Ученые записки Крымского федерального университета имени В. И. Вернадского
Юридические науки. – 2022. – Т. 8 (74). № 1. – С. 176-182.

УДК 343.231
DOI 10.37279/2413-1733-2022-8-1-176-182

ОБ ИСПОЛЬЗОВАНИИ ЦИФРОВЫХ ИСТОЧНИКОВ ПОЛУЧЕНИЯ ИНФОРМАЦИИ ПОДРАЗДЕЛЕНИЯМИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ, ОСУЩЕСТВЛЯЮЩИМИ ОПЕРАТИВНО-РОЗЫСКНУЮ ДЕЯТЕЛЬНОСТЬ

Лагуточкин А. В., Мащенко А. Д.

Крымский филиал Краснодарского университета МВД России

В статье раскрывается вопросы получения и использования цифровых источников получения информации подразделениями органов внутренних дел, осуществляющих оперативно-розыскную деятельность. Использование глобальных компьютерных сетей (в первую очередь сети Интернет) выступает при этом одной из важнейших предпосылок глобализации межгосударственных отношений и построения информационного общества. Избрав цель занять достойное место среди ведущих стран мира в области развития информационного общества, наша страна активно развивает собственную информационную и телекоммуникационную инфраструктуру. Можно констатировать, что от декларирования намерений в указанной сфере государство перешло к конкретным действиям, и на этом пути уже достигнуты заметные результаты. В компьютерных сетях формируется сложнейшая система криминогенных факторов. Нарастающая проблема слабой защищенности глобальных сетей от преступных проявлений носит комплексный характер и имеет много составляющих (организационную, техническую, правовую, экономическую, социальную и др.), затрагивая не только международные, общие для всех стран, но и национальные интересы отдельных государств.

Ключевые слова: информационный поиск, оперативно-розыскная деятельность, телекоммуникационная сеть Интернет, массивы сведений, искусственный интеллект.

В современных условиях развития информационного общества, научно-технического прогресса, информационно-аналитическое обеспечение деятельности оперативных подразделений становится важным элементом противодействия внутренним и внешним угрозам криминального элемента среды. Оперативно-розыскная информация, получаемая из информационно-телекоммуникационных ресурсов, способствует выработке практических мер решения современных тактических и стратегических задач ОРД. Сегодня оперативным подразделениям следует уделять пристальное внимание внедрению современных способов получения информации с помощью глобальной сети Интернет [3].

Анализ экспертных оценок использования возможностей глобальной информационной сети доказывает, что информационная поисковая работа оперативных подразделений ОВД сводится к банальному использования ресурсов интернета для решения узкого круга задач ОРД. Одним из самых эффективных способов сбора оперативно-розыскной информации о лицах, представляющих оперативный интерес, является мониторинг глобальной сети Интернет. Программными средствами, с помощью которых осуществляют компьютерную разведку оперативные сотрудники, являются поисковые системы Google, Yandex и другие, которые позволят осуществлять поиск благодаря комбинации ключевых слов. Использование этих поисковых систем осуществляется через стандартные браузеры Opera, Mozilla, Firefox, Google Chrome и т. д. Также, эффективным способом сбора информации о лицах, представляющих оперативный интерес, является мониторинг социальных сетей, в частности

«ВКонтакте», «Instagram», «Одноклассники», «Facebook» и другие. Это дает возможность получить фотографии, установить родственные связи, дружеские, коммерческие интересы, места отдыха и т. д. [5].

В последнее время наблюдается массовое перемещение информации обо всех сферах противоправной деятельности по информационному полю Интернета. Именно этими факторами сегодня определяется рост важности оперативного поиска в сети Интернет в интересах правоохранительных органов, в частности ОВД. Учитывая это, информационные ресурсы Интернета в деятельности оперативных подразделений ОВД крепко держат позиции одного из основных источников получения оперативно-розыскной информации.

На сегодняшний день особую актуальность приобретает проблема обнаружения и фиксации в интернет-пространстве стабильных и достоверных источников получения необходимой оперативно-розыскной информации, дальнейшего упорядочения и оптимизации полученной информации. С целью решения указанной проблемы сотрудникам оперативных подразделений ОВД следует изучать особенности размещения информации в Интернет-ресурсах, а также методики её выявления, проверки и дальнейшей фиксации.

В ходе проведения оперативно поисковых мероприятий в глобальной сети «Интернет» можно получить самые различные по своему характеру и содержанию сведения: данные о личной информации лица, его местонахождении, интересах, социальных связях, местах времяпровождения. Однако, данные сведения носят информативный характер и могут быть использованы, как вспомогательные для определения закономерностей или проверки определенных факторов, в то время, как информация, представляющая интерес для органов внутренних дел представляется совокупностью сведений, указывающих на признаки преступления или административного правонарушения, его причастность, аморальное поведение личности, взаимоотношения с преступным сегментом и многое другое. Введу высокой вариативности, динамичности, скорости получения информации сотрудникам оперативных служб надлежит постоянно применять передовые достижения науки и техники, использовать специальный софт и «расширения», информационные сети и социальную инженерия для повышения результативности исполнения вмененных им полномочий.

При проведении поисковых действий в сети «Интернет» сотрудник правоохранительных органов должен иметь уверенные навыки владения персональным компьютером, разбираться в основах социальной инженерии, владеть «сленгом Интернета», знать наиболее популярные сайты и форумы, иметь исправную технику и доступ в информационное пространство [8]. Так, по последним двум критериям на сегодняшний день никаких проблем не имеется, ведь смартфоны достаточно крепки вошли в обиход человека, а услугу интернет провайдера имеют низкую стоимость, однако, в иных направлениях имеются определенные затруднения. К сожалению, познания сотрудников об информационном пространстве ограничиваются знанием таких социальных сетей, как «ВКонтакте», «Instagramm», «Tik-Tok», месседжеров «Viber», «WhatApp», «Telegramm» и более того, определенные функции данных интернет ресурсов и программного софта не используются сотрудниками по причине их неосведомленности. Для примера, в пределах «Telegramm» функционирует специальный бот – «Глаз Бога», который позволяет отслеживать, анализировать и си-

стематизировать множество данных из открытых источников, что при условии наличия номера телефона позволяет идентифицировать его, узнать характерные черты внешности, а также получить первичную информацию, и в ряде случаев установить контакт. Имеются так же проблемы в понимании основ социальной инженерии – психологическом манипулировании людьми с целью совершения определенных действий или разглашения конфиденциальной информации.

Верным представляется вывод о том, что если пользователь систематически совершает идентичные или схожие действия, то он имеет в них определенную заинтересованность, в связи с чем оперативникам надлежит понимать потенциальные склонности различных категорий граждан, что позволит выдвигать и проверять оперативные версии. В рамках проводимого исследования представляет интерес работы некоторых авторов, проводивших анализ выявления корреляции возрастных особенностей человека и сопутствующих наклонностей.

Говоря о профессионализме сотрудников при проведении оперативного поиска в «закрытом» сегменте информационного пространства, надлежит указать о необходимости высокой степени конспирации, должной владении «локальными» данными непосредственно той социальной группы, в которой осуществляется деятельность оперативным сотрудником, что в совокупности с эрудированностью и находчивостью позволит естественным образом пребывать на закрытых тематических форумах, сайтах, быть членом социальных групп и выполнять возложенные задачи максимально продуктивно. Наглядным примером может быть «Дело Сети» – когда с помощью оперативного внедрения посредством сети «Интернет» в круг потенциальных террористов, сотрудники ФСБ РФ выявили преступную ячейку, предотвратили противоправное посягательство, а виновные лица были привлечены к уголовной ответственности. Отличительной особенностью членов данного формирования была антиполитическая идеология и намерения свергнуть государственный строй, дестабилизировать обстановку в стране. Внедренный оперативный сотрудник был достаточно эрудирован, что бы длительный период времени участвовать в беседах террористов и не привлекать к себе лишнее внимание, что способствовало успеху проводимого мероприятия.

Сотруднику правоохранительных органов, кроме обычных юридических особенностей того или иного преступления, надлежит постоянно совершенствовать свой кругозор и расширять его границы. Такого рода ситуация во многом обусловлена тем, что, не смотря на факт того, что отличительной тактической особенностью оперативного поиска через глобальную сеть «Интернет» является то, что модель её деятельности характеризуется, как «от факта к человеку» или же на опережение, т.е. лишь при наличии информации, которая дает оперативнику основания полагать, что в скором времени будет осуществлено преступление, невозможно полностью исключить модель «от человека к преступлению». Примером тому может быть общение с потенциальным преступником, где без должных знаний об определенной сфере преступности, правоохранитель может не понимать, о чем идет речь, тем самым не только упустить значимую информацию, но и дискредитировать себя.

Оперативный сотрудник должен уметь не только пользоваться глобальной сетью «Интернет», но и такими специализированными программами, как «TOP» и «Telegram», так как преимущественно с их участием происходит совершение преступления, а сам софт содержит информацию, которая представляет оперативный и

доказательственный интерес. Более того, именно с помощью данных программ функционируют различные преступные онлайн-магазины, к примеру «Гидра», «Umbrella», а также бывшие интернет ресурсы – «Silk road» и «Lolita city» и множество других.

Основополагающий аспект осуществления не только оперативного поиска в сети «Интернет», но и всей деятельности ОВД РФ в целом. По нашему мнению, основным кадровым просчетом является планирование работы не от фактического количества трудоспособных сотрудников, а от штатного их количества, в особенности при наличии «кадрового голода» в системе МВД РФ, результатом чего становится невозможность объективной оценки потенциала вверенного подразделения и постановка невыполнимых задач.

Говоря о материальной базе, то по данному вопросу в рамках ведомства так же имеется ряд проблем, а именно отсутствие бесперебойного доступа в сеть «Интернет», установление ведомственных ограничений и чрезмерная закрытость. Так, в последнее время имеется тенденция в подключении всех персональных компьютеров сотрудников к «внутреннему» (ведомственному)
сегменту «Интернета» по прямому подключению с предварительно настроенными ограничениями с целью полноценной интеграции специального программного софта и электронного документооборота. Однако, большинство государственных инстанции до сих пор работают по «нарочному» принципу, что не коим образом не упрощает документооборот, а равно делает техническую интеграцию МВД РФ бесполезной. Введу того, что оперативный поиск производится в местах, где граждане часто проводят свой досуг, а имеющийся контент может быть развлекательного характера, посещение данных сайтов прямо запрещено с рабочего места, что делает проведение данного поискового мероприятия невозможным на рабочем месте, за исключением использования сотрудником собственных ресурсов.

Анализируя же вопросы проведения оперативного поиска в закрытом сегменте информационного пространства, в рамках данного организационного аспекта ситуация представляется более затрудненной. Так, для доступа необходим специальный софт, установка которого на рабочие персональные компьютеры невозможна, введу их не сертифицированного характера и иностранного производства. Вместе с этим, наличие кадровых проблем не позволяет обучить человека не то что основам социальной инженерии, а особенностям различных преступных групп, их манера ведения речи, конспирации, коллективным особенностям, что заблаговременно обрекает оперативный поиск на неудачу введу дискредитации оперативного сотрудника.

Производители программного обеспечения предлагают готовые программные решения и аппаратно-программные комплексы для массово-параллельной обработки данных, разрешающие агрегировать циркулирующие в Интернете данные объемом в десятки терабайт и производить их глубокий анализ, обеспечивающие обнаружение неизвестных событий и неочевидных закономерностей, автоматизированное выявление латентных связей между объектами различной природы (событиями, людьми, предметами, сведениями и др.), визуализацию результатов о наличии неявных связей, структуру которых трудно передать иными способами. С их помощью решаются алгоритмические задачи, представляющие интерес и для ОРД:

– классификация (отнесение новых объектов к одному из известных классов с целью установления предполагаемых характеристик таких объектов и их возможных реакций на различные воздействия);

– кластеризация (группировка объектов на основе схожих свойств);

– ассоциация (выявление закономерностей между связанными событиями);

– анализ отклонений (обнаружение нехарактерных событий);

– прогнозирование (определения наиболее вероятных вариантов развития изучаемых явлений).

С целью формирования системы обнаружения необходимой оперативно-розыскной информации в сети Интернет следует постоянно осуществлять мониторинг Интернет-ресурсов [7]. Однако следует отметить, что сегодня поиск оперативной информации не может ограничиваться и быть связан исключительно с сетью Интернет. Все большее распространение получает термин под названием «Big Data», который открывает неограниченные возможности для оперативного поиска информации [2].

Что же собой представляет «Big Data»? По своей сути «Big Data», представляет собой массив информации, имеющей определённую структуру, либо без таковой, постоянно пополняющуюся и подлежащую анализу. Более того, анализ Больших Данных создает реальную технологическую основу использования оперативно-розыскных методов для прогнозирования социально опасных событий [6].

В перечень устройств и услуг, поддерживаемых возможностями цифровой фиксации информации «Big Data», можно отнести использование услуг сотовой связи; устройств виртуальной реальности (например, очки «Google» помогают в режиме «online» получать информацию о характеристиках отдельных устройств); систем геопозиционирования, которые обеспечивают привязку физических объектов к конкретным географическим координатам на местности; технологии распознавания физических и цифровых изображений (лиц, местности, номеров автомобилей, различных аудио звуков); беспилотных летательных аппаратов для видеомониторинга территорий (например, использование их в зоне проведения антитеррористической операции); нательных датчиков (например, в правоохранительной деятельности для отслеживания фактического нахождения лиц, свобода передвижения которых ограничена законом); концепции «интернета вещей» – широкой сети устройств, подключенных к Интернету, оснащенных датчиками (смартфонов, автомобилей, промышленного оборудования, носимых устройств). Все эти «вещи» собирают данные и обмениваются ими [4]. Почему бы тогда не использовать сбор и анализ данных с целью решения зада возложенных на органы внутренних дел?

Возможности межмашинного взаимодействия практически безграничны и это доказывает фактичекое применение Big Data, коммерческими организациями. Технология межмашинного взаимодействия способна обеспечить небывалую прозрачность практически любой отрасли жизнедеятельности людей: авиакомпании способны отдалённо отслеживать и оптимизировать работу самолетов и наземных служб; организации здравоохранения предлагают лечение по результатам анализа генома в реальном времени, рекламные агентства способны таргетировать свою рекламу на интересующую её аудиторию.

Все рассмотренные нами выше технологии и технологические средства порождают большие объемы цифровых данных «Big Data», составляющие оперативный

интерес, которые могут быть зафиксированы и использованы в ходе оперативно-розыскной деятельности. Однако для успешного использования Big Data в оперативно-розыскной деятельности необходимо решить ряд достаточно сложных организационных и правовых вопросов: создание технической и технологической базы, закрепление правовых норм, регулирующих порядок доступа и использования Big Data, что позволит обеспечить поиск, сбор и систематизацию информации о субъектах оперативной внимания; строить «поведенческие профили» для лиц, совершающих преступления определенных видов; определять оптимальные варианты эффективного воздействия на выявленные в социальных сетях группы криминальной направленности и много другое [1]. В настоящее время существует правовой пробел в сфере регулирования хранения, анализа и использования информации Big data. В октябре 2018 г. депутатом Романовым, был инициирован законопроект, внесённый для Рассмотрения Государственной Думой: «О внесении изменений в федеральный закон «Об информации, информационных технологиях и защите информации», который по сути явился первой попыткой прямого регулирования больших данных, однако после предварительных рассмотрений, законопроект был отклонён и возвращён инициаторам на доработку. В 2020 г. Министерство цифрового развития, связей и коммуникаций инициировало законопроект, направленный на правовое регулирование использования Big data, однако в середине 2020 г., законопроект был отозван инициатором, для реформирования и переработки, проблема регулирования так и остаётся нерешенной.

Таким образом, исходя из всего вышесказанного, необходимо отметить следующее. Эффективное использование оперативного поиска в Интернет-ресурсах, а также Big Data, при осуществлении ОРД возможно при условии формирования соответствующей правовой базы применения указанных технологий и решения сложных вопросов кадрового обеспечения. Стандарты, по которым сегодня идет подготовка специалистов для дальнейшего прохождения службы в оперативных подразделениях полиции, до сих пор не предусматривают получения глубоких знаний о методах получения оперативно-значимой информации, необходимых для расследования преступлений в современном информационном пространстве и формирования соответствующих умений и навыков, что говорит о необходимости повышения квалификации сотрудников в данной сфере.

В заключении важно отметить, что в условиях, когда организованная преступность проявляет интерес к технологиям Big Data и Интернет-пространству в целом, отставание оперативных подразделений в овладении ими представляется крайне опасным. Работая на опережение, в сфере изучения и применения технологии Big data, мы сможем предотвратить большое количество потенциальных правонарушений, которые могут быть совершены либо в отношении этих данных, либо с их использованием.

Список литературы:

1. Батоев В. Б. «Большие данные (Big Data)» и предиктивная аналитика в оперативно-разыскной деятельности: проблемы использования и пути решения // Вестник Волгоградской академии МВД России. – 2020. – № 1 (52). – С. 11–17.

2. Кудрявцева Л. Г. Новые информационные технологии Big Data // Актуальные вопросы экономики, коммерции и сервиса. – 2019. – С. 99–103.

3. Осипенко А. Л. Оперативно-розыскная деятельность в информационном обществе: адаптация к условиям цифровой реальности // Научный вестник Омской академии МВД России. – 2019. – № 4 (75). – С. 38–46.
4. Павличенко Н. В., Тамбовцев А. И. Будущее профессии оперуполномоченный – Big Data и аналитика // Труды академии управления МВД России. – 2020. – № 2 (54). – С. 62–68.
5. Пучнин А. В., Горбова В. В. Способы получения оперативно-значимой информации в сети Интернет // Охрана, безопасность, связь. – 2019. – № 4-2 (4). – С. 56–64.
6. Титов М. В., Иванов С. И. Получение компьютерной информации – как новый вид оперативно-розыскного мероприятия // Молодая наука. Сборник научных трудов научно-практической конференции для студентов и молодых ученых. Научный редактор Н.Г. Гончарова. – 2017. – С. 395–396.
7. Иванов С. И. Особенности проведения оперативно-разыскных мероприятий в сети Интернет // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. – 2018. – № 18-1. – С. 23–24.
8. Зоз В. А., Чехун А. Ф. Идентификация личности преступника по виртуальным следам в сети Интернет // Актуальные проблемы теории и практики оперативно-розыскной деятельности: материалы IX Всероссийской научно-практической конференции. Редколлегия: А.А. Сафронов [и др.]. Краснодар, 2021. – С. 75–79.

Lagutochkin A. V., Mashchenko A. D. On the use of digital sources of information by internal affairs bodies carrying out operational-search activities // Scientific notes of V. I. Vernadsky crimean federal university. Juridical science. – 2022. – T. 8 (74). № 1. – P. 176-182.

The article reveals the issues of obtaining and using digital sources of information by internal affairs units, carrying out operational and investigative activities. The use of global computer networks (primarily the Internet) is one of the most important prerequisites for the globalization of interstate relations and the building of an information society. Having chosen the goal of taking its rightful place among the world's leading countries in the development of the information society, our country is actively developing its own information and telecommunications infrastructure. We can state that the state has moved from declaring intentions in the mentioned sphere to concrete actions, and notable results have already been achieved on this way. A complex system of criminogenic factors is taking shape in computer networks. The growing problem of poor protection of global networks from criminal manifestations is complex and has many components (organizational, technical, legal, economic, social, etc.), affecting not only international, common to all countries, but also the national interests of individual states.

Keywords: information search, operational-search activity, Internet telecommunications network, information arrays, artificial intelligence.

Spisok literatury:

1. Batoev V. B. «Bol'shie dannye (Big Data)» i prediktivnaya analitika v operativno-razysknoj deyatel'nosti: problemy ispol'zovaniya i puti resheniya // Vestnik Volgogradskoj akademii MVD Rossii. – 2020. – № 1 (52). – S. 11–17.
2. Kudryavceva L. G. Novye informacionnye tekhnologii Big Data // Aktual'nye voprosy ekonomiki, kommercii i servisa. – 2019. – S. 99–103.
3. Osipenko A. L. Operativno-rozysknaya deyatel'nost' v informacionnom obshchestve: adaptaciya k usloviyam cifrovoj real'nosti // Nauchnyj vestnik Omskoj akademii MVD Rossii. – 2019. – № 4 (75). – S. 38–46.
4. Pavlichenko N. V., Tambovcev A. I. Budushchee professii operupolnomochennyj – Big Data i analitika // Trudy akademii upravleniya MVD Rossii. – 2020. – № 2 (54). – S. 62–68.
5. Puchnin A. V., Gorbova V. V. Sposoby polucheniya operativno-znachimoj informacii v seti Internet // Ohrana, bezopasnost', svyaz'. – 2019. – № 4-2 (4). – S. 56–64.
6. Titov M. V., Ivanov S. I. Poluchenie komp'yuternoj informacii – kak novyj vid operativno-rozysknogo meropriyatiya // Molodaya nauka. Sbornik nauchnyh trudov nauchno-prakticheskoj konferencii dlya studentov i molodyh uchenyh. Nauchnyj redaktor N.G. Goncharova. – 2017. – S. 395–396.
7. Ivanov S. I. Osobennosti provedeniya operativno-razysknyh meropriyatij v seti Internet // Aktual'nye problemy bor'by s prestupleniyami i inymi pravonarusheniyami. – 2018. – № 18-1. – S. 23–24.
8. Zoz V. A., CHekhun A. F. Identifikaciya lichnosti prestupnika po virtual'nym sledam v seti Internet // Aktual'nye problemy teorii i praktiki operativno-rozysknoj deyatel'nosti: materialy IX Vserossijskoj nauchno-prakticheskoj konferencii. Redkollegiya: A.A. Safronov [i dr.]. Krasnodar, 2021. – S. 75–79.

.