УДК 354.42/44:343.9

Гавловський Владислав Данилович – начальник відділу Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України, кандидат юридичних наук, старший науковий співробітник

Щодо відслідковування осіб із використанням соціальних мереж

У статті досліджуються питання інформаційної безпеки, пов'язані з незаконним збором персональних даних користувачів соціальних мереж, та наступним протиправним їх використанням.

Ключові слова: інформаційна безпека, соціальні мережі, персональні дані, засоби збору інформації, діяльність спеціальних служб, діяльність злочинних організацій.

Постановка проблеми. На процеси глобалізації та інформатизації впливає прогрес науки і техніки, який може мати як позитивні, так і негативні наслідки. З одного боку, людина отримує доступ до нових можливостей. З іншого – стикається з усе більш різноманітними ризиками, які є загрозливими її безпеці, свободам, приватному життю. Останнім часом у глобальних інформаційно-телекомунікаційних мережах усе більшого поширення набуває новий вид протиправної деструктивної діяльності – відслідковування осіб, збирання та аналіз персональних даних користувачів, що потім передаються для несанкціонованого використання стороннім особам, здебільшого для комерційних, а у ряді випадків і злочинних, цілей, відбувається розголошення та протиправне використання конфіденційної інформації щодо сфери приватного життя особи, порушуються особисті конституційні права людей.

Актуальність теми дослідження. Ми маємо акцентувати увагу на тому, що найбільш суспільно небезпечною складовою є те, що, фактично, відслідковування, викрадення, збирання та аналіз персональних даних користувачів, є саме підготовчим етапом для вчинення інших системних та організованих протиправних дій проти як конкретної безпосередньо відслідковуваної особи, так і для певних інституцій,

зокрема, і державних інституцій, з якими така особа може мати певні відносини. Варто наголосити, що саме останній аспект створює потенційні передумови для виникнення реальних загроз національній безпеці держави. Вочевидь, що спілкування пересічного громадянина у мережі навряд чи може зацікавити іноземні спецслужби та організації, проте, приватне спілкування секретоносіїв, державних службовців певного рівня та інших категорій осіб, що становлять потенційний оперативний інтерес для таких іноземних служб і організацій, а також їх близьких родичів, навпаки, є достатньо цінною розвідувальною інформацією, яка у подальшому використовується з метою здійснення розвідувально-підривної діяльності проти України. Саме така інформація може бути використана на шкоду нашій державі при підготовці вербувальних акцій, акцій протиправного впливу на прийняття певних стратегічних для держави рішень у політичній, економічній чи соціальній сферах тощо.

Аналіз останніх публікацій за темою дослідження. Проведенням наукових досліджень окремих аспектів організаційно-правової протидії вчиненню різнорідних деструктивних діянь із використанням для цього специфічних можливостей соціальних мереж займаються такі вчені, як В. М. Бутузов, В. М. Горовий, А. І. Марущак, О. О. Поляруш, В. П. Шеломенцев, О. М. Юрченко та інші. Низка наукових праць за даною тематикою виконана безпосередньо автором представленої статті. Зокрема, нами вже неодноразово наголошувалось, що сучасний стан накопичення та збереження персональних даних особи у соціальних мережах створює плідне підґрунтя для вчинення злочинів, у тому числі організованими злочинними угрупуваннями, а також для втягування наших співгромадян іноземними спецслужбами, терористичними та іншими злочинними організаціями у протиправну діяльність [1, 2].

Отже, представлена стаття є логічним продовженням здійснюваного автором комплексного дослідження із виявлення та вивчення передумов, способів і методів учинення різних деструктивних дій, що вчиняються із використанням соціальних мереж, **із метою** розробки заходів організаційно-правової протидії таким видам протиправної діяльності.

Виклад основного матеріалу. Перш за все, доцільно наголосити, що переважна більшість користувачів соціальних мереж навіть не уявляє ступеня потенційної небезпеки та можливих негативних наслідків у випадку витоку та протиправного використання власних персональних даних, що містяться у соціальних мережах, створюючи тим самим передумови для подальших деструктивних дій із такою інформацією. До речі, за інформацією Forbes, компанія Appinions провела дослідження, згідно з яким з'ясовано, що користувачі більше бояться втрати даних, що містяться в облікових записах у соціальних мережах, ніж витоку інформації про банківські картки [3].

У практичному аспекті ми маємо наголосити на тому, що раніше мали місце переважно факти лише викрадення персональних даних користувачів, проте останнім часом усе більшого поширення набуває відслідковування конкретних користувачів, соціальних та особистих зв'язків і уподобань пристрастей конкретних користувачів соціальних мереж. Найбільш поширеним це явище є в соціальній мережі Facebook. При цьому, як правило, таке відслідковування проводиться з використанням різних сучасних технологій. Наприклад, із використанням файлу ідентифікатора cookie, за допомогою якого відбувається відстеження користувачів, по-перше, тих у кого вже є аккаунт на Facebook і які працюють у соціальній мережі; по-друге, тоді, коли користувачі, не авторизовані в системі після натискання кнопки "Вихід", насправді залишаються в мережі; по-третє, Facebook може відстежувати ваші дії в мережі Інтернет, навіть якщо ви не є користувачем цієї соціальної мережі [1].

Показовим є той факт, що соціальною мережею Facebook у 2007 році було запущено соціальну маркетингово-рекламну систему Facebook Beacon ("Маяк"). Система повідомляла друзям користувача соціальної мережі, які ресурси він відвідав і на яких з них зробив покупки чи щось замовив. Але реакція користувачів була негативною. Позицію незадоволених користувачів підтримали відомі правозахисники та експерти з особистої безпеки і наприкінці того ж року додаток Beacon було відключено в обмін на відкликання колективного позову. Позивачі вважали, що фахівцями Facebook було порушено низку законів щодо охорони особистих даних, а саме про таємницю споживчих покупок: зокрема, закон про конфіденційність електронних комунікацій, закон про захист споживчих прав та комп'ютерної злочинності штату Каліфорнія.

У підсумку, незважаючи на ліквідацію функції Beacon, послідував колективний позов користувачів, і за судовим рішенням Facebook в 2009 році зобов'язали виплатити 9,5 млн доларів США у вигляді компенсації [4].

Ми маємо констатувати, що попит на персоніфіковану конфіденційну інформацію про користувачів постійно зростає. Доказом цього є факт, що розробники соціальних мереж створюють усе нові інтерфейси і платформи для збору саме такої інформації. Зокрема, в соціальній мережі Facebook розроблено і впроваджено користувальницький інтерфейс Timeline, який дозволяє користувачам відстежувати всі події в своєму житті від моменту реєстрації в соціальній мережі. Таку інформацію, вочевидь, будуть використовувати як соціальні мережі, так і їх "замовники" в своїх цілях, зокрема і протиправних.

Більше того, придбавши соціальний геологаційний сервіс Glancee, Facebook може проводити пасивне визначення місцеперебування конкретного користувача мережі. Цей сервіс – ніби "дружнього стеження", спові-

щає користувача про те, що поруч знаходяться його "друзі", їх зв'язки та особи зі схожими інтересами. На відміну від Forsquare, Glancee показово не вимагає реєстрації. Він працює у "тіні", фактично проводячи моніторинг GPS-даних. Показово, що творці додатку рекламують сервіс, як "спосіб виявити навколо себе приховані зв'язки". Варто звернути увагу на те, що під слушним приводом, сьогодні соцмережа Facebook розробляє відповідний додаток і для смартфонів [5].

Відслідковування переміщення користувачів соціальних мереж також проводиться через відслідковування IP-адрес, з яких користувач заходив, наприклад, в особисту пошту. Зокрема, співробітники Інституту Макса Планка в Німеччині протягом 2009–2011 років слідкували за кореспонденцією 43 млн користувачів поштового аккаунту Yahoo! [6].

Крім того, відслідковування користувачів можливе з використання кнопки "Like" від Facebook, яка дозволяє користувачам оцінювати інформацію на сайті в режимі онлайн. Німецькі правозахисники в галузі захисту приватності інформації вимагають видалити цю кнопку. Вони заявили, що використання кнопки "Like" протирічить німецькому та європейському законодавству, оскільки в результаті інформація про користувачів – інтереси, тривалість перебування на тій чи іншій сторінці, переходи з одного сайту на інший надходить до США, де згодом використовується для таргетування реклами, аналізу поведінки користувачів на сайті тощо. Представники соціальної мережі підтвердили, що, натискаючи цю кнопку, така інформація як IP-адреси могла передаватися. Вони також відмітили, що ці дані, відповідно до європейського законодавства, через 90 днів видаляються. Однак Facebook, як і кожна американська компанія, згідно з Патріотичним Актом, зобов'язана зберігати цю інформацію значно довше і за необхідності надавати її спецслужбам США [7].

Окремо слід зупинитися на діяльності системи візуального розпізнавання, що застосовується у мережі Facebook. Безпосередньо сервіс автоматичного розпізнавання обличчя особи був запущений для того, щоб допомогти користувачам знаходити і позначати друзів на фотографіях. Спеціальна програма аналізує фотографії і пропонує користувачеві різні варіанти імен того чи іншого знайомого. Ця система успішно впроваджується в США, у тому числі відповідна програма написана для мобільних пристроїв Apple і призначена для поліції. Як видається, нові технології можуть допомагати швидше і легше ідентифікувати злочинців, адже зафіксовані на камеру спостереження кадри можна порівняти з базою біометричних даних. Однак тут лунають застереження. Зокрема, Йоганнес Каспар вказує: "Збирання даних – це також засіб соціальної дискримінації. Це у багатьох випадках може призводити до значних зловживань цим інструментарієм" [8]. Наприклад, аналіз

індивідуальних рис обличчя може мати випадкові збіги. Як приклад, якщо профіль футбольного фаната буде схожий на профіль якогось футбольного хулігана, йому навіть не продадуть квиток на матч.

У зв'язку з рішучими протестами з боку захисників приватних даних спочатку уряд Німеччини, а потім Євросоюз прийняли рішення про заборону цієї технології, яка, на їхню думку, порушує відразу низку законів про захист даних користувача. І соціальна мережа Facebook відключила сервіс автоматичного розпізнавання обличчя особи користувачів у Європі. Також було відзначено, що банк із "відбитками облич" мільйонів людей пов'язаний із величезним ризиком зловживань. Як приклад, така система може бути використана в недемократичних країнах з метою слідкування за опозицією або використана злочинцями. Так, за інформацією А. Аквісті, спеціаліста по інформаційним технологіям, зловмисники, використовуючи цю функцію, зможуть досить швидко з'ясувати п'ять цифр полісу соціального страхування – одного з основних документів США [9].

Для відстежування громадян постійно розроблюються та впроваджуються все нові програми і, варто наголосити, це здійснюється не лише розробниками соцмереж. Так, за даними британської газети The Guardian, американський військовий підрядчик Raytheon розробив програмне забезпечення під назвою RIOT (Rapid Information Overlay Technology). Це система, створена для швидкого отримання інформації про підозрюваних громадян із соціальних мереж, у тому числі Facebook, Twitter і Foursquare. Журналісти назвали це доказом того, що влада використовує соціальні мережі для високотехнологічного стеження за громадянами. За допомогою цієї програми можна отримати відомості про активність підозрюваного: про його соціальні контакти, карти переміщень тощо. Інформація отримується також з EXIF-заголовків фотографій, опублікованих в особистих фотоальбомах на різних сайтах. За даними журналістів, ця розробка була передана урядовим агентствам США [10].

Останнім часом усе більше окремих активістів, громадських організацій регулярно звинувачують адміністрації соціальних мереж взагалі, й Facebook зокрема, в несанкціонованому і незаконному зборі інформації про користувачів і передачі цих даних третім особам. При цьому, пошук інформації про користувачів для маркетингових потреб, спецслужб проводився в нелегальному режимі. Це створювало низку проблем, адже основна задача Facebook – як можна краще використати величезну базу даних з більш ніж мільярдом користувачів, близько 240 млрд фотографій і понад трильйон зв'язків. Шукаючи вихід із цієї ситуації, Facebook створили черговий додаток – програму пошуку Graph Search. Це новий інструмент для спостереження за активністю користувачів стає легальним і ніби перестає бути відслідковуванням.

Пошукова система Graph Search відрізняється від веб-пошуку, наприклад Google. Якщо останній був створений, щоб за допомогою ключових слів представляти можливий результат, який максимально відповідає ключовим словам, то Graph Search, навпаки, об'єднує фрази. Для прискореного пошуку потрібних даних пропонуються різні фільтри. Пошукові запити можна уточнювати більш складними фільтрами для отримання уточнених відповідей. Якщо даних пошуку немає чи недостатньо, тоді підключається програма-пошуковик Bing, яка інтегрована з Facebook. Тобто, результати web-пошуку також доступні, хоча не основні. При цьому запити можна робити в текстовому режимі фразами. Наприклад, "Де пообідати в моєму районі?". При цьому програма зафіксує географічне розташування і видасть інформацію про переваги місцевого населення. Можливо отримати список усіх співробітників певної компанії в певному місті, потім проглянути посади кожного з них. Можна одержати компрометуючу інформацію, наприклад, список всіх одружених чоловіків у певному місті, яким подобаються повії. І відразу ж список їхніх дружин [11].

Пошук проводиться по інформації, яка знаходиться в профілі чи в публічному доступі. До речі, нові налаштування не дозволяють закривати інформацію, яка знаходиться в профілі. Всіх інших налаштувань приватності Facebook дотримується. Варто також відмітити, що в Facebook вимагається реєстрація тільки під своїм реальним ім'ям, проте, в деяких країнах це визнається порушенням законодавства. Так, згідно з нормами Закону Німеччини "Про телекомунікації", громадяни країни мають право використовувати свої псевдоніми на будь-яких сервісах у мережі Інтернет.

У свою чергу, в "самій демократичній країні" – Сполучених Штатах Америки внесено поправки до Закону CFAA (Computer Fraud and Abuse Act "Акт про порушення і зловживання роботою комп'ютера", відповідно до якого американцям забороняється отримувати не авторизований доступ до інформації на захищеному комп'ютері. Тобто, на думку професора Університету імені Джорджа Вашингтона Оріна Керр, який в минулому працював прокурором і є фахівцем з комп'ютерної злочинності, правопорушником може вважатися особа, яка використовує помилкове ім'я (і, звичайно, псевдонім) у соціальній мережі або вказує там неправдиву інформацію про себе [12].

Пошук проводиться по відкритій інформації в аккаунтах, але, напевно, в пошуковику закладено можливості зчитувати закриту інформацію фахівцям соцмережі, а також спецслужб.

До того ж, якщо від "інформаційних витоків" потерпають транснаціональні корпорації, урядові інтранети, банки, то не виключено,

що збором інформації із соцмережі та відслідковуванням зможуть скористатися маркетингові компанії, а також злочинні угрупування.

Поки що новий проект працює в бета-версії і лише в англомовному сегменті. Російськомовним користувачам пошуковик стане доступним пізніше. До речі, російськомовний сегмент Інтернету сьогодні, за даними W3Tech (аналітичного підрозділу Q-Success), є другим за популярністю в онлайні та складає понад 5,9 % усіх веб-сайтів світової мережі Інтернет (англійський – 54,7 %, німецький до 5,9 %). Цікаво, що за даними цього ж ресурсу, російську мову використовують 79 % усіх українських сайтів (маються на увазі сайти зони UA) [13].

Тому соціальна мережа Facebook зацікавлена в проникненні в Росію, так як на внутрішньому ринку ця компанія поки представлена значно слабше російських сервісів. Наприкінці минулого року відбулася зустріч засновника соціальної мережі Марка Цукенберга з російським прем'єром Дмитром Медведєвим, в ході якої вони обговорили можливість присутності Facebook у Росії не тільки як соцмережі, а й як компанії, яка працює з самими передовими технологіями.

На думку експертів, ця угода – це угода між державою і володільцями соцмережі за схемою "розширення за контроль" [14]. Розвиток не анонімних мереж для держави є пріоритетним, вони – прекрасне джерело інформації для спецслужб. Установлення контролю над соціальними мережами відповідає загальній доктрині РФ щодо кіберпростору, яка відстоює право всіх держав займатися управлінням мережі Інтернет.

Росія і Китай пропонують передати контроль над мережею Інтернет ООН, а саме Міжнародному союзу електрозв'язку (International Telecommunication Union, ITU), і, разом з цим, виробити правила адресації та нумерації в мережі, поєднавши їх з місцевим законодавством і встановивши контроль над циркуляцією інформації в кожній країні [15].

Тобто, тотальний контроль онлайн-активності громадян – це лише питання часу. Спроби державної машини контролювати соціальні мережі та відслідковувати їх користувачів будуть лише посилюватися.

І, звичайно ж, російські спецслужби отримають додаткову можливість збирати закриту інформацію про користувачів соцмережі та проводити відслідковування.

Очевидно, такі технології будуть використані російськими спецслужбами для збору інформації та відслідковування зарубіжних російськомовних користувачів, у тому числі й громадян України, в першу чергу, українців, які представляють певний інтерес.

Висновки. Отже, необхідно зазначити, що, фактично, ми можемо вести мову саме про системне використання іноземними організаціями та спецслужбами соціальних мереж, діяльність яких перебуває і юридично, і фактично поза межами правового регулювання нашої держави. Діюча

в Україні правоохоронна система неспроможна забезпечити належний ефективний захист наших співвітчизників і національних інтересів від протиправних діянь, що реально вчиняються проти них із використанням незаконно отриманих із соціальних мереж персональних даних користувачів. Це, в свою чергу, зумовлює об'єктивну необхідність негайного вироблення на державному рівні принципово нових підходів до забезпечення захисту інтересів особи, суспільства та держави у цій сфері.

Список використаних джерел

1. Гавловський В. Д. До питання несанкціонованого збору та систематизації персональних даних користувачів через соціальні мережі / В. Д. Гавловський // Боротьба з організованою злочинністю і корупцією : наук.-практ. журнал. – 2011. – № 2–3 (25–26). – С. 312–320.

2. Гавловський В. Д. Використання соціальних мереж іноземними спецслужбами як потенційна загроза національній безпеці України / В. Д. Гавловський // Актуальні проблеми управління інформаційною безпекою держави : зб. мат-лів. наук.-практ. конф. (30 берез. 2012 р., м. Київ). – К. : Наук.-вид. відділ НА СБ України, 2012. – С. 56–59.

3. Appinions: Пользователи больше боятся потери данных из соцсетей чем из банковских систем / [Электронный ресурс]. – Режим доступа :
http://www. securitylab. ru/news/439417. php.

4. Апелляционный суд встал на сторону Facebook в споре по поводу выплат из-за Beacon / [Электронный ресурс]. – Режим доступа :
http://www.3dnews. ru/software-news/635594/.

5. Интернет-паноптикум Facebook / [Электронный ресурс]. – Режим доступа :
http://www. sostav. ua/news/2012/10/02/127/52214.

6. За нами следят через Интернет / [Электронный ресурс]. – Режим доступа :
http://ukrlenta. net/za-nami-sledyat-cherez-internet.

7. Німецькі поборники приватності угледіли загрозу в соціальній мережі Facebook, а точніше в улюбленій користувачами кнопці like / [Електронний ресурс]. – Режим доступу :
http://briz. if. ua/9590. htm.

8. Обережно! Розпізнавання обличчя / [Електронний ресурс]. – Режим доступу :
http://www. dw. de.

9. Лицевая идентификация может помогать преступникам / [Електронний ресурс]. – Режим доступу :
http://www. infox. ru/hi-tech/tech/2011/08/02/Licyevaya_idyentifik_print. phtml.

10. Владу США звинуватили у шпигунстві за громадянами за допомогою соціальних мереж / [Електронний ресурс] – Режим доступу :
http://svit24. net/technology/67-technology/56606-vladu-ssha-zvynuvatyly-u-shpygunstvi-za-gromadjanamy-za-dopomogoju-socialnyh-merezh.

11. Истинные возможности поиска по графу Facebook в примерах / [Электронный ресурс]. – Режим доступа :
http://www. xakep. ru/post/59987/.

12. Соколова Е. В США за использование ложного имени в Интернете могут посадить [Электронный ресурс] / Е. Соколова. – Режим доступа : http://radiovesti. ru/article/show/article_id/26139.

13. Русский стал вторым по популярности языком в Интернете / [Электронный ресурс]. – Режим доступа : http://ain. ua/2013/03/22/117693.

14. Кто заинтересован в государственной рекламе Facebook в России / [Электронный ресурс]. – Режим доступа : http://www. ng. ru/columnist/2012-10-02/4_facebook. html.

15. Савин Л. Холодная кибервойна [Электронный ресурс] / Л. Савин. – Режим доступа : http://www. stoletie. ru/geopolitika/holodnaja_kibervojna_632.htm).

В статье исследуются вопросы информационной безопасности, связанные с незаконным сбором персональных данных пользователей социальных сетей, с последующим противоправным их использованием.

The article deals with the investigation of the information security issue related to the illegal collection of personal data of users of the social networks, followed by their wrongful use.

Стаття надійшла до редакції журналу 27 березня 2013 року.