]Национальный исследовательский Нижегородский государственный университет имени Н. И. Лобачевского, Нижний Новгород, Россия

[1, 2]vvf0109@yandex.ru.

[3, 4]afanasev_alexey@bk.ru

***Аннотация.*** Статья посвящена изучению возможности сбора оперативно значимых сведений из открытых источников. Исследуются перспективы внедрения метода получения информации из открытых источников информации в сети «Интернет». Цель исследования определяется необходимостью усовершенствования данного метода при выявлении и раскрытии преступлений. Рассматриваются основные этапы сбора общедоступной информации, определяются критерии ее оценки. Делается вывод о важности использования рассматриваемого метода при получении оперативно значимой информации.

***Ключевые слова:*** открытые источники информации, метод *OSINT*, сбор информации, сеть «Интернет», метаданные

***Для цитирования:*** Васюков В. Ф., Афанасьев А. Ю. К вопросу о получении оперативно значимой информации из открытых источников информации сети «Интернет» // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2024. № 1 (65). С. 79–86. https://doi.org/10.36511/2078-5356-2024-1-79-86.

Original article

# On the issue of obtaining operationally significant information from open sources of information on the Internet

***Vitaly F. Vasyukov*[1, 2], *Alexey Yu. Afanasyev*[3, 4]**

[1]Moscow State University of International Relations of the Ministry of Foreign Affairs of Russia (MGIMO), Moscow, Russian Federation

[2]Scientific Center for Road Safety of the Ministry of Internal Affairs of Russia, Moscow, Russian Federation

[3]Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, Nizhny Novgorod, Russian Federation

[4]National Research Nizhny Novgorod State University named after N. I. Lobachevsky, Nizhny Novgorod, Russian Federation
[1, 2]vvf0109@yandex.ru.
[3, 4]afanasev_alexey@bk.ru

***Abstract.*** The article is devoted to studying the possibility of collecting operationally significant information from open sources. The prospects for introducing a method for obtaining information from open sources of information on the Internet are explored. The purpose of the study is determined by the need to improve this in identifying and solving crimes. The main stages of collecting publicly available information are considered, and the criteria for its evaluation are determined. The conclusion is drawn about the importance of using the method in question when obtaining operationally significant information.

***Keywords:*** open sources of information, OSINT method, information collection, Internet, metadata

***For citation:*** Vasyukov V. F., Afanasyev A. Yu. On the issue of obtaining operationally significant information from open sources of information on the Internet. *Legal Science and Practice: Journal of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 2024, no. 1 (65), pp. 79–86. https://doi.org/10.36511/2078-5356-2024-1-79-86.

Развитие сети «Интернет» коренным образом изменило природу публичной информации, появилось больше возможностей каждому пользователю делиться новостями, мнениями, знаниями без какого-либо дополнительного редактирования. При этом целые корпорации стали создавать платформы, которые в настоящее время повсеместно побуждают пользователей добровольно делиться широким спектром личной информации на персональных сайтах, в социальных сетях, блогах, чатах и т. д.

В результате в современном мире редко можно встретить человека, который не пользуется сетью «Интернет» и не имеет учетные записи на различных сайтах социальных сетей. При этом в определенных социальных группах стало нормой размещать в общем доступе свои фотографии, видеоролики, в том числе сделанные в отдельные периоды жизни [1, с. 356].

Не являются исключением и лица, занимающиеся противоправной деятельностью. В отдельных случаях сеть «Интернет» является неотъемлемым инструментом популяризации ложной информации, служащей элементом механизма мошенничества.

С точки зрения оперативно-розыскной деятельности возможность идентификации человека по его цифровым следам в киберпространстве предполагает использование современных методов и средств поиска и анализа оперативно значимой информации в открытом и закрытом сегменте сети «Интернет», которая в совокупности позволяет обеспечить решение задач борьбы с преступностью в целом [2, с. 68].

Информация, полученная в результате анализа результатов оперативно-розыскных мероприятий, может быть дополнена сведениями из открытых источников сети «Интернет», получивших общепринятое обозначение *OSINT* (*Open Source Intelligence* — разведка на основе открытых источников), под которыми понимается систематический сбор, обработка и анализ информации, находящейся в открытом доступе [3].

Начало разработки указанного метода было положено во время Второй мировой войны, когда У. Донован в структуре Управления стратегических служб было создано подразделение по анализу общедоступной информации. Сотрудники подразделения анализировали содержание газет, журналов и радиопередач иностранных государств [4].

В настоящее время метод *OSINT* в той или иной мере применяется как один из главных инструментов раскрытия преступления, а также поиска скрывшихся преступников.

Метод получения информации из открытых источников информации условно следует разделять на три этапа. На *первом этапе* производится определение параметров запроса — формируется информация, которую необходимо получить в ходе поиска. Для этого выделяются основные ключевые слова (ФИО, псевдонимы, название аккаунтов, никнеймы, номера телефонов, адреса электронной почты). Как правило, такая информация может быть получена в ходе первоначальных оперативно-розыскных мероприятий. На *втором этапе* происходит загрузка и обработка данных с помощью различных ресурсов, к которым может получить доступ оперативный сотрудник.

На *третьем этапе* в результате проведенного анализа делается выгрузка данных, которая может быть получена как вручную субъектом мониторинга, так и в автоматизированном режиме с помощью программного обеспечения

либо специализированных аппаратно-программных комплексов. При этом в случае получения информации в автоматизированном режиме производится ее *визуализация,* то есть сегментное экспонирование данных в графическом формате (таблицы, изображения, графы, диаграммы и другие интуитивно понятные формы).

В отдельных случаях *OSINT* является незаменимым инструментом получения оперативно значимой информации о незаконной деятельности организованных групп, занимающихся незаконным обналичиваем денежных средств, распространением наркотиков, оружия, порнографических материалов и др. Как показывает практика, довольно часто участники таких групп размещают свой адрес/идентификатор (связанный с их онлайн-профилем и псевдонимом) на форумах (*Reddit, 4Chan, 8Chan*) или в разделах комментариев на сайтах, посвященных специализированной тематике [5, с. 132]. В данном контексте следует упомянуть о существовании десятков сайтов, специально предназначенных для выявления пользователей аккаунтов и связанных с ними адресов (например, *walletexplorer.com*).

Большой пласт информации находится в сети «Даркнет», к которой нельзя получить доступ с помощью стандартных веб-браузеров, при этом общеизвестные поисковые системы не способны индексировать содержимое этой сети. Для получения доступа необходимо использовать специализированное программное обеспечение — *TOR, I2P, Freenet* и др. [6].

Между тем мониторинг информационных ресурсов в данной сети также является частью метода получения информации из открытых источников. В частности, особую важность могут представлять сведения, полученные при исследовании специализированных форумов, созданных для общения покупателей и продавцов о сведениях, вещах, услугах, имеющих криминальный характер (*Dread, Darknet Avengers, The Hub, Exploit.in* и др.).

На таких форумах в анонимном режиме пользователи свободно делятся информацией о законспирированных сервисах, распространяют адреса этих сервисов, предлагаемые ими товары и услуги, дают комментарии о качестве сервиса, приводят никнеймы наиболее (или наименее) успешных трейдеров.

В этой связи следует исходить из того, что никнеймы, используемые в сети лицами, осуществляющими незаконную деятельность, могут остаться неизменными. Это объясняется тем, что, во-первых, успех их незаконной коммерческой деятельности в сети, как правило, тесно связан с их репутацией (т. е. с комментариями, оставленными о них на онлайн-площадках или форумах). Во-вторых, лица, представляющие оперативный интерес, проводят в сети значительную часть своей жизни, сильно привязываются к цифровым псевдонимам, которые становятся неотъемлемой частью их виртуальной личности.

*Так, например, после ареста в рамках расследования дела об использовании клонированных дебетовых карт американский хакер Альберт Гонсалес начал сотрудничать с Секретной службой США, консультируя и обучая ее агентов по вопросам, связанным с информационными технологиями.*

*Однако одновременно с этим Гонсалес вновь организовал работу группы хакеров, с которой провел серию крупных компьютерных атак на системы нескольких американских компаний, в результате чего им были получены персональные данные миллионов пользователей кредитных карт. В дальнейшем эти данные продавались Гонсалесом третьим лицам в целях изготовления карт-клонов, позволяющих получить доступ к счетам клиентов банковских организаций. Причастность Гонсалеса к этой незаконной деятельности была обнаружена после ареста очередного «покупателя данных» при его попытке въезда в США. Анализ содержимого его ноутбука показал, что никнеймом его сообщника был "Soup Nazi". Точно такой же псевдоним Гонсалес использовал с момента своего первого задержания и сохранял его даже при взаимодействии с агентами Секретной службы* [7].

Следует иметь в виду, что виртуальные псевдонимы часто имеют определенную корреляцию как в открытом, так и закрытом сегменте сети, что может связать незаконную виртуальную деятельность фигуранта с его реальной личностью. Например, при осуществлении анонимного серфинга могут использоваться одни и те же криптоадреса и при законной деятельности, либо может использоваться адрес электронной почты, связанный с аккаунтом, который уже был ранее скомпрометирован.

Метод *OSINT* может быть эффективен и в рамках получения информации о незарегистрированных криптобиржах, предоставляющих услуги лицам, занимающимся легализацией преступных доходов с использованием криптовалютных обменников, а также *P2P*-платформ.

Это связано с тем, что подобные криптобиржи работают по той же репутационной схеме, что и нелегальные онлайн-рынки, рентабельность которых во многом будет зависеть от отзывов покупателей в специальных окнах для комментариев или на специализированных форумах, где другие пользователи получают информацию о качестве сервиса (о том, работает ли он еще или уже закрыт, не является ли он мошенническим и т. д.).

В таком контексте оперативные сотрудники могут анонимно получить доступ к этим форумам или страницам, как и любой другой пользователь сети, и в целях установления сведений о незаконных или незарегистрированных криптобиржах, действующих в интересующей стране (или предоставляющих услуги лицам из этой страны), и, исходя из этого, попытаться выявить тех, кто может работать с лицом, представляющим оперативный интерес [8, с. 538].

Информация из открытых источников также может быть полезна для лучшего понимания образа жизни, активов подозреваемого или мест, где он проживает, осуществляет деловую или общественную деятельность. Это связано с тем, что иногда даже самые аккуратные злоумышленники могут раскрыть компрометирующую информацию через публикации в социальных сетях.

Общепринято говорить о двух типах общедоступных сведений, которые могут быть использованы в оперативных целях. Первый тип включает в себя информацию, размещенную пользователем (сообщения, фотографии, видео и т. д.), отражающую информацию о его окружении, местоположении, статусе, идеологии и т. д. Так, к примеру, фотографии могут содержать определенные «метки», связывающие их с профилями пользователей социальной сети, или людей, не имеющих аккаунты в этой социальной сети).

Второй тип данных включает в себя сведения о технических характеристиках файлов — метаданных. Например, данные *EXIF (Exchangeable image file format*) можно обнаружить при исследовании видеофайлов, а также при анализе изображений. Также можно получить информацию об аппаратных устройствах, с помощью которых было сделано исследуемое видео или изображение.

Следует добавить, что в зависимости от используемого оборудования метаданные изображения или видеозаписи могут также включать информацию о дате, времени и месте, в котором были они созданы. Указанные данные дают возможность установить первоначальную информацию о лицах или организациях, связанных с этими файлами, а также аккаунтами в социальных сетях, на которых они были размещены (самый тривиальный пример — с помощью сертификатов *SSL (Secure Sockets Layer)*, которые в определенных условиях позволяют определить владельца сайта).

Преимущество использования *OSINT* в качестве инструмента выявления противоправной деятельности заключается в том, что он не требует от сотрудников оперативных подразделений углубленных знаний технического характера, то есть мониторинг пользовательской активности на первоначальной стадии может производиться без привлечения специалистов.

Кроме того, появились различные технологические инструменты, значительно увеличивающие эффективность поиска информации из открытых источников. Так, в настоящее время существует ряд поисковых систем, ориентированных на конкретные поисковые запросы.

Как отмечает П. А. Фаниев, в поисковом сервисе *Google* используется альтернативная технология *PageRank*, принцип ранжирования информации в зависимости от «важности» страницы, которая зависит от количества и качества ссылающихся на нее страниц. Иными словами, чем больше ссылок ведет на страницу, тем более важной она признается и тем ближе она будет в очередности в выводе ответа на поисковый запрос [9, с. 84].

Между тем специализированная поисковая система *NameCHK* представляет собой инструмент для проверки наличия имени пользователя на множестве онлайн-сервисов. В свою очередь, поисковая система *Tineye* позволяет установить, имеется ли имя пользователя в сети «Интернет». При этом ресурс *Pipl* ищет совпадения по различным критериям: имена, адреса электронной почты, номера телефонов и др.

Также в открытом доступе существуют сайты, предоставляющие информацию о характере и статусе (онлайн или офлайн) скрытых сервисов или страниц в сети «Даркнет», а также их зеркалах (например, *Dark.fail, TNO Dark Web Monitor* и др.).

В контексте сказанного не будет лишним упомянуть, что в сети «Даркнет» для выполнения задач *OSINT* можно использовать поисковую систему *GitHub*. Между тем отдельного внимания заслуживает информационная платформа *Maltego*, которая используется как инструмент сбора данных о конкретных объектах, в качестве которых могут выступать люди, компании

или веб-сайты. Удобство платформы заключается в том, что полученные в ходе мониторинга данные выгружаются в виде набора связанных графов [10, с. 74].

При этом поисковая система *Spokeo* сканирует огромный репозиторий открытых источников, таких как социальные сети, адреса электронной почты, публичные записи, телефонные справочники и др., а затем выдает информацию, найденную на конкретное лицо или организацию [11, с. 320].

Следует отметить, что сотрудники Базельского института (Швейцария) разработали собственный инструмент поиска открытых источников информации "*Basel Open Intelligence*", осуществляющий автоматический поиск по имени человека или организации в сочетании с более чем 200 ключевых слов. Сведения, найденные в результате поиска, перечисляются вместе с основным текстом, извлеченным из веб-сайта, исключая не относящийся к делу контент (например, рекламу, меню или уведомления о *cookie*), а выделенные ключевые слова подчеркиваются для облегчения чтения [12].

В отдельных иностранных государствах сбором сведений из открытых источников занимаются частные организации так называемые «брокеры данных». На основании обработки информации из множества источников такими организациями составляются подробные персональные профили, включающие следующие данные: пол, возраст, образование, история трудоустройства, семейное положение, характер использования социальных сетей, политические взгляды, уровень доходов, наличие транспортных средств и недвижимости и т. д. При сотрудничестве уполномоченных сотрудников правоохранительных органов с такими организациями для составления цифрового профиля полученная информация может стать бесценной [13].

Как отмечается в иностранной литературе, метод *OSINT* имеет ряд преимуществ перед классическими мероприятиями, направленными на получение оперативно значимой информации:

1) рентабельность — сбор данных *OSINT* очень экономичен по сравнению с традиционной разведывательной деятельностью;

2) простота доступа — мероприятия по сбору данных могут проводиться в онлайн-режиме, при этом характер онлайн-контента делает его доступным из любой точки мира и в любое время;

3) доступность — ресурсы *OSINT* собираются только из общедоступных источников без ограничения прав и законных интересов граждан [14].

Между тем существуют определенные проблемы при использовании указанного метода:

1) неограниченный объем — может быть получен большой объем данных, который возможно обработать только с использованием аппаратно-программных комплексов;

2) достоверность — несмотря на полезность полученных сведений в рамках проведения мониторинга сети, чаще всего они имеют ориентирующий характер, поэтому не будут отражаться в материалах уголовного дела. Более того, след абонентской активности в сети может быть оставлен умышленно в целях противодействия правоохранительным органам;

3) трудоемкость анализа — даже в случае обработки данных с помощью специализированного программного (аппаратного) обеспечения, полученные результаты необходимо проверять оперативным путем, что может привести к привлечению большого количества сотрудников оперативного подразделения [15].

В то же время, как показывает зарубежный опыт, при раскрытии преступлений метод *OSINT* наиболее эффективен в сочетании с традиционными методами оперативного сыска.

Так, в 2017 году 18-летняя Аиша Зугбих-Коллинз была найдена в своей квартире мертвой. Причиной смерти стала передозировка синтетическим опиоидом *U*-47700 (*U*4). Мать жертвы, подозревая, что та приобрела наркотик в сети «Интернет», предоставила сотрудникам полиции адрес электронной почты дочери.

В ходе проведения осмотра квартиры погибшей были найдены следы наркотического вещества в упаковке теста на беременность. Оперативным путем установлено, что этот тест был получен потерпевшей в местном почтовом отделении незадолго до смерти.

В свою очередь возле трупа также был найден блокнот с записью буквенно-цифрового кода, оказавшегося личным криптографическим ключом жертвы для программы шифрования сообщений *Pretty Good Privacy (PGP).* Получив доступ к электронной почте потерпевшей с помощью этого кода, полицейские смогли выяснить, что наркотическое вещество было приобретено на виртуальном рынке в сети «Даркнет» у продавца под псевдонимом *"Pedro el grande"*, который по данным сайта совершил более 10 тыс. сделок.

С использованием легендированного аккаунта сотрудником полиции была проведена

Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, 2024, no. 1 (65)

контрольная закупка у продавца *"Pedro el grande"* дозы наркотического средства *U*4. После получения посылки в распоряжении полиции оказалась аналогичная упаковка наркотика в виде теста на беременность. Как в последующем оказалось, указанный тест в качестве маскирующей упаковки был приобретен фигурантом через онлайн-магазин, принимающий оплату только криптовалютой. При чем к криптокошельку, с которого прошел платеж за тесты, были прикреплены два адреса электронной почты, созданных Т., проживающим в американском городе Гринвелл.

В дальнейшем были получены сведения о том, что Т. получал многочисленные международные посылки из Китая (одной из стран, где производится наркотик *U*4). Установив оперативное наблюдение за домом Т., сотрудниками полиции был выявлен весь механизм отправки наркотического вещества, осуществляемого с помощью городской почтовой службы. Таким образом, следует сделать вывод о том, что умелое комбинирование и анализ полученных сведений может иметь значение для раскрытия преступлений [16].

Полезными источниками информации о человеке или группе людей являются социальные сети, где люди делятся личной информацией и взаимодействуют с семьей, друзьями, коллегами, незнакомыми людьми. При чем сведения, полученные из одной социальной сети, могут быть вручную включены в поисковые запросы в других социальных сетях, а объединение всей информации, как правило, может быть очень результативным.

Также важным методом сбора информации в социальных сетях является отправка поисковых запросов. Самый простой подход использует функции внутреннего поиска, предоставляемые самой социальной сетью. Однако функции поиска различаются в зависимости от соответствующей социальной сети, используемой при мониторинге [17, с. 140].

Существует ряд приложений, расширений браузера или веб-сервисов, специализированных на различных социальных сетях, с помощью которых можно систематизировать определенную информацию. Проблемы возникают из-за того, что некоторые социальные сети позволяют применять строгие настройки конфиденциальности в профиле, что препятствует детальному изучению. Однако можно идентифицировать публичные сообщения, которые напрямую не отображаются на странице личного профиля. Также следует проанализировать подключенные учетные записи, не имеющие ограничения по доступу и раскрывающие информацию о лице, представляющего оперативный интерес.

Резюмируя вышесказанное, отметим, что использование метода получения сведений из открытых источников может способствовать получению оперативно значимой информации при раскрытии преступлений, не только совершенных с использованием информационных технологий, но и реализованных классическим способом. Это делает сбор данных из таких источников чрезвычайно важной задачей для оперативных подразделений и, по сути, формирует приоритетные направления в поиске лиц, осуществляющих противоправную деятельность.

**Список источников**

1. Преступления в сфере высоких технологий и информационной безопасности: учебное пособие / В. Ф. Васюков [и др.]; под науч. ред. А. Г. Волеводза. Москва: Прометей, 2023. 1086 с.

2. Батоев В. Б. О технологии поиска по открытым источникам "OSINT" в оперативно-розыскной деятельности // Вестник Уфимского юридического института МВД России. 2023. № 2 (100). С. 66–71.

3. Akhgar B., Bayerl P., Sampson F. Open Source Intelligence Investigation. *Advanced Sciences and Technologies for Security Applications*. Springer, Cham. 2016. URL: https://doi.org/10.1007/978-3-319-47671-1_10.

4. Böhm I., Lolagar S. Open source intelligence. Int. Cybersecur // Law Rev. 2021. No 2. Pp. 317–337.

5. Янгаева М. О., Павленко Н. О. OSINT. Получение криминалистически значимой информации из сети Интернет // Алтайский юридический вестник. 2022. № 2. С. 131–135.

6. Pastor-Galindo J., Nespoli P., Gómez Mármol F., & Martínez Pérez G. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends // IEEE Access. 2020. No. 8. Pp. 10282–10304.

7. Lee D. Study on OSINT-Based Security Control Monitoring Utilization Plan. Studies in Computational Intelligence. 2023. Vol. 1074. Pp. 576–590.

8. Рукавишникова Г. А., Титов П. М. Общая характеристика технологий OSINT на платформе Telegram для использования в получении значимой информации // Вопросы российской юстиции. 2023. № 27. С. 537–546.

9. Фаниев П. А. Тихая разведка *OSINT* как способ получения криминалистически значимой информации // Научный портал МВД России. 2023. № 2 (62). С. 82–87.

10. Гаянов А. А. Разведка с использованием OSINT-технологий в интересах правоохранитель-

ных органов // Вопросы деятельности подразделений органов внутренних дел Российской Федерации: сборник научных трудов. Тверь, 2023. С. 73–78.

11. Минченко В., Вильдяйкин Г. Ф. Разведка на основе открытых // источников (*OSINT*) и ее методология в современных реалиях: материалы III Всероссийской национальной научной конференции студентов, аспирантов и молодых ученых: в 3-х ч. / отв. ред. Э. А. Дмитриев [и др.]. 2020. С. 319–322.

12. Голушко А. П., Дрянных Ю. Ю. Цель и задачи поиска информации в открытых источниках (*Open Source Intelligence*) // Внедрение результатов инновационных разработок: проблемы и перспективы: сборник статей по итогам Международной научно-практической конференции, 2019. С. 158–161.

13. Vykhodets Yu. O., Teteriatnyk H. K. Some issues of the use of osint in the investigation of crimes in the conditions of military aggression of the Russian Federation. Legal Novels. 2022. No. 18. Pp. 70–76.

14. Böhm I., Lolagar S. Open source intelligence. Cybersecur. Law. Rev. 2021. No. 2. Pp. 317–337.

15. Quick D., Choo KK., R. Digital Forensic Data and Open Source Intelligence (DFINT+OSINT). In: Big Digital Forensic Data. SpringerBriefs on Cyber Security Systems and Networks. Springer, Singapore, 2018.

16. Rajamäki J. OSINT on the dark web: child abuse material investigations. Information & Security. 2022. Vol. 53. Pp. 21–32.

17. Клевцов К. К. Особенности взаимодействия правоохранительных органов с зарубежными поставщиками услуг виртуальных валют (на примере LocalBitcoins) // Вестник Московского университета МВД России. 2023. № 1. С. 139–145.

## References

1. Crimes in the field of high technology and information security: Textbook. allowance / V. F. Vasyukov [and others] / ed. by A. G. Volewodza. Moscow: Prometheus Publ., 2023. 1086 p. (In Russ.)

2. Batoev V. B. On open source search technology “OSINT” in operational investigative activities. *Bulletin of the Ufa Law Institute of the Ministry of Internal Affairs of Russia*, 2023, no. 2 (100), pp. 66–71. (In Russ.)

3. Akhgar B., Bayerl P., Sampson F. Open Source Intelligence Investigation. *Advanced Sciences and Technologies for Security Applications.* Springer, Cham. 2016. URL: https://doi.org/10.1007/978-3-319-47671-1_10.

4. Böhm I., Lolagar S. Open source intelligence. Int. Cybersecurity. *Law Rev Publ*., 2021, no. 2, pp. 317–337.

5. Yangaeva M. O., Pavlenko N. O. OSINT. Obtaining forensically significant information from the Internet. *Altai Legal Bulletin*, 2022, no. 2, pp. 131–135. (In Russ.)

6. Pastor-Galindo J., Nespoli P., Gómez Mármol F., & Martínez Pérez G. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends // *IEEE Access,* 2020, no. 8, pp. 10282–10304.

7. Lee D. Study on OSINT-Based Security Control Monitoring Utilization Plan. Studies in Computational Intelligence, 2023, vol. 1074, pp. 576–590.

8. Rukavishnikova G. A., Titov P. M. General characteristics of OSINT technologies on the Telegram platform for use in obtaining significant information. *Issues of Russian Justice*, 2023, no. 27, pp. 537–546. (In Russ.)

9. Faniev P. A. Silent OSINT reconnaissance as a way to obtain forensically significant information. *Scientific portal of the Ministry of Internal Affairs of Russia,* 2023, no. 2 (62), pp. 82–87. (In Russ.)

10. Gayanov A. A. Intelligence using OSINT technologies in the interests of law enforcement agencies. Issues of activity of departments of internal affairs bodies of the Russian Federation: collection of scientific papers. Tver, 2023. Pp. 73–78. (In Russ.)

11. Minchenko V., Vildyaykin G. F. Intelligence based on open // sources (OSINT) and its methodology in modern realities. Materials of the III All-Russian National Scientific Conference of Students, Postgraduate Students and Young Scientists: in 3 parts / ed. by E. A. Dmitriev (responsible editor) [and others]. 2020. Pp. 319–322. (In Russ.)

12. Golushko A. P., Dryannykh Yu. Yu. The purpose and objectives of searching for information in open sources (Open Source Intelligence). Implementation of the results of innovative developments: problems and prospects*:* collection of articles based on the results of the International Scientific and Practical Conference. 2019. Pp. 158–161. (In Russ.)

13. Vykhodets Yu. O., Teteriatnyk H. K. Some issues of the use of osint in the investigation of crimes in the conditions of military aggression of the Russian Federation. *Legal Novels*, 2022, no. 18, pp. 70–76.

14. Böhm I., Lolagar S. Open source intelligence. Cybersecur. *Law. Rev,* 2021, no. 2, pp. 317–337.

15. Quick D., Choo K.K.R. Digital Forensic Data and Open Source Intelligence (DFINT+OSINT). In: Big Digital Forensic Data. SpringerBriefs on Cyber Security Systems and Networks. Springer, Singapore, 2018.

16. Rajamäki J. OSINT on the dark web: child abuse material investigations. *Information & Security Publ.,* 2022, vol. 53, pp. 21–32.

17. Klevtsov K. K. Features of interaction between law enforcement agencies and foreign virtual currency service providers (using the example of LocalBitcoins). *Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia*, 2023, no. 1, pp. 139–145.

**Информация об авторах**

***В. Ф. Васюков*** — доктор юридических наук, профессор, главный научный сотрудник отдела изучения проблем нормативного правового и аналитического обеспечения Научного центра БДД МВД России, профессор кафедры уголовного права, уголовного процесса и криминалистики Московского государственного университета международных отношений МИД России (МГИМО);

***А. Ю. Афанасьев*** — кандидат юридических наук, начальник кафедры криминалистики Нижегородской академии МВД России, доцент кафедры судебной экспертизы Национальный исследовательский Нижегородский государственный университет имени Н. И. Лобачевского.

**Information about the authors**

***V. F. Vasyukov*** — Doctor of Sciences (Law), Professor, Chief Researcher of the Department for Studying Problems of Regulatory Legal and Analytical Support of the Scientific Center for Traffic Safety of the Ministry of Internal Affairs of Russia, Professor of the Department of Criminal Law, Criminal Procedure and Forensics of the Moscow State University of International Relations of the Ministry of Foreign Affairs of Russia (MGIMO);

***A. Yu. Afanasyev*** — Candidate of Sciences (Law), Head of the Department of Criminology of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, Associate Professor of the department of forensic examination National Research Nizhny Novgorod State University named after N. I. Lobachevsky.

Статья поступила в редакцию 01.02.2024; одобрена после рецензирования 26.02.2024; принята к публикации 05.03.2024.

The article was submitted 01.02.2024; approved after reviewing 26.02.2024; accepted for publication 05.03.2024.