Научная статья
УДК 343.9

О ТЕХНОЛОГИИ ПОИСКА ПО ОТКРЫТЫМ ИСТОЧНИКАМ «OSINT» В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Владимир Батоевич Батоев
Научно-производственное объединение «Специальная техника и связь МВД России», Москва, Россия, vbatoev@mail.ru

Аннотация. В статье рассмотрены вопросы использования сбора и анализа оперативно значимой информации по открытым источникам в сети Интернет в целях решения задач борьбы с преступностью. Освещены передовые практики добывания информации, представляющей оперативный интерес. Автором обозначен ряд проблем правового и организационного характера в деятельности отечественных оперативно-розыскных органов, устранение которых предлагается рассматривать направлением совершенствования информационно-аналитического обеспечения оперативно-розыскной деятельности. С учетом огромного потенциала повсеместного внедрения и использования технологий разведки по открытым источникам автором обосновывается необходимость придания им приоритетного значения при проведении научных исследований, подготовке специалистов данного направления, материально-техническом оснащении и переоснащении современными технологическими средствами деятельности оперативно-розыскных подразделений.

Ключевые слова: преступность, разведка, открытые источники, информация, оперативно-розыскная деятельность.

Для цитирования: 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.

Original article

ON THE OPEN SOURCE SEARCH TECHNOLOGY “OSINT” IN OPERATIONAL INVESTIGATIVE ACTIVITIES

Vladimir B. Batoev
Scientific and Production Association “Special Equipment and Communications” of the Ministry of Internal Affairs of Russia, Moscow, Russia, vbatoev@mail.ru

Abstract. The article considers the issues of using the collection and analysis of operationally relevant information on open sources on the Internet in order to solve the problems of combating crime. The best practices of obtaining information of operational interest are highlighted. The author identifies a number of legal and organizational problems in the activities of domestic operational investigative bodies, the elimination of which is proposed to be considered as a direction for improving information and analytical support for operational investigative activities. Taking into account the huge potential of the widespread introduction and use of open source intelligence technologies, the author substantiates the need to give them priority when conducting scientific research, training specialists in this field, equipping and re-equipping operational search units with modern technological means.

Keywords: crime, intelligence, open sources, information, operational investigative activities.

For citation: Batoev V. B. On the open source search technology “OSINT” in operational investigative activities // Bulletin of Ufa Law Institute of the Ministry of Internal Affairs of Russia. 2023. No. 2 (100). P. 66–71.

В настоящее время в условиях тотальной цифровизации практически всех сфер общественных отношений вопросы информационного обеспечения деятельности оперативных подразделений органов внутренних дел (далее – ОВД) приобрели качественно иное значение, где процессы оперативного и разведывательного поиска оперативно значимой информации сместились в сторону использования современных достижений в области добывания, анализа и хранения цифровой информации. Перед оперативно-розыскными органами ОВД встала задача совершенствования имеющихся средств и методов осуществления информационного поиска в сетевом пространстве, размеры информации в котором позволяют заключить о влиянии ее количества на качество. Ежедневно генерируемые населением огромные по размерам массивы разнородной информации предоставляют субъектам оперативно-розыскной деятельности (далее – ОРД) беспрецедентные возможности совершенствования информационного обеспечения деятельности оперативных подразделений при решении задач борьбы с преступностью посредством поиска и анализа информации об объектах оперативной заинтересованности.

Анализ практики позволяет прийти к следующим выводам: по подсчетам компаний «IDC» и «Seagate» к 2025 году общемировой объем данных превысит 175 зеттабайт[1]; ежедневно ресурсами сети Интернет пользуются около 5 млрд человек во всем мире, а на территории Российской Федерации – практически 90 % населения (около 130 млн человек), что вывело Россию на 6 место в рейтинге стран-лидеров[2]. Данные цифры позволяют заключить, что в условиях цифровизации организации общественных процессов современный индивидуум фактически лишен возможности удовлетворять ряд своих потребностей традиционным образом. В данном случае, наоборот, человеку в условиях неизбежного формирования цифрового общества и экономики в ближайшей перспективе будет предоставлен широкий спектр высокотехнологичного инструментария в рамках жизнедеятельности, когда основная масса услуг будет предоставляться в электронно-цифровой форме. Это предполагает создание цифрового профиля гражданина с его цифровыми следами в интернет-пространстве, изучение которых позволит сформировать паттерны его поведения и интернет-активности и идентифицировать как личность.

С точки зрения ОРД 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.

К числу эффективных инструментов поиска и обнаружения информации в сети Интернет следует отнести программные решения по проведению разведывательно-поисковых мероприятий по открытым источникам, иными словами использование технологии «OSINT» (Open Source Intelligence) [1]. В отечественной практике субъектов ОРД по проведению поиска в открытых источниках оперативно значимой информации сформировался положительный опыт использования аналитических комплексов, что, разумеется, не нуждается в каком-либо обосновании.

Основным предназначением подобных аппаратно-программных комплексов (далее – АПК) является поиск в открытых источниках в сети Интернет информации, ее анализ, построение взаимосвязей между событиями, фактами, явлениями, иначе говоря:

[1] Эксперт: объем данных в мире к 2025 году вырастет более чем в пять раз // URL: https://tass.ru/ekonomika/6209822 (дата обращения: 16.01.2023).

[2] Чернышенко: 90 % населения России являются пользователями Интернета // URL: https://rg.ru/2022/09/28/chernyshenko-90-naseleniia-rossii-iavliaiutsia-polzovateliami-interneta.html (дата обращения: 16.01.2023).

– обработка различных массивов информационных данных (как из сети Интернет, так и представленных на магнитных носителях) в сочетании с их объединением, формированием единой базы данных, истории событий в хронологическом порядке;

– анализ источников данных в сети Интернет по ключевым понятиям (события, организации, даты, персональные данные и др.);

– построение временных графов, взаимосвязей и взаимозависимостей;

– сигнализирование инициатору о появлении искомых событий, фактов, явлений по ключевым параметрам запроса.

Аппаратно-программные комплексы, использующие метод «OSINT», обеспечивают: формирование собственной базы архивных документов, никак не зависящей от состояния сохранности информации на первоисточнике; дальнейший поиск, оценку и систематизацию данных в архиве; проведение анализа поступивших сведений с учетом исторической ретроспективы; построение графов скрытых взаимосвязей, установить которые аналитику практически невозможно; дальнейшее сигнализирование инициатору о произошедших изменениях в цепочках данных, событий, явлений, фактов и появлении новых данных; определение приоритетности событий в рамках заданного определенного промежутка времени с предоставлением данных в визуализированном формате в виде графов, диаграмм, графиков, а также с возможностями их картирования в геоинформационных системах.

Подобные АПК используются также в рамках маркетинговой деятельности по вопросам проведения конкурентной разведки в бизнесе, организации деятельности служб безопасности коммерческих организаций и др. Однако изучение ее целей и сопоставление сквозь призму ОРД позволяет отметить, что их основная сфера использования сводится к осуществлению наблюдения за происходящими событиями по определенно заданным тематикам; получению информации из открытых источников сети Интернет; оказанию помощи аналитикам при проведении прогнозирования развития тех или иных событий и явлений, формировании отчетов и гипотез; обеспечению реализации многоступенчатого анализа сведений, включающего в себя разбор черновиков, проведение вероятностного и статистического анализа данных, извлечение формализованных и структурированных данных, проведение семантического анализа с дальнейшим извлечением фактов из неструктурированных данных.

С точки зрения негласного характера ОРД подобные АПК позволяют в графическом виде выявлять неочевидные закономерности, обусловленные частотой взаимодействия объектов оперативной заинтересованности, их геоинформационной привязкой точек возникновения данных, что в совокупности позволяет субъектам использовать «скрытые» знания. В настоящее время использование рассматриваемой технологии можно рассматривать инновационным средством повышения уровня информационного обеспечения оперативно-розыскной деятельности в рамках проведения оперативно-розыскных, оперативно-технических и оперативно-аналитических мероприятий, вид которых определяется в соответствии с целями их проведения.

Особое значение для оперативно-розыскной практики имеют возможности АПК визуализировать обработанные данные, что позволяет отображать оперативно значимую информацию в картографическом виде, в формате графиков и гистограмм с возможностью фильтрации сведений в пространственно-временном выражении; графировать выявленные «скрытые» связи и зависимости между извлеченными данными.

При этом подобные АПК используют следующие виды разведки данных – пассивную и активную. В рамках пассивной разведки АПК осуществляет сбор первоначальной информации об объекте оперативной заинтересованности в целях подбора соответствующего способа активной разведки, в рамках которой осуществляется целенаправленный сбор оперативно значимой информации об объекте оперативной заинтересованности.

Помимо проведения разведки на открытых источниках посредством использования АПК существует широкий спектр общедоступных OSINT-инструментов, которые может беспрепятственно использовать любой субъект ОРД. К их числу следует отнести:

– инструменты поиска оперативно значимой информации в мессенджерах (например, в мессенджере «Telegram» – @HowToFind_bot (информация о различных базах данных и ссылках), @AvinfoBot (информация по номеру телефона в виде ссылок на социальные сети, о марке и номере автотранспортного средства, операторе связи, о поданных объявлениях обладателя этого номера на «Avito», «Drom», «Auto» и др.), @buzzim_alerts_bot (позволяет находить человека по нику и отслеживать упоминания о нем в новостных лентах), @mailsearchbot (информация о email-адресах и паролях к ним), @deanonym_bot (информация о номере сотового телефона пользователя мессенджера «Telegram») и др.);

– поисковые системы, позволяющие выявить сообщения, группы, пользователей, ботов и др. («Tgstat.ru», «Lyzem.com», «Buzz.im» и др.);

– вспомогательные компьютерные программы утилиты, не требующие для своего функционирования операционной системы (например, «Snoop Project» – утилита для поиска людей по ник-нейму и др.).

Безусловно, потенциал данного метода заключается в его общедоступности; простоте использования; наличии огромного и постоянно нарастающего объема цифровых данных как источника оперативно значимой информации; глобальном распространении сети Интернет, где человеку все сложнее оставаться не вовлеченным в процессы цифровизации общественных отношений и удовлетворять свои потребности традиционным образом. В связи с этим данный метод повышения уровня информационного обеспечения ОРД заслуживает не только пристального внимания, но и реализации в антикриминальной практике наряду с развитием дистанционных форм контроля и надзора за лицами, представляющими оперативный интерес, роботизацией деятельности субъектов обеспечения правопорядка, использованием средств массовой коммуникации, применением технологий искусственного интеллекта и анализа больших данных [2].

Использование подобных АПК как в деятельности оперативно-розыскных органов, служб безопасности коммерческих организаций, маркетинговых компаний, так и обычными гражданами не противоречит нормам действующего законодательства. Это объясняется отсутствием прямых законодательных запретов на подобные действия, так как размещаемая информация относится к категории открытой и общедоступной, что определяется условиями использования самих ресурсов, на которых подобная информация размещается.

В деятельности оперативно-розыскных органов имеются недостатки в вопросах использования «OSINT» при решении задач ОРД. В настоящее время использование данной методики необходимо внедрить в деятельность всех без исключения оперативных подразделений ОВД. При этом рассматриваемая технология нуждается в придании ей статуса приоритетного направления совершенствования информационной основы решения задач ОРД наряду с традиционными формами и методами, и получении повсеместного внедрения и использования на всех уровнях организации ОРД.

К числу основных проблем в данной сфере относятся вопросы деанонимизации личности пользователя сети Интернет [3; 4]. В оперативно-розыскной практике выработан положительный опыт деанонимизации личности пользователей сети Интернет [5; 6; 7], особенно в деятельности оперативных подразделений ОВД по контролю за оборотом наркотиков, по противодействию экстремизму. Процессы идентификации личности пользователей информационно-телекоммуникационными ресурсами вполне реализуемы посредством деанонимизации пользователей VPN-сервисами через иные сайты, либо путем сопоставления соединений, либо деанонимизации пользователей с использованием cookie-файлов, либо с использованием отпечатков браузера и др. [8] Так, Д. М. Фарахиев

выделяет методы деанонимизации пользователей сети «TOR» на примере пассивных атак timing-атака, метод «circuit fingerprinting», а также активных атак Raptor-атака, DoS-атака, spoofing-атака и др. [9].

Невзирая на малозначимость обозначенной проблемы, отметим, что субъекты ОРД в целом и сотрудники оперативных подразделений ОВД обязаны активно использовать технологию «OSINT» в виде программного софта, мобильных приложений, аппаратно-программных комплексов при решении оперативно-розыскных задач на всех организационных уровнях, не зацикливаясь на специализации компетенций по использованию данной технологии узким кругом оперативных подразделений ОВД. Применение данного метода позволит обеспечить переход информационного обеспечения ОРД на качественно иной уровень, где посредством поиска и обработки информации из открытых источников представится возможным существенно обогатить оперативно-розыскные данные информацией ориентирующего характера, которую можно будет использовать при решении оперативно-розыскных задач.

Следует отметить, что повсеместное внедрение в оперативно-розыскную практику метода разведки по открытым источникам «OSINT» потребует создания базовых технологических условий, принятия комплекса мер организационного, правового и материально-технического характера. Особое внимание следует обратить на необходимость обеспечения данного направления деятельности оперативных подразделений ОВД специализированными высококвалифицированными кадрами, что подразумевает проведение современной подготовки и переподготовки специалистов в данной области. С юридической точки зрения полагаем, что необходима тщательная проработка на законодательном уровне вопросов использования данного метода в деятельности субъектов ОРД в целом с обозначением правовой формы, в которую данные действия будут обличены, иными словами, необходимо определить в рамках какого оперативно-розыскного мероприятия целесообразно трактовать с правовой точки зрения использование искомого метода добывания оперативно значимой информации в целом со всеми вытекающими юридическими последствиями их использования в качестве результатов ОРД в частности.

Помимо этого, считаем целесообразным на постоянной основе осуществлять мониторинг передового зарубежного опыта в рассматриваемом направлении и обращаем внимание научной общественности на необходимость проведения глубоких научных исследований в искомой сфере общественных отношений с обязательной выработкой научно обоснованных предложений и рекомендаций по вопросам подготовки и проведения разведки в открытых источниках сети Интернет.

Современные реалии и бурно протекающие технологические процессы предписывают оперативно-розыскным органам своевременно осознавать и принимать во внимание огромный потенциал поиска информации по открытым источникам «OSINT», а также придать данному направлению статус преимущественного развития информационного обеспечения ОРД, в том числе в рамках неизбежной цифровизации всех сфер организации общественных процессов.

СПИСОК ИСТОЧНИКОВ

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

2. Грибанов Е. В. Перспективные направления развития кибертехнологий предупреждения преступлений // Общество и право. 2021. № 4. С. 21–27.

3. Батоев В. Б. Использование мессенджеров в преступной деятельности: проблемы деанонимизации пользователей и дешифрования информации // Оперативник (сыщик). 2017. № 2 (51). С. 15–20.

4. Лазаренко А. В. Технологии деанонимизации пользователей TOR // Новые информационные технологии в автоматизированных системах. 2016. № 19. С. 257–262.

5. Афонькин Г. П., Смирнов Е. В., Чемерчев Д. В. Основы противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий // Полицейский вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации. 2021. № 1 (4). С. 10–17.

6. Гаврилин Ю. В., Парадников А. Г. Совершенствование выявления, раскрытия и расследования хищений, совершенных и использованием информационных банковских технологий (по итогам Всероссийского онлайн-семинара) // Труды Академии управления МВД России. 2020. № 2 (54). С. 123–130.

7. Земцова С. И. Программные продукты, используемые для деанонимизации фактов совершения наркопреступлений с использованием цифровой валюты // Криминалистика – наука без границ: традиции и новации: материалы всероссийской научно-практической конференции / сост. А. В. Бачиева, Э. В. Лантух. СПб.: Санкт-Петербургский университет МВД России, 2021. С. 112–115.

8. Поздышев Р. С. Деанонимизация личности преступника в сети Интернет // Вестник Уральского юридического института МВД России. 2022. № 2. С. 50–53.

9. Фарахиев Д. М. Способы и методы деанонимизации лиц, совершающих преступления в информационном пространстве // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. № 4. С. 249–254.

REFERENCES

1. Yangaeva M. O., Pavlenko N. O. OSINT. Obtaining criminalistically significant information from the Internet // Altai Legal Bulletin. 2022. No. 2. P. 131–135. (In Russ.)

2. Gribanov E. V. Perspective directions of development of cyber technologies of crime prevention // Society and law. 2021. No. 4. P. 21–27. (In Russ.)

3. Batoev V. B. The use of messengers in criminal activity: problems of deanonymization of users and decryption of information // Operative (detective). 2017. No. 2 (51). P. 15–20. (In Russ.)

4. Lazarenko A. V. Technologies of deanonymization of TOR users // New information technologies in automated systems. 2016. No. 19. P. 257–262. (In Russ.)

5. Afonkin G. P., Smirnov E. V., Chemerchev D. V. Fundamentals of countering crimes committed using information and telecommunication technologies // Police Bulletin of the All-Russian Institute for Advanced Training of Employees of the Ministry of Internal Affairs of Russian. 2021. No. 1 (4). P. 10–17. (In Russ.)

6. Gavrilin Yu. V., Paradnikov A. G. Improving the detection, disclosure and investigation of embezzlement committed and using information banking technologies (based on the results of the All-Russian online seminar) // Proceedings of the Academy of Management of the Ministry of Internal Affairs of Russia. 2020. No. 2 (54). P. 123–130. (In Russ.)

7. Zemtsova S. I. Software products used to deanonymize the facts of drug crimes using digital currency // Criminalistics-science without borders: traditions and innovations: materials of the All-Russian Scientific and Practical Conference / compiled by A.V. Bachieva, E. V. Lantukh. Saint Petersburg: Saint Petersburg University of the Ministry of Internal Affairs of Russia, 2021. P. 112–115. (In Russ.)

8. Pozdyshev R. S. Deanonymization of the criminal's identity on the Internet // Bulletin of Ural Law Institute of the Ministry of Internal Affairs of Russia. 2022. No. 2. P. 50–53. (In Russ.)

9. Farakhiev D. M. Ways and methods of deanonymization of persons committing crimes in the information space // Legal Science and practice: Bulletin of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia. 2022. No. 4. P. 249–254. (In Russ.)

Информация об авторе:
Батоев В. Б., кандидат юридических наук, доцент.

Information about the author:
Batoev V. B., Candidate of Law, Associate Professor.

Статья поступила в редакцию 17.01.2023; одобрена после рецензирования 27.01.2023; принята к публикации 23.06.2023.

The article was submitted 17.01.2023; approved after reviewing 27.01.2023; accepted for publication 23.06.2023.