ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

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

До питання несанкціонованого збору та систематизації персональних даних користувачів через соціальні мережі

У статті досліджуються питання інформаційної безпеки, пов'язані з новою реальною загрозою – фактичним збором і систематизацією персональних даних користувачів соціальних мереж, та наступним протиправним використанням таких даних.

Ключові слова: інформаційна безпека, мережа Інтернет, соціальні мережі, викрадення персональних даних, засоби збору інформації, діяльність спеціальних служб, діяльність злочинних організацій.

Інтенсивний розвиток протягом останніх десятиліть глобальних інформаційних мереж, безумовно, має бути визнаним одним із визначальних факторів загальних інтеграційних процесів у суспільстві. Без автоматизованих інформаційних систем, реалізованих на основі комп'ютерних мереж, уже неможливе повноцінне існування та розвиток суспільства і держави в цілому, вони перетворилися у невід'ємний елемент життєзабезпечення різноманітних сфер суспільного та державного життя. Саме завдяки сучасним інформаційним системам створено реальні умови для загального доступу: до різноманітних інформаційних ресурсів незалежно від фактичної відстані між джерелом інформації та особою, зацікавленою в її отриманні.

В той же час, як справедливо наголошується у наукових джерелах, процеси інформатизації всіх галузей людської діяльності впливають і на таку сферу, як злочинна діяльність – з'являються нові види та способи злочинних посягань, пов'язаних з використанням комп'ютер-

них технологій, злочинність освоює інформаційний простір, середовище комп'ютерних мереж [1, с. 7].

Актуальність представленої праці пов'язана з тим, що останнім часом усе більшого поширення набуває новий вид деструктивної діяльності у глобальних інформаційно-телекомунікаційних мережах – відслідковування осіб, збирання конфіденційних даних користувачів та їх дії як у кібернетичному, так і матеріальному (фізичному) просторі. При цьому, отримана у такий спосіб особиста конфіденційна інформація протиправно використовується не тільки самими соціальними мережами, а і певними організаціями для досягнення своїх, здебільшого комерційних, а у ряді випадків і злочинних цілей, відбувається розголошення та протиправне використання конфіденційної інформації щодо сфери приватного життя людини, порушуються особисті конституційні права людей. Крім того, як раніше вже наголошував автор, сучасний стан накопичення та збереження персональних даних особи у соціальних мережах створює плідне підґрунтя для втягування наших співгромадян іноземними спецслужбами, терористичними та іншими злочинними організаціями у протиправну діяльність [2, с. 253].

На сьогодні наукові дослідження загальних проблем "викрадення особистості" через соціальні мережі вітчизняними вченими фактично не проводились. Представлена праця є продовженням раніше розпочатого автором дослідження проблем інформаційної безпеки, пов'язаних із викраденням персональних даних та іншої конфіденційної персональної інформації через соціальні мережі, що є сегментом мережі Інтернет.

Отже, метою даної роботи є вказати та висвітлити новий вид загрози у сфері інформаційного простору – через соціальні мережі під приводом забезпечення виконання ними своїх функцій проводиться системне відслідковування, збирання та аналіз персональних даних користувачів, що потім передаються для несанкціонованого (протиправного) використання у власних інтересах стороннім особам.

Не викликає сумнівів той факт, що у соціальних мереж є технічні можливості відслідковувати інформацію про своїх користувачів, їх активність у мережі Інтернет незалежно від того знаходяться чи не знаходяться вони в соціальній мережі, тобто після виходу зі сторінок соціальної мережі, а також про користувачів мережі Інтернет, які взагалі не мають аккаунта в соціальній мережі, шляхом створення профілів незареєстрованих користувачів. Вочевидь також те, що реальне використання соціальними мережами таких технічних можливостей є протиправним, а, отже, не повинне застосовуватись. Однак і тут виникає низка законодавчих колізій, зокрема, досить проблемним є застосування правових норм, що захищають особисті конфіденційні дані, наприклад, у контексті територіального принципу дії законодавства переважної бі-

льшості держав у світі. На практиці, соціальна мережа може бути зареєстрована на території однієї країни та організаційно забезпечуватися з її території, в той час, як її користувачі досить часто перебувають на території інших держав, тобто поза межами правового захисту за національним законодавством держави, з території якої відбувається викрадення їх персональних даних. Крім того, власники можуть використовувати цю інформацію для розвитку свого власного бізнесу чи надавати конфіденційні особисті відомості та іншу інформацію про користувачів у кращому випадку за запитами національних спецслужб чи поліції, а в гіршому – передавати її представникам різноманітних злочинних організацій (терористичних, екстриміських, загальнокримінальних тощо).

Досить показовим з точки зору підтвердження факту відслідковування, збирання та систематизації інформації, що містить персональні дані та конфіденційну інформацію щодо користувачів інформаційно-телекомунікаційного простору, є аналіз документальних матеріалів щодо цього аспекту діяльності соціальної мережі Facebook.

Зокрема, про те, як Facebook стежить за відвідувачами мережі Інтернет, досить наочно розповів аспірант Тілбургского університету (Нідерланди) А. Роозендааль у своїй статті, розміщеній в архіві мережі досліджень соціальних наук – Social Science Research Network (SSRN) [3]. Це підтвердив і хакер Н. Кубріловік, проаналізувавши HTTP-заголовки запитів, що відправляються браузерами на facebook. com, він виявив наявність видозмінених cookie-файлів, що з'являються після виходу зі сторінки Facebook [4].

Той факт, що Facebook створює досьє як на користувачів цієї соціальної мережі, так і на тих, хто ще не зареєстрований на сервісі був підтверджений після перевірки компанії Facebook Ireland ірландським відомством, яке займається захистом персональних даних – Офісом уповноважених із захисту персональних даних і приватності.

Виправдовуючись перед громадськістю, представник соціальної мережі заявив: "Ми даємо користувачам можливість відправляти через Facebook запрошення друзям електронною поштою. Така практика поширена практично на всіх сервісах, які використовують запрошення, від обміну документами до організації заходів" [5].

У свою чергу, німецьке агентство Data Protection Authority опублікувало доповідь, в якій викриває соціальну мережу Facebook у відслідковуванні навіть тих користувачів, які видалили свою сторінку і покинули цей Інтернет-проект. Й. Каспар, глава адміністрації Data Protection Authority, висловився з цього питання, заявивши, що для відслідковування Facebook використовує cookie-файли, здатні передавати інформацію про комп'ютер користувача та його переміщення по все-

світній павутині. За словами Й. Каспара, це пряме порушення німецьких і навіть загальноєвропейських норм конфіденційності, та, якщо самі користувачі не дають згоду на таке слідкування за ними, Facebook повинна видалити всі свої файли з їхніх комп'ютерів. Агентство Data Protection Authority дійшло висновку, що cookie-файли від Facebook можуть залишатися в персональному комп'ютері власника вилученої сторінки на термін до двох років, і допомогти може лише повне видалення всіх таких файлів з використанням спеціалізованого програмного забезпечення [6].

До того ж Центр захисту недоторканності особистого життя в Німеччині оприлюднив заяву, в якій вказувалося, що керівництво соціальної мережі передає особисту інформацію про користувачів третім особам у США. "Користувачі Facebook повинні знати, що вони відслідковуються компанією", – заявили представники Центру, відзначивши, що це порушення закону Євросоюзу із захисту особистої інформації [7].

Про тотальне відслідковування даних користувачів наголошує і Джуліан Ассанж, засновник Wikileaks. До того ж він відмічає, що ці дані передаються до баз даних спецслужб. Він назвав Facebook "самим нахабним інструментом шпигунства з усіх, що коли-небудь були створені людиною". "Користувачі повинні розуміти, що, додаючи контакт у свій Facebook, вони працюють на американські розвідки, оновлюючи їх бази даних. Інші розвідки можуть або зламати Facebook, або отримати цю інформацію від американців у обмін на якісь послуги" [8].

Розглянемо більш детально як проводиться відслідковування даних користувачів соціальною мережею Facebook.

Перший сценарій відстеження відноситься до користувачів, у яких вже є аккаунт на Facebook. Коли обліковий запис створено, Facebook видає файл ідентифікатор, так званий cookie, що містить унікальний ідентифікатор (ID) користувача. Cookie – це невеликий фрагмент даних, створений веб-сервером або веб-сторінкою та зберігається на комп'ютері користувача у вигляді файлу, який веб-клієнт (зазвичай веб-браузер) щоразу пересилає веб-серверу в HTTP-запиті при спробі відкрити сторінку відповідного сайту. Застосовується для збереження даних на стороні користувача, на практиці зазвичай використовується для: аутентифікації користувача; зберігання персональних переваг і налаштувань користувача; відстеження стану сесії доступу: користувача; ведення статистики про користувачів. До речі, це прості текстові дані і вони не можуть виконувати будь-які дії самостійно. Зокрема, cookie не можуть бути ні вірусами, ні шпигунськими програмами [9].

Отже, cookie сприяють відображенню імені користувача в полі для логіну при повторних візитах. Вони містять всю інформацію, яка необхідна для авторизації в соціальній мережі, що і дозволяє фахівцям

Facebook відрізняти одного користувача від іншого при зборі інформації про нього. При вході на Facebook через інший пристрій використовуються тимчасові cookie, які замінюються файлами з тим же ID після входу в аккаунт.

Cookie використовується як маркетинговий інструмент, який збирає інформацію про відвідані користувачем сторінки, соціальні мережі, інтернет-магазини, банківські сервери тощо. Іншими словами, вони формують картину звичок і способу життя користувачів. Ця інформація важлива для маркетологів, які на основі цих даних здійснюють більш таргетовану рекламу. Причому користувачеві досить зайти на сторінку соціальної мережі навіть на кілька хвилин, і потім інформація про його подальше переміщення по Інтернету протягом декількох днів чи місяців або навіть років буде зберігатися на сервері соціальної мережі. Розробники сервісу установлюють більш тривалий час збереження даних облікового запису користувача для того, щоб зібрати якомога більше інформації.

Другий сценарій. Соціальна мережа Facebook постійно відслідковує дії користувачів, збираючи їхні дані, навіть тоді, коли користувачі не авторизовані в системі.

Натискаючи кнопку "Вихід" на своїй сторінці в Facebook, користувач насправді залишається в мережі – просто одні файли cookie підміняються іншими, що і створює видимість виходу. При переході на будь-який інший сторонній сайт, де є кнопка Like (Мені подобається), але яка керована Facebook, натискуючи на цю кнопку, користувач соціальної мережі забезпечує Facebook деталями логіна і повідомленням про те, що йому подобається, опублікованому на сторінці профілю. Слід відмітити, що кнопка від мережі Facebook встановлена більше ніж на 350 найпопулярніших сайтах з першої тисячі, то можна сказати, що це є дуже серйозним інструментом для відслідковування даних про користувачів. При цьому користувачі навіть не підозрюють, що мережа Facebook продовжує збирати всі потрібні їй відомості про того чи іншого учасника, про те на які сайти він ходить, якими сервісами він користується, і якщо мова йде про мобільний доступ, де він у даний момент знаходиться.

Однак інформація про користувача відправляється на Facebook незалежно від того, чи була кнопка "Мені подобається" реально активована чи ні.

Третій сценарій. Facebook може відстежувати ваші дії в мережі Інтернет, навіть якщо ви не є користувачем цієї соціальної мережі. Якщо користувач не має аккаунта на Facebook, то cookie та ID користувача є недостуупними. У цьому випадку HTTP GET запит (використовується для запиту вмісту зазначеного ресурсу) кнопки "Мені подобаєть-

ся" не видає cookie. Проте, коли відвідується сайт, що має Facebook Connect (сервіс, що надається соціальною мережею Facebook, за допомогою якого користувачі можуть, використовуючи свій логін і пароль від Facebook, користуватися іншими популярними соціальними сайтами), цей додаток заводить cookie. З цього моменту при відвідуванні інших сайтів з кнопкою "Мені подобається" запитуються дані користувача з cookie. Це означає, що Facebook отримав ще одну порцію інформації, не питаючи дозволу.

Якщо врахувати, що cookie можуть бути дійсні протягом двох років, стає зрозуміло чому і як поширюються дані користувачів. Маючи cookie, можна відстежити практично всі дії в мережі. Кожен сайт, який включає будь-який вміст Facebook, буде ініціювати взаємодії з його серверами, розкриваючи інформацію про відвідуваний сайт разом із cookie.

Отже, якщо ви ніколи не були на Facebook – варто вам зареєструватися і вся ваша історія буде доступна для соціальної мережі. При реєстрації ваш тимчасовий ID надсилається на Facebook як частина запиту для завантаження сторінки і сервер відповідає створенням вже нового ідентифікатора для зареєстрованого користувача, пов'язуючи його з усіма вашими доступними даними.

Як пояснює голландський учений Роозендааль, зв'язок між цим старим і новим ідентифікатором таємно здійснюється серверами Facebook. Це означає, що вся зібрана в минулому інформація про користувача може бути прив'язана до щойно створеного, чистого аккаунту на Facebook. З цього моменту будь-які запити вмісту Facebook будуть супроводжуватися унікальним ID користувача [10].

Із технічної точки зору, слід також відмітити, що у сервісу мікроблогів Twitter кнопка Like має такий же ефект і використовують її навіть частіше ніж від Facebook. Тільки слідкує вона не за всіма користувачами, а за тими, хто авторизувався на сайті хоча б один раз за останній місяць. Але спостереження ведеться абсолютно завжди, незалежно чи закритий у вас браузер або вимкнений комп'ютер.

Соціальні мережі Facebook, Twitter і Google всі як один заперечували відслідковування, але потім усе ж пояснили, що збір даної інформації використовується тільки для рекомендації реклами. Як приклад, ви зайшли на сайт "Як справлятися з депресією", так Google вам порадить таблетки, які вам би порадив рекламодавець. Така реклама дуже ефективна, адже вона завжди під рукою. Але які причини б не переслідували мережі, відслідковування є відслідковуванням [11].

Вочевидь, що й інші соціальні мережі також відслідковують своїх користувачів. Так популярний російський соціальний сервіс Вконтакте багато що запозичує в Facebook, у тому числі й у питанні відслід-

ковування користувачів. У результаті в базі даних російської соціальної мережі вже зібраний гігантський компромат на всіх своїх користувачів, готовий у будь-який момент опинитися в руках спецслужб, Вконтакт також стежить за переміщеннями користувачів на інших сайтах [12].

Ще більшого занепокоєння викликає проблема несанкціонованого витоку конфіденційної персональної інформації через технічний механізм (прикриття) з соціальних мереж і використання її спецслужбами окремих держав.

Так, директор розвідувального центру при ЦРУ США Open Source Ctyter Даг Накуін повідомив журналістам, що ввірений йому підрозділ стежить за змістом соціальних мереж практично в усьому світі, зокрема, щоденно фільтрується до п'яти мільйонів твістів [13].

За повідомленням офіційного сайту ЦРУ, із грудня 2006 року цей структурний елемент американського розвідувального співтовариства використовує мережу Facebook для вербування кандидатів для роботи у національних секретних службах [14, с. 87]. Аналогічна інформація надходить про використання соціальних мереж спецслужбами Великобританії, зокрема, розвідувальною службою МІ-6 [15].

До речі, і у вітчизняних спеціальних наукових джерелах останнім часом оприлюднюються думки про те, що спецслужби іноземних держав мають певні можливості для цілеспрямованого моніторингу соціальних мереж з метою виявлення серед громадян України корисних їм, у тому числі придатних для конфіденційного співробітництва [14, с. 88], та про те, що загрози несанкціонованого збирання персональних даних і побудови прихованих каналів зв'язку можуть бути реалізовані на рівні спеціальних служб та інших силових структур, що мають протиправні наміри з різним рівнем мотивації [16, с. 19].

Підсумовуючи, ми маємо зробити висновок, що подібні маніпуляції не можуть бути проведені, а ні випадково, а ні окремою особою, а ні навіть будь якою організованою групою, без відповідної негласної підтримки на певному, в ряді випадків і державному, рівні. Ми маємо визнати, що такий системний збір, зберігання, аналіз і систематизація персональних даних користувачів загалом пояснюється тим, що має місце постійне, системне та організаційно досконале використання спеціальними службами певних держав і злочинними організаціями соціальних мереж для негласного збору різнопланової розвідувальної інформації шляхом протиправного використання їх технічних можливостей. Завдяки цьому, протиправно створюються значні інформаційні масиви, що містять величезну кількість персональних даних, у ряді випадків негласно викрадених із персональних комп'ютерів користувачів, конфіденційних відомостей, що стосуються фактично індивідуально

необмеженого кола осіб. У свою чергу, така інформація, після її відповідної обробки, систематизації та аналізу може бути використана (а з великою вірогідністю можна стверджувати, що вже досить тривалий час використовується) задля вивчення осіб (у першу чергу, представників органів влади та управління), які потенційно можуть становити оперативний інтерес для спеціальних служб іноземних держав чи бути вразливою жертвою корисливого злочину або бути втягненими злочинними організаціями у різні види протиправної діяльності (терористичної, екстремістської, загальнокримінальної тощо).

Отже, стан, пов'язаний із обігом інформації у соціальних мережах, що сьогодні практично перебувають поза межами правового регулювання та контролю з боку суспільства і держави, має розглядатись як одна із загроз національній безпеці України, під якою, відповідно до Закону України "Про основи національної безпеки України" від 19 червня 2003 року № 946-IV, розуміють захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечується сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національним інтересам [17].

Список використаних джерел

1. Бутузов В. М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : монографія / В. М. Бутузов. – К. : КИТ, 2010. – 408 с.

2. Гавловський В. Д. До питання захисту персональних даних у соціальних мережах / В. Д. Гавловський // Б-ба з орг. злоч. (теорія і практика) : наук.-практ. журнал. – К. : МНДЦ при РНБО України, 2011. – № 24. – С. 252–262.

3. На Facebook подают в суд в Калифорнии: соцсеть тоже шпионила за пользователями / [Електронний ресурс]. – Режим доступу :
http://hitech. newsru. com/article/03Oct2011/fcbksuit).

4. Facebook постоянно следит за пользователями / [Електронний ресурс]. – Режим доступу:
http://www. versii. com. ua/news/240639.

5. Facebook збирає досьє на тих, хто ще не зареєстрований / [Електронний ресурс]. – Режим доступу :
http://vidgolos. com/119526-facebook-zbiraye-dosye-na-tix-xto-shhe-ne. html.

6. Германия обвиняет Facebook в слежке за пользователями / [Електронний ресурс]. – Режим доступу :
http: // infox. ru / hi- tech / internet/2011/11/03 /Gyermaniya_obvinyaye phtml.

7. Facebook постоянно следит за пользователями / [Електронний ресурс]. – Режим доступу :
http://www. versii. com. ua/news/240639.

8. "Шпионы кардинала": за нами следят "айфоны", "андроиды", социальные сети и даже ФСБ. Паникуем? / [Електронний ресурс]. – Режим доступу :
http://www. aif. ru/techno/article/42864.

9. HTTP cookie [Електронний ресурс] / Википедия. – Режим доступу : http://ru. wikipedia. org/wiki/HTTP_cookie.

10. Голландский ученый уличил кнопку Facebook “Мне нравится” в глобальном шпионаже / [Електронний ресурс]. – Режим доступу : http://hitech. newsru. com/article/03dec2010/fcbkilikebttn.

11. Facebook, Twitter и Google всё таки следят за вами / [Електронний ресурс]. – Режим доступу : http://www. vsozial. ru/news/facebook_twitter_vsjo_taki_sledjat_za_vami.

12. Будьте осторожны – за Вами следят он лайн / [Електронний ресурс]. – Режим доступу : http: // www. postsovet. ru/blog/264723. html.

13. Спецслужбы раскинули социальные сети / [Електронний ресурс]. – Режим доступу : http: // www/pravda. ru/society/hov/08-11-2011/1097800-cru-0.

14. Хома О. В. Соціальні мережі Інтернету як засіб збору іноземними спецслужбами персональних даних про особистість / О. В. Хома // Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф., 22 берез. 2011 р. : [у 2 ч.]. – К. : Наук.-вид. відділ НА СБ України, 2011. – Ч. 2. – С. 86–90.

15. Метью Тейлор MI-6 шукає рекрутів на Facebook [Електронний ресурс] / Метью Тейлор. – Режим доступу : http: //www. guardian. co. uk/technology.

16. Довгань О. Д. Соціальні мережі в завданнях забезпечення кібербезпеки держави / О. Д. Довгань, С. В. Мельник // Актуальні проблеми управління інформаційною безпекою держави : зб. мат. наук.-практ. конф., 22 берез. 2011 р. : [у 2 ч.]. – К. : Наук.-вид. відділ НА СБ України, 2011. – Ч. 2. – С. 19–21.

17. Про основи національної безпеки України : Закон України від 19 черв. 2003 р. № 964-IV // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351.

В статье исследуются вопросы информационной безопасности, связанные с новой реальной угрозой – фактическим собиранием и систематизацией персональных данных пользователей социальных сетей, с последующим противоправным использованием таких данных.

The article deals with the questions of the information safety, related to the new real threat - actual acquisition and systematization of the personal data of the users of the social networks, with the subsequent illegal use of such information.

Стаття надійшла до редакції журналу 23 грудня 2011 р.