УДК 343.985

Е. В. Червинский
старший оперуполномоченный отдела экономической безопасности Управления КГБ Республики Беларусь по Витебской области
Д. Г. Цапаев
старший оперуполномоченный Брестского межрайотдела Управления КГБ Республики Беларусь по Брестской области

О НЕКОТОРЫХ АСПЕКТАХ ИСПОЛЬЗОВАНИЯ ВОЗМОЖНОСТЕЙ СОЦИАЛЬНЫХ СЕТЕЙ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

На современном этапе своего развития общество вышло на новый уровень информационного обмена и общения. Просторы Интернета практически полностью покорили внимание многих, невзирая на возраст и профессиональные особенности. Пользование социальными сетями прочно закрепилось в сознании человечества. Подавляющее количество пользователей Интернета имеют аккаунты в социальных сетях, причем чаще всего этих аккаунтов несколько.

Согласно данным опроса, проведенного Информационно-аналитическим центром при Администрации Президента Республики Беларусь 82,5% пользователей интернета Беларуси зарегистрированы в различных социальных сетях (Одноклассники (Odnoklassniki.ru) – 70 %, ВКонтакте (Vk.com) – 65,5 %, Мой мир (My.mail.ru) – 17 %, Twitter – 4,5 %, Facebook – 4 %).

По данным Национального статистического комитета, на конец марта 2016 года самыми частыми поводами для выхода в Интернет среди белорусов стало общение в социальных сетях и поиск информации. Больше всего в социальных сетях общаются пользователи между 16 и 24 годами – 94,7 % всей аудитории этого возраста. Количество интернет-пользователей, отдающих предпочтение социальным сетям среди других возрастных групп: от 25 до 54 лет – 75,8 %, от 55 до 64 – 61,1 %. К примеру, популярную российскую социальную сеть «ВКонтакте» ежедневно посещают 1,6 млн белорусов, ежемесячно – 2,5 млн, среди зарегистрированных пользователей 375 тыс. учащихся, 104 тыс. руководителей, 118 тысяч служащих, 158 тысяч рабочих, 466 тысяч специалистов, 112 тысяч домохозяек.

Система регистрации в социальной системе подразумевает оставление о себе личных сведений (фамилия, имя, возраст, место проживания, места учебы, работы). Значительная часть пользователей перечисляет свои хобби, политические и религиозные взгляды, личные пристрастия. Список друзей позволяет четко определить круг общения.

Сложившиеся обстоятельства свидетельствуют о скоплении значительного массива открытой информации, представляющей определенный интерес для правоохранительного блока в ходе обеспечения национальной безопасности Республики Беларусь, который нельзя оставлять без внимания.

Исследования психологов показали, что в киберпространстве люди становятся более раскрепощенными, психологические защиты ослабевают. Этот эффект называется растормаживание. Иначе говоря, стремясь найти друзей детства и единомышленников, граждане оставляют о себе довольно много информации, воспользоваться которой не представляет особого труда.

Как известно, возможности социальных сетей используют как рядовые граждане, так и спецслужбы по всему миру. Рассмотрим несколько примеров.

Рядовые граждане – по результатам опроса, проведенного MASMI Russia, 7 % респондентов искренне ответили, что собирают в соцсетях информацию об интересующих их людях, еще 4 % мониторят круг знакомств и поведение своих близких. Иными словами, порядка 11% пользователей социальных сетей используют их как элемент слежки, получения информации о третьих лицах.

Банки – собирают в социальных сетях информацию о реальных доходах клиентов для возвращения непогашенных долговых обязательств с заемщиков.

Кадровые службы – знакомятся с кандидатами на вакансии также в соцсетях. Для них это дополнительная и регулярно обновляемая база данных.

Криминальные элементы – получают сведения о материальном положении граждан, местонахождении принадлежащих им объектах недвижимости, определяют местонахождение человека в конкретный момент времени (некоторые соцсети адаптированы под сервисы, позволяющие отслеживать объект по географическим координатам). Эти сведения бесценны для потенциальных воров. Кроме того, соцсети содержат достаточно информации, которая может быть использована сетевыми мошенниками.

Террористы – используют соцсети для обмена информацией. Например, спецслужбы США обнаружили удаленный аккаунт 19-летнего Дж. Царнаева, обвиняемого в организации теракта в Бостоне, в социальной сети Instagram. По данным спецслужб, аккаунт террориста просуществовал совсем недолго и был удален незадолго до теракта в Бостоне. Однако размещенная на нем информация, в том числе фотографии, помогли идентифицировать лиц, с которыми Дж. Царнаев контактировал перед террористическим актом, явившихся впоследствии дополнительными свидетелями преступной деятельности террориста. Приведенный пример наглядно показывает, что социальные сети используют также правоохранительные органы.

Спецслужбы и разведки – осуществляют сбор информации о местах базирования военных частей и подразделений армии потенциального противника. Пользователи, которые ищут сослуживцев, указывают номера частей и их дис-

локацию в своих аккаунтах. Фотографии наглядно демонстрируют род войск и природный ландшафт расположения армейских частей. Осознав такую уязвимость, только в 2008 году Министерство обороны Канады распространило меморандум, согласно которому военным не следует оставлять личные сведения о себе в социальных сетях, так как за подобными сайтами пристально наблюдают боевики «Аль-Каиды». По этой причине присутствие в соцсетях запрещено большинству «силовиков» и разведчикам. Сведения из социальной сети являются идеальной информацией для вербовщиков (например, вербовщики ИГИЛ).

В качестве наглядного примера также отметим события 2010 года, когда Фонд электронных рубежей выиграл иск к Министерству юстиции США и пяти другим федеральным ведомствам, в котором в соответствии с Законом о свободе информации требовал раскрыть секретные инструкции, описывающие работу спецслужб с социальными сетями. В результате разбирательств, полученный на руки 33-страничный документ свидетельствовал о том, что правительственные агенты используют сайты Facebook, MySpace, LinkedIn, Twitter и многие другие социальные ресурсы, создавая фальшивые учетные записи для общения с подозреваемыми, выяснения круга знакомств и выведывания информации личного характера (записи в блоге, фотографии, видеоролики). В числе прочего это позволяет проверить алиби подозреваемого, сравнить его показания в полицейском участке с сообщениями, отправленными на Twitter во время совершения преступления.

Вышеперечисленные примеры показывают, что имеющаяся в соцсетях информация может быть использована в различных направлениях. В то же время встает вопрос о качественном анализе размещенной информации, способах ее интерпретации для последующего применения в служебной деятельности. И в данном случае на помощь приходит психология.

Так, при изучении через социальные сети объекта заинтересованности (подозреваемого), потенциального кандидата на службу в правоохранительные органы или лица, с которым, возможно, будут впоследствии установлены конфиденциальные отношения, могут применяться несколько психологических методов (например, метод анализа независимых характеристик, анализ содержания страницы пользователя, биографический метод, анализ продуктов деятельности и другие), причем как по отдельности, так и в совокупности. Совокупность полученной информации позволяет получить немало полезной информации об особенностях личности, имеющей значение для составления полноценного психологического портрета.

Весьма актуальным аспектом в оперативно-розыскной деятельности (далее – ОРД) при использовании социальных сетей как источника получения информации становится определение степени подлинности представленной поль-

зователем в Интернете информации. Другими словами, речь идет об установлении подлинности аккаунта, подлежащего анализу. Прежде всего, необходимо определить, не является ли аккаунт так называемым фейком (фейк – от английского *fake* – подделка, так называют пользователей социальных сетей, выдающих себя за других людей). Фейки могут быть специально созданными программами сугубо технического назначения – для рассылки спама, рекламы, а также могут быть созданы и управляться конкретным живым человеком. Иначе говоря, фейковый аккаунт – это анкета, представляющая собой либо несуществующего человека, либо вовсе не того индивида, чьи данные легли в основу аккаунта.

В научном сообществе проблематика использования возможностей социальных сетей в ОРД остается малоизученной и требует дальнейшей разработке. Попытки в этом направлении предпринимает Генеральная прокуратура Республики Беларусь, разъясняя порядок проведения некоторых оперативно-розыскных мероприятий в сети Интернет, однако указанная информация имеет ограничительный гриф и недоступна для широкого круга научного сообщества.

Отдельными учеными отмечается, что в целях эффективного использования правоохранителями полученных данных необходима в первую очередь правовая регламентация понятий «информационные технологии» и «Интернет». Однако в действующем оперативно-розыскном законодательстве Республики Беларусь отсутствуют нормы, регламентирующие использование субъектами ОРД информационных технологий, в том числе глобальной сети Интернет. Основной упор законодателем пока делается на базы данных (учетов), информационные системы, которые содержат сугубо формализованные сведения (юридические факты).

Таким образом, в процессе осуществления ОРД необходимо понимать, что получение информации посредством изучения социальных сетей это всего лишь дополнительный источник информации, который может использоваться как на первоначальных, так и на последующих стадиях осуществления ОРД. Непосредственное комплексное сочетание оперативно-розыскных мероприятий с использованием сведений социальных сетей позволяет получить наиболее полную информационную модель о признаках подготавливаемого, совершаемого или совершенного преступления, а также о лицах, его подготавливающих, совершающих или совершивших и иные сведения, представляющие оперативный интерес. Вместе с тем необходимо всегда помнить об обязательном проведении качественного и критического анализа получаемой информации из социальных сетей.