2. Скобелев, В. Актуальные вопросы применения медиации и иных форм защиты права / В. Скобелев // Юридический мир. – 2021. – № 4. – С. 52–62.
3. Скобелев, В. Актуальные вопросы применения медиации и иных форм защиты права / В. Скобелев // Юридический мир. – 2021. – № 5. – С. 52–62.
4. Скобелев, В. Актуальные вопросы применения медиации и иных форм защиты права / В. Скобелев // Юридический мир. – 2021. – № 6. – С. 54–62.
5. Здрок, О. Н. Примирительные процедуры в гражданском процессе / О. Н. Здрок. – Минск: БГУ, 2018. – 283 с.
6. Основы альтернативного разрешения споров: пособие / В. И. Самарин [и др.]; под ред. О. В. Мороза [и др.]. – Минск: БГУ, 2016. – 223 с.
7. Таранова, Т. С. Новые вопросы о применении медиации в надзорном производстве в судах общей юрисдикции / Т. С. Таранова // Право в современном белорусском обществе: сб. науч. тр. / Нац. центр законодательства и правовых исслед. Респ. Беларусь; редкол.: Н. А. Карпович (гл. ред.) [и др.]. – Минск: Колорград, 2021. – Вып. 16. – С. 341–349.
8. Тихиня, В. Г. Медиация как примирительная процедура досудебного урегулирования гражданско-правовых конфликтов / В. Г. Тихиня // Юстиция Беларуси. – 2020. – № 8. – С. 2124.
9. Скобелев, В. П. Еще раз к вопросу об источниках регулирования гражданского процесса / В. П. Скобелев // Юстиция Беларуси. – 2019. – № 7. – С. 16–22.
10. Административно-правовые споры в социальной сфере: теоретико-прикладные вопросы / О. И. Чуприс [и др.]; под ред. О. И. Чуприс. – Минск: БГУ, 2016. – 267 с.
11. Кулюшин, Е. Н. Суд первой инстанции как субъект административного судопроизводства: автореф. дис. ... канд. юрид. наук: 5.1.3 / Е. Н. Кулюшин; Уральск. гос. юрид. ун-т. – Екатеринбург, 2022. – 31 с.
12. Мельников, А. А. Правовое положение личности в советском гражданском процессе / А. А. Мельников; отв. ред. В. С. Тадевосян. – М.: Наука, 1969. – 248 с.

УДК 343.13

РАЗВЕДКА ПО ОТКРЫТЫМ ИСТОЧНИКАМ (OSINT) ИНФОРМАЦИИ В СЛЕДСТВЕННОЙ ДЕЯТЕЛЬНОСТИ

Слащинин Олег Андреевич

*следователь главного следственного управления
Следственного комитета Республики Беларусь, ул. Фрунзе, 9, 220034,
г. Минск, Республика Беларусь, mailtemp@mail.ru*

Аннотация. В статье рассматриваются теоретические и практические аспекты разведки по открытым источникам (OSINT). Анализируются перспективы и возможные проблемы использования рассматриваемой разведывательной дисциплины в следственной деятельности.

Автором обосновывается вывод о том, что фактические данные, полученные с использованием OSINT, должны оцениваться как потенциально недостоверные и, соответственно, подлежать тщательной проверке в рамках доказывания по уголовному делу, в частности, дополнительно сопостав-

ляться с другими доказательствами, собранными преимущественно не из открытых источников.

Ключевые слова: доказательства, Интернет-разведка, разведка по открытым источникам, следственная деятельность, уголовный процесс, утечки данных, OSINT.

OPEN SOURCE INTELLIGENCE IN INVESTIGATIVE ACTIVITY

Oleg Slashchynin

*Investigator of the Main Investigative Department
of the Investigative Committee of the Republic of Belarus, 9 Frunze Str.,
220034, Minsk, Republic of Belarus, mailtempus@mail.ru*

Abstract. The article discusses the theoretical and practical aspects of open source intelligence (OSINT). The prospects and possible problems of using OSINT are analyzed in investigative activity.

The author substantiates the conclusion that the factual data obtained using OSINT should be assessed as potentially unreliable and, accordingly, be subject to thorough verification as part of the evidence in a criminal case, in particular, be additionally compared with other evidence.

Key words: criminal procedure, data leak, evidences, Internet intelligence, investigative activity, open source intelligence, OSINT.

Стремительная цифровизация общества и государства вместе с расширением сетевого пространства повлекли за собой рост доступности информации и увеличению числа источников ее получения. Доступность информации характеризуется открытостью размещения (хранения) ее источников или возможностью ведения с ними удаленной работы. В свою очередь, множественность указанных источников напрямую связана с многообразием человеческого знания, совершенствованием и количественным увеличением ресурсов их накопления. Эти явления выражаются в каталогизации и оцифровке накопленных человечеством знаний, увеличении числа сетевых и иных информационных ресурсов, создающих новые условия взаимодействия соискателя с информацией и источниками ее получения.

Изложенные обстоятельства не могут не сказаться на условиях работы правоохранительных органов, задачи которых неразрывно связаны со сбором, проверкой и оценкой информации. Использование в данном случае всех доступных источников получения сведений о лицах, предметах, фактах, событиях, явлениях или процессах, соответственно, положительно скажется на результатах осуществления правоохранительной деятельности. Так, органы предварительного следствия, используя при доказывании большее число источников доказательств, несомненно повысят уровень выполнения требований о всестороннем,

полном и объективном исследовании обстоятельств уголовных дел. Однако, вместе с появившимися возможностями перед следователем встают новые вызовы, связанные как с необходимостью сбора доказательств из общедоступных источников, так и с проблемами их последующей проверки и оценки.

В настоящее время у специалистов различных отраслей экономики, связанных с поиском и обработкой информации, набирает популярность использование OSINT (англ. – Open Source INTelligence) или разведки по открытым источникам. Несмотря на широкое медиаосвещение OSINT как нового явления, стоит указать, что данная разведывательная дисциплина появилась еще в середине XX века и используется в военной и политической сферах по настоящее время. Ее сущность заключается в поиске, выборе, сборе и анализе информации из общедоступных источников с использованием разведывательных методов и инструментов. Зачастую OSINT воспринимается лишь как Интернет-разведка по открытым сетевым источникам. Однако Интернет-разведка является хоть и самым перспективным направлением OSINT, но не единственным во всей разведывательной дисциплине. Применительно к следственной деятельности использование OSINT может означать собирание, проверку и оценку доказательств с использованием методов и инструментов разведки по открытым источникам информации.

Источником получения доказательств может выступать любой материальный носитель (накопитель), сохранивший в своей структуре сведения (данные) и одновременно способный идентифицировать их происхождение (откуда информация поступает, возникает или получается). Основные материалы носителей (накопителей) можно условно разделить на традиционные (например, бумага, фотоматериал, пластмасса) и машиночитаемые (например, оптические, полупроводниковые, магнитные).

Традиционные носители информации, произведенные рукописным или полиграфическим способом, как правило, могут быть обнаружены следователем в следующих местах их системного аккумулирования:

- фонды архивных учреждений (например, Национальный архив Республики Беларусь, Национальный исторический архив Беларуси);
- печатные и документальные фонды государственных органов и иных организаций;
- библиотечно-информационные фонды (например, Национальная книжная палата Беларуси, Национальная библиотека Беларуси);
- фонды печатных средств массовой информации и информационных агентств;

- музейные фонды (например, Национальный исторический музей Беларуси, Белорусский государственный музей истории Великой Отечественной войны);

- частные публичные фонды и коллекции.

Может показаться, что использование отдельных информационных ресурсов (например, фондов архивных учреждений, музейных фондов, частных публичных фондов и коллекций) в следственной деятельности маловероятно. Однако, на практике возникают совершенно нетипичные следственные ситуации, где результативное собирание доказательств может происходить и в вышеуказанных ресурсах (например, при расследовании уголовного дела по факту геноцида населения Беларуси во время Великой Отечественной войны и послевоенный период [1]). Так, доказательственная информация может содержаться в различного рода официальных документах, отчетах и справках, судебных актах, фотокарточках, газетах, журналах, научно-исследовательских работах, стенограммах, телеграммах, картографических и изобразительных изданиях, пресс-релизах, бюллетенях, сохраненных самиздатах, а также иных печатных изданиях и рукописных материалах.

Машиночитаемые накопители информации (например, накопители на магнитных жестких дисках или твердотельные накопители) в силу своей распространенности не имеют конкретно определенных мест их системного аккумулирования. Однако в связи с возможностью реализации удаленного доступа к указанными накопителям, предлагается построить их классификацию на основе разновидности осуществляемого к ним сетевого подключения, а именно:

- транслируемые посредством радиовещания или цифрового телевидения;

- получаемые по локальной компьютерной сети (Инtranет) или в рамках подключения к одной электронно-вычислительной машине;

- получаемые по глобальной компьютерной сети (например, Интернет, Фидонет, FTN и иные компьютерные сети региональных размеров).

В связи с возможностью возникновения на практике нетипичных следственных ситуаций, следует указать на теоретическую вероятность наличия аудио-визуальной доказательственной информации в сообщениях (сигналах), передаваемых посредством радиовещания или цифрового телевидения. Помимо транслируемых телепередач интерес для собирания доказательств могут представлять как радиоэферы крупных вещательных организаций, так и радиоэферы в любительском диапазоне радиочастот.

Также большой массив потенциальных цифровых доказательств содержится на машиночитаемых накопителях информации, объединенных в локальные сети государственных органов и иных организаций. В зависимости от деятельности осуществляемой владельцем (оператором) сети, могут создаваться и развертываться различные электронные информационные ресурсы и системы. Их примерный перечень содержится в выпускаемом Министерством связи и информатизации Республики Беларусь каталоге «Информационные ресурсы и системы Беларуси» [2]. Так, в Государственном регистре информационных ресурсов в настоящее время зарегистрировано 30 347 информационных ресурсов и 375 информационных систем [3].

Наиболее перспективным направлением собирания доказательственной информации можно считать ее поиск на хостах – устройствах (серверах) с машиночитаемыми накопителями информации, постоянно подключенных к глобальной компьютерной сети (например, Интернет) посредством своих локальных/региональных/магистральных провайдеров. Перспективность и, соответственно, возможная высокая результативность этого направления связана с одновременным сетевым подключением огромного количества хостов и объемами содержащихся в их накопителях цифровых данных (по сравнению с масштабами отдельных локальных компьютерных сетей или объемами фондов традиционных носителей информации). Независимо от своего фактического месторасположения, следовательно, имея доступ к сети, к которой подключен интересующий хост, и зная сетевой адрес последнего, может удаленно считать определенное содержимое его накопителей.

Вышеописанные носители (накопители) информации, исходя из своих характеристик, в соответствии с частью второй ст. 88 и ст. 100 Уголовно-процессуального кодекса Республики Беларусь могут признаваться источниками доказательств в качестве «иных документов» и «других носителей информации». Упомянутые носители (накопители) информации могут также признаваться вещественными доказательствами, если обладают признаками таковых.

Установив круг основных материальных носителей (накопителей) информации, их свойства, а также общедоступные места их аккумулярования или адреса доступа, следовательно, должен определить примерный перечень искомых в рамках OSINT информационных объектов. В связи с высокой разнородностью фактических данных, представляющих интерес при исследовании обстоятельств уголовного дела, далее будут описаны лишь отдельные информационные объекты, обладающие большим доказательственным потенциалом. Перечень указанных объектов, несмотря на возможную сущностную близость или их

происхождение из другого схожего информационного объекта, может быть представлен следующим образом:

- клиентская часть персональных, корпоративных, новостных веб-сайтов, а также сетевых ресурсов государственных органов и международных организаций. Представляет собой визуальный интерфейс веб-страницы, которая отображается в сетевом браузере следователя. Сюда входят загружаемый код веб-страницы (HTML, CSS, JavaScript и иные), а также размещаемые владельцем (оператором) ресурса контент и видимые файловые вложения (текст, изображения, аудио-видеозаписи, картографические данные, документы, исполняемые и иные электронные файлы);

- пользовательский контент и вложения. Является разновидностью вышеуказанной клиентской части сетевых ресурсов с той лишь особенностью, что данные размещаются не их владельцами (операторами), а пользователями по предложенной веб-страницей (веб-приложением) форме. Контент и вложения зависят от предлагаемых форм их размещения: форум (имиджборд), социальная сеть, аудио-видеохостинг или стриминговый сервис, конференция Юзнета, блог-платформа, доска объявлений и иные;

- контент и вложения систем мгновенного обмена сообщениями и веб-чатов, размещаемые (при отсутствии веб-версии мессенджера) посредством клиентских программ (например, Telegram, WhatsApp, Skype, ICQ, Pidgin);

- открытые FTP-сервера и иные общедоступные сетевые хранилища (репозитории). Представляют собой умышленно или случайно открытые удаленные сетевые ресурсы (хосты), где хранятся доступные для скачивания электронные файлы различных форматов и размеров. В данном случае также подразумеваются одноранговые файлообменные сети (BitTorrent и иные P2P сети);

- контент, вложения и сетевые хранилища, доступные лишь при подключении к скрытым сетям с непубличной (нестандартной) адресацией сетевых ресурсов (например, Tor, I2P, Freenet). Для доступа к указанным ресурсам требуется использовать специальное программное обеспечение или сетевой браузер;

- контент, вложения веб-страниц и сетевые хранилища, не индексируемые поисковыми системами или не связанные с гиперссылками, размещенными на индексируемых сетевых ресурсах;

- массивы утечек данных серверной части веб-сайтов и иных сетевых ресурсов. Под упомянутыми массивами подразумевается ранее скрытое владельцами (операторами) сетевого ресурса содержимое данных его серверной части, но опубликованное третьими лицами

в открытый доступ после совершения последними несанкционированного доступа к указанной серверной части и копирования ее содержимого.

Рассмотрев теоретические аспекты разведки по открытым источникам информации, необходимо раскрыть практическую часть использования методов и инструментов OSINT. Также, следует определить совместимость указанных методов и инструментов с порядком собирания доказательств, предусмотренным ст. 103 Уголовно-процессуального кодекса Республики Беларусь. Так, все используемые в OSINT методы и инструменты можно условно разделить на две категории: пассивные и активные. Пассивные методы и инструменты предполагают проведение разведывательных мероприятий без какого-либо прямого взаимодействия с изучаемым объектом/субъектом, а в свою очередь, активные – наступательное взаимодействие на изучаемые объекты/субъекты (например, установление сеанса авторизации в учетную запись, логгирование IP-адресов и иных идентификаторов, обратный просмотр домена, удаленный контакт с оператором ресурса. Как правило, использование активных методов и инструментов наиболее характерно для осуществления оперативно-розыскной деятельности. Исходя из особенностей порядка собирания доказательств, в следственной деятельности могут использоваться следующие методы OSINT:

- получение доказательств по письменному запросу (либо их изъятие при проведении следственных действий);
- разведывательный поиск, выбор, сбор и анализ цифровых данных на удаленных сетевых ресурсах в рамках проведения осмотра компьютерной информации, который, в свою очередь, можно условно поделить на несколько этапов:

1. Определение и аккумулялирование списка имеющихся ключевых слов об искомом объекте/субъекте (идентификаторы и сетевые имена учетных записей, абонентские номера, адреса электронных почтовых ящиков, адреса криптокошельков и иных виртуальных кошельков, доменные имена, URL-адреса, IP-адреса и MAC-адреса устройств, User-Agent браузеров, пароли, персональные данные, псевдонимы, названия и хеш-суммы файлов, ключи и сигнатуры изображений, сохраненные координаты и иные метаданные) [4];

2. Выбор и настройка применяемых инструментов, установление круга возможных источников цифровых доказательств;

3. Индексирование установленных источников по ранее определенным ключевым словам (с использованием выбранных инструментов);

4. Оценка обнаруженной информации на предмет относимости к исследуемым обстоятельствам, ее анализ, пополнение списка клю-

чевых слов, протоколирование полученных доказательств, повторное индексирование.

Для разведывательного поиска, выбора, сбора и анализа цифровых данных также могут применяться следующие OSINT-инструменты:

- поисковые системы общего назначения (например, Google, Baidu Search, Яндекс) с использованием операторов расширенного поиска (например, `intext:`, `«»`, `-`, `site:`, `link:`, `AND`, `filetype:`), а также метапоисковые системы (например, `dogpile`, `searX`);
- специализированные поисковые системы по подключенным к сети устройствам (IoT), кешированным веб-страницам, изображениям, FTP-серверам и иным открытым сетевым хранилищам (например, `Shodan`, `Censys`, `Wayback Machine`);
- программные инструменты (веб-приложения) автоматизированного поиска, выбора, сбора и агрегирования данных (например, `Reconng`, `Maltego`, `SpiderFoot`);
- иные программные модули и веб-платформы (фреймворки) с упорядоченными веб-сканерами, базами данных, справочными службами, реестрами и целевыми поисковыми системами (например, `Intelligence X`, `OSINT Framework`).

Несмотря на кажущуюся перспективность использования OSINT в следственной деятельности, следует указать на возможность возникновения проблем, связанных с оценкой достоверности отдельных доказательств, полученных из общедоступных источников. Обнаруженные в ходе OSINT носители (накопители) информации не всегда могут обладать свойством идентификации происхождения их доказательственного содержания, например, в случаях:

- их обнаружения на удаленном сетевом ресурсе с неустановленным или не идущим на контакт с правоохранительными органами владельцем (оператором);
- использования программных инструментов (их модулей) с закрытым исходным кодом или запускаемых на серверной части сетевого ресурса (например, чат-бот в Telegram), детально не раскрывающих способ и источники получения запрошенных доказательств;
- их установления в массиве утечек данных, ранее не публиковавшихся в открытом доступе или не имеющих установленных владельцев (операторов);
- анонимного опубликования пользовательского контента или выпуска самиздата;
- наличия на сетевом ресурсе программных ошибок размещения, обработки и хранения контента (например, недостоверная временная отметка публикации) или файловых вложений (внесение службами се-

тевого ресурса изменений в оригинальный электронный файл или его метаданные).

Опираясь на требования части первой ст. 104 Уголовно-процессуального кодекса Республики Беларусь, доказательства в приведенных следственных ситуациях должны подлежать всесторонней, полной и объективной проверке. Если имеются сомнения в их достоверности, следователь должен принять меры к получению других доказательств (в первую очередь, собранных не из общедоступных источников), подтверждающих или опровергающих проверяемые доказательства. При невозможности их сопоставления с другими доказательствами, соответственно, отсутствии возможности определения их достоверности, собранная в рамках OSINT информация не может быть положена в основу принимаемых следователем процессуальных решений. Однако данная информация может иметь ориентирующее значение для последующего собирания доказательств при производстве предварительного следствия или при проведении оперативно-розыскных мероприятий по поручению следователя.

Наряду с популяризацией OSINT, стоит отметить активное преобразование уже существующих и появление новых разведывательных (суб-)дисциплин, которые также могут быть использованы в правоохранительной деятельности: ADINT (разведка по рекламным модулям), CYBINT (киберразведка), FININT (финансовая разведка), GEOINT (геопространственная разведка), HUMINT (социальная инженерия / агентурная разведка), IMINT (видовая разведка по аэро съемке и космической съемке), MEDINT (разведка по медицинским данным), TECHINT (техническая разведка вооружений), SIGINT (радиоэлектронная разведка) и иные.

Список цитированных источников

1. Расследование уголовного дела о геноциде [Электронный ресурс]: Генеральная прокуратура Республики Беларусь. – Режим доступа: prokuratura.gov.by/ru/activity/rassledovanie-ugolovnogo-dela-o-genotside. – Дата доступа: 05.03.2023.

2. Информационные ресурсы и системы Беларуси [Электронный ресурс]: каталог / М-во связи и информатизации Респ. Беларусь. – Вып. 20, 8 февр. 2022 г. – Режим доступа: www.mpt.gov.by/sites/default/files/katalog_8022572_06-07_22_04_02_2022.pdf. – Дата доступа: 05.03.2023.

3. Статистика Государственного регистра информационных ресурсов и информационных систем [Электронный ресурс]. – Режим доступа: gris.bel/statistics. – Дата доступа: 05.03.2023.

4. Валесюк, А. Д. Использование возможностей ресурсов сети Интернет при расследовании уголовных дел / А. Д. Валесюк // Совершенствование следственной деятельности в условиях информатизации: сб. материалов междунар. науч.-практ. конф., Минск, 12–13 апреля 2018 г. / Ред. журн. «Промышленно-торговое право». – Минск, 2018. – С. 52–56.