УДК 343.1

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ OSINT В ХОДЕ ОБЫСКА МЕСТА НАХОЖДЕНИЯ ЭЛЕКТРОННОЙ ИНФОРМАЦИИ

Яковлева Кристина Юрьевна

Московский университет МВД России имени В.Я. Кикотя
e-mail: kristina15.03.1998@yandex.ru

USING OSINT TECHNOLOGY DURING THE SEARCH OF THE LOCATION OF ELECTRONIC INFORMATION

Yakovleva Kristina Y.

Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot

Аннотация. Появление электронной формы фиксации, передачи и использования информации диктуют потребность в приспособлении и (или) разработке новых способов собирания доказательств, а, следовательно, их проверки и оценки доказательств. Создавшееся положение направляет исследователей продолжать работу по поиску путей, обеспечивающих более эффективное использование электронной информации в уголовном судопроизводстве. Теоретическое понимание электронной информации, является тем «базисом», на котором в последующем появится «надстройка» в виде правовых норм, регулирующих общественные отношения в процессе её использования в уголовном процессе. Применение элементов технологии OSINT в ходе производства следственных действий, а конкретно обыска места нахождения электронной информации позволит оперативно и достоверно собирать доказательства, содержащие электронную информацию, что отразиться на эффективности расследования преступлений, как в сфере компьютерной информации, так и по другим делам в уголовно-процессуальном доказывании, в которых используется электронная информация. Автором научной статьи выделяются признаки OSINT в уголовно-процессуальном доказывании и сформулировано определение «использование технологии OSINT в уголовно-процессуальном доказывании».

Abstract. The emergence of an electronic form of recording, transmitting and using information dictates the need to adapt and (or) develop new ways of collecting evidence, and, consequently, their verification and evaluation of evidence. This situation directs researchers to continue their work on finding ways to ensure more effective use of electronic information in criminal proceedings. The theoretical understanding of electronic information is the "basis" on which a "superstructure" will appear in the form of legal norms regulating public relations in the process of its use in criminal proceedings. The use of OSINT technology elements in the course of investigative actions, specifically the search of the location of electronic information, will allow for the prompt and reliable collection of evidence containing electronic information, which will affect the effectiveness of the investigation of crimes, both in the field of computer information and in other cases in criminal procedural evidence in which electronic information is used. The author of the scientific article highlights the signs of OSINT in criminal procedural proof and formulates the definition of "the use of OSINT technology in criminal procedural proof". The definition of "the location of electronic information", which is necessary to determine the location of the search for electronic information during the search, is disclosed.

Keywords: electronic information, OSINT technology, search, inspection, results of operational investigative activities, collection of evidence, reliability of evidence.

Раскрыта дефиниция «место нахождение электронной информации», которая необходима для определения места поиска электронной информации в ходе производства обыска.

Ключевые слова: электронная информация, технология OSINT, обыск, осмотр, результаты оперативно-розыскной деятельности, собирание доказательств, достоверность доказательств.

Для цитирования: Яковлева К.Ю. Использование технологии OSINT в ходе обыска места нахождения электронной информации // Проблемы правовой и технической защиты информации. 2023. №11. С. 131-136.

For citation: Yakovleva K.Y. Using OSINT technology during the search of the location of electronic information // Legal and Technical Problems Information Protection. 2023. No. 11. P. 131-136.

Одним из актуальных вопросов процесса цифровизации в уголовном процессе представляет использование больших данных в уголовно-процессуальном доказывании. А. И. Зазулин отмечает, что для реализации поиска информации по Интернет-источникам применяются инструменты OSINT [5, с. 95].

Согласно ГОСТ Р 59926-2021/ISO/IEC TR 20547-2:2018 OSINT (open source intelligence) – разведка на основе открытых источников [1]. Данный инструмент разработан в США Дэвидом Бойденом (David Boyd) компанией Data Tactics для обработки и анализа разведывательных данных. Однако указанный инструмент представляет интерес и в рамках собирания доказательств, содержащих электронную информацию, по уголовным делам в России.

Исследована возможность применения OSINT в работе с большими данными в уголовно-процессуальном доказывании. М. О. Янгаева и Н. О. Павленко под OSINT понимают «разведывательную дисциплину, включающую в себя поиск, выбор, сбор разведывательной информации из общедоступных источников, а также ее анализ» [11, с. 133].

В.Ю. Иванов выделил ключевое отличие OSINT от других форм разведки, сущность которого заключается в том, что результатом её функционирования является «информация, добытая только из открытых источников без нарушения законодательства» [6, с. 63].

Согласно приказу Минцифры России от 7 апреля 2020 г. № 162 сведения о программном комплексе «Виток-OSINT» включены в реестр российского программного обеспечения [2], как «система сбора, хранения, обработки, анализа, моделирования и визуализации массивов данных». Соответственно, такой инструмент собирания электронной информации находит законодательное регулирование и применение в реализации основных информационных процессов.

Вместе с тем, для решения задач уголовного процесса технология OSINT также может быть применима с целью оперативности и достоверности собираемых доказательств, содержащих электронную информацию.

Применение данной технологии в ходе производства следственного действия осуществляется с помощью сети «Интернет». Соответственно оперативность обеспечивается за счет того, что указанная сеть общедоступна, и доступ к ней возможен с помощью разных технических средств и местоположений.

Собирание правоохранительными органами сведений из данной сети позволяет им самостоятельно обеспечить достоверность электронной информации разными способами (изъятием и (или)

копированием). Соответственно, по результату собирания исключён факт модификации электронной информации. В случае же искажения электронной информации или её уничтожения в процессе собирания, полученные сведения будут признаны недостоверными, соответственно недопустимым доказательством.

Однако автор научной статьи полностью согласен со следующей позицией О. В. Химичевой: «При всей очевидной полезности новых технологий для уголовного судопроизводства нельзя забывать про специфичность этого вида государственной деятельности, предполагающей в связи с совершенным преступлением серьезное вмешательство в повседневную жизнь попадающих в его орбиту участников. Именно поэтому все нововведения, какими привлекательными с позиций упрощения и ускорения процессуальных процедур они ни были, требует тщательной проработки с целью недопущения необоснованного, чрезмерного ограничения прав и законных интересов граждан и юридических лиц» [9, с. 171].

Автором научной статьи выделяются следующие признаки OSINT в уголовно-процессуальном доказывании:

– функционирование в открытых (общедоступных) Интернет-ресурсах, что позволяет исключить обязательность судебного санкционирования на производство следственного действия;

– следственное действие, в рамках которого осуществимо использование данной технологии, является обыск. Уголовно-процессуальная форма обыска вполне может допустить применение технологии OSINT. К тому же, данный обыск осуществим в местах нахождения электронной информации. Такое сужение объекта обыска позволяет определить его цель, которая направлена на поиск доказательственно значимой электронной информации, так как этот поиск будет осуществлять непосредственно в Интернет-ресурсах;

– местом производства обыска указываются: во-первых, адрес страницы сайта сети «Интернет», физические места дислоцирования серверов с необходимой электронной информацией могут быть, как на территории России, так и в других государствах, а также 2) автоматизированное рабочее место следователя;

– предлагается в ходе производства обыска места нахождения электронной информации предоставить следователю (дознавателю) право выбора фиксации хода следственного действия: привлечением к участию не менее двух понятых, или применением технических средств фиксации хода и результатов следственного действия. В связи с данным предложением потребуется дополнительное указание в части 1.1. статьи 170 УПК России на статью 182 УПК России.

Сущность данного обыска места нахождения электронной информации с помощью технологии OSINT заключается в следующем: применение элементов указанной технологии выражается в установлении связи данных одного лица, то есть персональные и другие данные, которое само же лицо разместила на разных страницах сети «Интернет». Такая связь является дополнительной частью достаточных данных для производства обыска (поиска) на нескольких страницах сети «Интернет».

Например, А. Б. Смушкин рекомендует применение методов OSINT с целью исследования открытой сети или в «Телеграм» для установления факта первичного поиска клиентов для криминального бизнеса» [7, с. 103].

В ходе анализа материалов архивных уголовных дел по г. Москве автором научной статьи обнаружен протокол мониторинга и осмотра интернет-сети, в котором при помощи поисковой системы «Яндекс» осуществлялось введение в адресную строку браузера основных слов и (или) словосочетаний обыска и осуществлялся поиск информации. В ходе мониторинга информации установлено наличие электронной информации в виде текстового сообщения на открытой странице сайта сети «Интернет». Осмотрен

адрес данной станицы. В результате чего указано название и содержательная часть сообщения, дата и время размещения имеющегося текста.

Обнаружен ещё один протокол осмотра сайта, в котором осмотрены публикации, размещенные в мессенджере «Telegram». С использованием официального приложения «Telegram» осуществлялся переход по ссылке. Установлено, что на момент осмотра у канала имелось определенное количество участников. Осуществлялся поиск новостной статьи. Установлено, что указанная статья размещена от определенного имени, дата и время.

Исследован акт осмотра (обследования и мониторинга) Интернет-сети в рамках проведения предварительной проверки по сообщению о преступлении в связи с обращением гражданина по факту распространения в телеграмм-канале клеветнических сведений в отношении гражданина. Произведен осмотр публикаций размещенной в мессенджере «Telegram» по определенному адресу сети «Интернет». С использованием официального приложения «Telegram» осуществлялся переход по ссылке. Установлено, что Телеграм-группа состоит из определенного количества участников. Осуществлялся поиск статьи с определенным заголовком с указанием даты создания. Установлено, что указанная статья размещена пользователем, имеющим ник-нейм и дата. Производилось копирование текста новостной статьи. К акту осмотра прилагается копия новостной статьи, дата.

Обобщая предложенные выше фрагменты материалов уголовных дел, полагается, что на досудебном производстве отмечены факты осуществления осмотров в сети «Интернет», в процессе производства которых применялся поиск электронной информации. Также, для науки уголовно-процессуального права и криминалистики появился практический подход к тактике производства осмотра сети «Интернет», а также фиксации определенных элементов (например, количество участников группы или канала мессенджера, содержание новостных статей и другое).

Соответственно, осуществление поисковых действий относится к проведению обыска, а осмотру присуще действия, производящие описательный характер производства следственного действия. В данном случае, осуществление осмотра известного правоохранительным органам адреса страницы сайта сети «Интернет» возможно, но поиск или установление данного адреса не может быть результатом осмотра.

Согласно позиции С.А. Шейфера, «обыск – это следственное действие, основанное на наблюдении и осуществляемая с соблюдением установленной законом процедуры принудительное обследование помещений, жилища и иных мест, отдельных граждан, их одежды, с целью отыскания и изъятия вещественных доказательств, документов и ценностей, имеющих значение для дела, а также разыскиваемых лиц и трупов» [10, с. 67]. Данное определение является подтверждением невозможности применения осмотра доказательства, содержащего электронную информацию, будучи не изъятой и (или) скопированной в ходе обыска, так как именно обыск включает в себя поиск и установление необходимого адреса страницы сайта сети «Интернет».

Место нахождения электронной информации – это электронные носители информации, на которых размещены файлы, содержащие электронную информацию, информационные процессы (обработка, передача и хранение) которых осуществляются с помощью технических средств и программного обеспечения. К электронным носителям информации можно отнести:

– электронные адреса страницы сайта сети «Интернет» на сервере;

– мессенджеры («Telegram», «WhatsApp», «ВКонтакте» и другие) на сервере;

– электронные носители информации, доступ к которым затруднён, то есть указанные носители находятся на

территории государств, с которыми отсутствует международные соглашения о взаимодействии по раскрытию и расследованию преступлений в сфере компьютерной информации (глава 28 Уголовного кодекса Российской Федерации от 13 июня 1996 г. № 63) и другие.

В рамках производства обыска места нахождения электронной информации осуществимо применение элементов связи электронной почты, номера телефона и тех страниц сети «Интернет», на которых регистрируется пользователь. Следователь (дознаватель), имея достаточно данных, которые будут основаны, в том числе и на этих связях, может проводить обыск на нескольких страницах сети «Интернет».

В уголовном процессе технология OSINT – эта технология, которая применима в ходе производства такого следственного действия, как обыск места нахождения электронной информации. Объяснением этому является то обстоятельство, что в основу принципа работы данной технологии заложен поиск. Среди всех имеющихся следственных действий, известных уголовному процессу, обыск – единственный способ собирания доказательств, который осуществляется посредством производства обыска в каком-либо месте или у какого-либо лица (статья 182 УПК России).

Применение технологии OSINT в оперативно-розыскной деятельности отличается от использования такой технологии в уголовном процессе. Отличие заключается в том, что указанная технология применяется в ходе производства следственных действий, соответственно фиксируется в протоколе факт её использования.

Оперативно-розыскной деятельности присуща особая правовая природа [8, с. 14], в рамках которой применение данной технологии как специальной техники и известность об её работе может и не быть, например, в рамках производства оперативно-розыскных мероприятий. В силу того, что отсутствует на законных основаниях информация о средствах и методах поиска и получения электронной информации, которая в качестве полученного результата оперативно-розыскной деятельности может использоваться в доказывании по уголовному делу (статья 89 УПК России).

А. А. Бессонов отмечает, что «можно использовать сведения из:

1. утечек баз данных разнообразных российских сервисов (Яндекс.Еда, Гемотест, СДЭК, Почта России и других);
2. поиск по открытым источникам сети «Интернет», социальным сетям и Даркнету (Dark Net), возможен с программным комплексом «Охотник» [3]. К решаемым с его помощью задачам относятся:

– установление людей и связей между ними, включая скрытые и удаленные данные, социальные сети;

– поиск различных объектов и событий по географическим координатам;

– мониторинг закрытых преступных сообществ, форумов и маркетплейсов Даркнета;

– анализ контента социальных сетей и веб-страниц;

– анализ операций с криптовалютами» [4, с. 44].

Таким образом, совокупность сформулированных признаков позволяет автору научной статьи предложить следующее определение: использование технологии OSINT в уголовно-процессуальном доказывании – это технология собирания доказательств, содержащих электронную информацию, из открытых страницах сайта сети «Интернет», осуществляемая проведением обыска места нахождения электронной информации, с целью дальнейшего использования в проверке и оценке таких доказательств по уголовному делу.

Исследования в сфере поиска и анализа электронной информации из открытых источников существенно могут расширить возможности следственных действий в уголовном процессе специальными инструментами технологии OSINT, что, в свою очередь, приведет к повышению эффективности и оперативности расследования преступлений.

Библиографический список

1. *ГОСТ Р 59926-2021/ISO/IEC TR 20547-2:2018. «Национальный стандарт Российской Федерации. Информационные технологии. Эталонная архитектура больших данных. Часть 2. Варианты использования и производные требования» (утв. и введен в действие Приказом Росстандарта от 2 декабря 2021 г. № 1685-ст) // М.: ФГБУ «РСТ», 2022, сайт: URL: https://clck.ru/35xtY4 (дата обращения: 20.11.2023).*
2. *Приказ Минкомсвязи России от 07.04.2020 № 162 «О включении сведений о программном обеспечении в единый реестр российских программ для электронных вычислительных машин и баз данных» (Приложение № 1), сайт: URL: https://clck.ru/35xsDo (дата обращения: 20.11.2023). Реестр программного обеспечения, сайт: URL: https://reestr.digital.gov.ru/reestr/307657 (дата обращения: 20.11.2023).*
3. *Свидетельство о государственной регистрации программ для ЭВМ от 7 декабря 2021 г. № 2021680077. Российский производитель ООО «Ти Хантер».*
4. *Бессонов А. А. Использование в раскрытии преступлений информации из открытых источников информации (OSINT) // Актуальные вопросы теории и практики оперативно-разыскной деятельности: Межведомственная научно-практическая конференция, 16 сентября 2022 г. : сборник научных трудов. – М.: Московский университет МВД России имени В.Я. Кикотя, 2022. С. 40-45.*
5. *Зазулин А. И. Osint для адвоката. Как работать и источниками информации в интернете // Уголовный процесс. – 2021. – № 10(202). – С. 90-96.*
6. *Иванов В. Ю. Использование OSINT в раскрытии и расследовании преступлений // Вестник Уральского юридического института МВД России. 2023. № 1. С. 62–66. С. 63.*
7. *Смушкин А. Б. Криминалистические аспекты исследования даркнета в целях расследования преступлений // Актуальные проблемы российского права. – 2022. – № 3. – С. 102-111.*
8. *Сумин А. А. Использование результатов оперативно-розыскной деятельности в досудебных стадиях уголовного судопроизводства: актуальные проблемы теории и практики: учебное пособие. – Москва : Московский ун-т МВД России им. В. Я. Кикотя, 2015. – 80 с.*
9. *Химичева О. В. Следственные действия: о цифровой трансформации их производства / О. В. Химичева // Криминологический журнал. – 2023. – № 2. – С. 170-174.*
10. *Шейфер С. А. Следственные действия. Основания, процессуальный порядок и доказательственное значение. М.:, Юрлитинформ. – 2004. – 184 с.*
11. *Янгаева М. О., Павленко Н. О. OSINT. Получение криминалистически значимой информации из сети Интернет // Алтайский юридический вестник. –2022. – № 2 (38). – С. 131-135.*