УДК 354.42/.44:343.4

Кучеренко Марія Сергіївна –
Радник начальника Департаменту правової підтримки та захисту малого та середнього бізнесу при Кабінеті Міністрів України,

Мельник Алла Олексіївна –
старший науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України

До питання дефініції та характеристики суспільної небезпеки крадіжки особистості у соціальних мережах

У статті досліджуються проблеми інформаційної безпеки, що пов'язані з новою загрозою для українського інформаційного простору, а саме із визначенням і суспільною небезпекою крадіжки особистості у соціальних мережах.

Ключові слова: інформаційна безпека, мережа Інтернет, кіберпростір, крадіжка особистості, викрадення персональних даних, соціальні мережі.

Постановка проблеми. Сьогодні автоматизовані системи, реалізовані на основі комп'ютерних мереж, а також мережа Інтернет, як всесвітня інформаційна система загального доступу, стали невід'ємними елементами суспільного життя, без яких повноцінне функціонування суспільства видається неможливим.

Однією із тенденцій формування в Україні інформаційного суспільства є збільшення масової Інтернет-аудиторії та створення специфічного "мережного" соціокультурного середовища. Одним із проявів даної тенденції необхідно вважати зростаючу популярність соціальних мереж. Як свідчать дослідження Міжнародної консалтингової компанії J'son&Partners Consulting, країни СНД, а, відповідно, і Україна, є світовими лідерами у збільшенні кількості користувачів соціальних мереж, адже станом на 2010 рік щорічний приріст зареєстрованих осіб становив близько 30 % і налічував понад 8 млн осіб [1, с. 253]. Наразі можна

зазначити, що ці цифри лише збільшуються. Так, наприклад, за останніми статистичними дослідженнями кількість користувачів мережі Facebook становить 750 млн користувачів, найбільшої китайської соціальної мережі Qzone – 480 млн користувачів, а найпопулярнішої в країнах СНД мережі VKontakte – 135 млн користувачів [2].

Сьогодні у світі діє велика кількість різноманітних соціальних мереж – спеціалізованих (наприклад, мережа лікарів, мережа студентів конкретного навчального закладу), загальних, всесвітніх (наприклад, Facebook) і тих, що популярні в одній конкретній країні (наприклад, Qzone).

Абсолютна ілюзія спілкування з реальними людьми, можливість пошуку давніх друзів, створення співтовариств, можливість завантажувати і розміщувати фото і відеоматеріали, віртуальні подарунки – це все те, що зробило соціальні мережі популярними [3, с. 16].

Актуальність даної проблеми полягає в тому, що поряд із появою зручного інструменту для спілкування людей – соціальними мережами, який можна використовувати з інформаційною, діловою чи особистою метою, цей інструмент одночасно можна використовувати у протиправних, а часом і злочинних цілях. Із розвитком високих технологій почали вдосконалюватись і способи вчинення традиційних злочинів (крадіжка, вимагання, шахрайство тощо), набуло розповсюдження неправомірне збирання та використання особистих даних. Існуюча на сьогодні система накопичення та зберігання персональних даних у соціальних мережах створює плідне підґрунтя для їх неправомірного використання, втягнення громадян України до злочинної діяльності як зарубіжними спецслужбами, так і різноманітними терористичними та злочинними організаціями. Система захисту персональних даних, яка сьогодні діє в Україні все ще залишається недосконалою та потребує подальшого доопрацювання для кращого захисту законних прав осіб на власні персональні дані.

Ступінь розробленості проблеми. Дотепер всеохоплюючі наукові дослідження проблеми "викрадення особистості" вітчизняними вченими ще не проводились. Сьогодні проблема соціальних мереж і захисту персональних даних у них отримала розробку в працях В. М. Бутузова та В. Д. Гавловського.

Отже, **мета даної роботи** – звернути особливу увагу на новий вид загрози в українському інформаційному просторі – системне відслідковування, аналіз та збирання персональних даних користувачів соціальних мереж для їх подальшої неправомірної передачі стороннім особам з метою використання у власних інтересах.

Виклад основного матеріалу. Розвиток інформаційних технологій, "віртуалізація" форм особистого спілкування та ведення бізнесу породжують не тільки вдосконалення способів учинення "традиційних" злочинів, а й стають підґрунтям для створення нових, сучасних

видів протиправних дій. Забезпечення безпеки персональних даних в Україні наразі ще не має достатнього законодавчого, і, перш за все, морального забезпечення. Прийняття Закону України "Про захист персональних даних" [4] є лише першим кроком у забезпеченні інформаційної безпеки та захисту прав громадян.

Необхідно зазначити, що заволодіння чужим ім'ям, діловою репутацією та чистою кредитною історією не є винаходом мережі Інтернет, але саме широке використання комп'ютерів та інформаційних систем сьогодні полегшує роботу особам, які бажають заволодіти чужими персональними даними.

Останнім часом серед так званих "кіберзлочинів" усе більше трапляється випадків "крадіжки особистості" (англ. "Identity theft"), під якою розуміють діяння, коли протиправно вилучаються та (або) використовуються персональні дані людини (індивіда) з метою незаконного отримання матеріальної вигоди чи інших протиправних діянь [1, с. 254]. Іноді надається й інше визначення даного явища: крадіжка особистості – це шахрайство, яке полягає в отриманні персональних або фінансових відомостей користувачів з метою використати ім'я люди або його посвідчення особи для здійснення фінансових операцій чи купівлі [5].

На нашу думку, більш вдалим є перше із зазначених визначень, однак цілком погодитись із ним ми не можемо. Адже, відповідно до ст. 2 Закону України "Про захист персональних даних": "Персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована" [4]. Тобто, це ті відомості, які позначають окремого індивіда та дозволяють ідентифікувати його з-поміж інших. Проте, як свідчить практика, крадіжки особистості часто вчиняються не лише з метою заволодіння відомостями, що ідентифікують особу, а й інформацією про її фінансовий стан, її кредитну історію. Отже, ми вважаємо, що необхідно розширити визначення крадіжки особистості, звернувши увагу саме на можливість неправомірного заволодіння не лише відомостями, яких достатньо для ідентифікації, але й іншими даними.

Станом на сьогодні заволодіння персональними даними як склад самостійного злочину ще не передбачено у вітчизняному кримінальному законі.

У Сполучених Штатах Америки зроблені певні кроки щодо захисту персональних даних. Зокрема, в цій державі крадіжка особистості пов'язана з широким використанням SSN (Social Security Number) в якості посвідчення особи. SSN – це дев'ятизначний номер, який має вигляд: ***-**-****, де перші три цифри – номер регіону, дві наступні – номер групи, і чотири останні – послідовний номер у даній групі. Цей номер присвоюється громадянам і резидентам США, основне його

завдання полягає в податковому та пенсійному обліку, однак наразі, із поширенням можливостей віддаленого доступу до товарів, послуг, які можуть бути надані без особистої присутності, функції цього номеру розширилися. Тепер його можуть вимагати при прийнятті на роботу, для отримання медичних послуг, у банках – при відкритті рахунків.

Спеціальним органом, до якого надходять скарги громадян щодо шахрайства у США, є Федеральна комісія по торгівлі (FTC, США). Як свідчить статистика, найбільша кількість скарг, які були отримані цим органом у 2010 році, стосувалась саме крадіжок персональних даних (крадіжок особистості). Всього за 2010 рік було зафіксовано 250 854 таких скарг, що склало близько 19 % від усієї кількості скарг на шахрайство (з 1,3 млн загальної кількості скарг). Особливо багато скарг на такий вид шахрайства надходить від власників мобільних телефонів, користувачів соціальних мереж, блогеррів, отримувачів СМС-повідомлень та електронних листів [6].

У Великобританії для крадіжки особистості також використовуються страхові ідентифікатори – так звані NINO (National Insurance Number) и NHS (National Health Service Number). Так, у Великобританії для того, щоб 17 років жити під чужим ім'ям і отримати кредити на суму понад 270 тис. доларів було достатньо паспорта, водійських прав і картки соціального страхування [7].

Соціальні мережі, як засіб спілкування людей, є системою з широким переліком персональних даних, які особа повинна оприлюднити про себе для реєстрації у відповідній мережі, і ще більший перелік відомостей, які особа може розмістити на своїй сторінці (з метою покращення обслуговування, полегшення пошуку друзів, з інших підстав), створює зручне підґрунтя для здійснення різноманітних шахрайських дій. Також необхідно зазначити, що ці шахрайські дії можуть набувати як прямого, "традиційного" характеру, який прямо передбачений у Кримінальному кодексі України, так і бути опосередкованими – коли заволодіння коштами в момент учинення протиправних дій може і не відбутись. Однак при цьому правопорушники отримують доступ до персональних даних користувача соціальної мережі, до переліку його друзів і рідних, а в деяких випадках, за допомогою шкідливих програм, зловмисники здатні перехоплювати управління комп'ютером користувача – що може стати підґрунтям для вчинення подальших шахрайських дій в мережі Інтернет щодо інших осіб (фішинг, "зомбовані" комп'ютери, вимагання грошей від імені родичів або друзів та інші прийоми Інтернет-шахрайства).

При реєстрації і подальшому використанні соціальної мережі особа добровільно повідомляє про себе значну кількість персональних даних – прізвище, ім'я, по-батькові, місце навчання, дату народження, місце проживання, рідне місто, номери телефонів (домашній, робочій та ін.), номер ICQ, ідентифікатор Skype, персональну сторінку в мережі

Інтернет, відомості про рід занять, віросповідання, політичні погляди, партійну приналежність, захоплення, коло родичів і друзів. Оприлюднюючи таку велику кількість особистих даних (які в звичайному житті особи схильні приховувати), користувачі соціальних мереж іноді навіть не підозрюють наскільки широкому колу осіб надана ними інформація може стати відомою. Більшість користувачів не усвідомлюють і не можуть усвідомити всю реальну та потенційну небезпеку можливого протиправного використання їх персональної інформації щодо фактично всіх сфер свого особистого та професійного життя.

Власники багатьох соціальних мереж переконують користувачів, що інформація, яку вони розміщують у мережі, є особистою та захищеною від сторонніх осіб. Але на практиці це є не зовсім вірним, адже, як мінімум, доступ до цієї інформації мають власники соціальних мереж та адміністратори, а як максимум, – практично всі особи (як особи, які мають можливість переглядати сторінку користувача, так і особи, які поставили собі за мету "зламати" сторінку користувача і вилучити персональні дані).

Як відомо, існує декілька поширених способів зламу сторінок у соціальних мережах – простий підбір пароля до аккаунту (для цього часто треба лише добре вивчити користувача, адже в якості пароля здебільшого може використовуватись дата народження, номер телефону, ім'я, тобто такі дані, які доступні на персональній сторінці користувача), відновлення паролю в електронній пошті за допомогою секретного запитання, відповісти на яке також найчастіше не складно для зловмисника, який добре вивчив користувача, чиї персональні дані він бажає отримати, брутфорс – перебір усіх можливих варіантів паролю за допомогою спеціальних програм (найчастіше використовується для електронної пошти, адже в соціальних мережах існує обмеження на кількість неправильно введених паролів), отримання паролів за допомогою спеціальних комп'ютерних програм – "троянів", які проникають до комп'ютера разом із якоюсь безпечною програмою, викрадають паролі та відправляють їх зловмиснику [1, с. 256–257].

Однією із суттєвих характеристик крадіжки особистості, як протиправного вилучення та (або) використання персональних даних людини з метою незаконного отримання матеріальної вигоди чи вчинення інших протиправних діянь, є те, що саме безпосереднє вилучення персональних даних відбувається, фактично, в особливому середовищі – кіберпросторі.

Останнім часом на проблеми та особливості кіберпростору, як особливого середовища вчинення злочинів звертається все більше уваги. Окремі дослідники визначають кіберпростір наступними чином: "Кіберпростір (кібернетичний простір) – це штучне електронне середовище існування інформаційних об'єктів у цифровій формі, що утворене в результаті функціонування кібернетичних комп'ютерних систем управління та обробки інформації та забезпечує користувачам доступ

до обчислювальних й інформаційних ресурсів систем, вироблення електронних інформаційних продуктів, обмін електронними повідомленнями, а також можливість за допомогою електронних інформаційних образів у режимі реального часу вступати у відносини (взаємодіяти) щодо спільного використання обчислювальних та інформаційних ресурсів системи (надання інформаційних послуг, ведення електронної комерції тощо)" [8, с. 80]. Інші дають більш лаконічне визначення: "Кібернетичний простір – простір, сформований інформаційно-комунікаційними системами, в якому проходять процеси перетворення (створення, зберігання, обміну, обробки та знищення) інформації, представленої у вигляді електронних комп'ютерних даних" [9, с. 43].

На нашу думку, більш всеохоплюючим є перше із зазначених визначень, яке і необхідно використовувати при визначенні певних дій осіб як крадіжки особистості. Варто зауважити, що фактично визначити місце вчинення крадіжки особистості дуже важко й іноді практично неможливо прив'язати до території певної окремої країни, через використання в процесі протиправного заволодіння персональними даними осіб сучасних інформаційних технологій і засобів зв'язку.

Також необхідно звернути увагу, що протиправне заволодіння персональними даними осіб може відбуватись різними особами з різною метою – як для незаконного збагачення, так і з розвідувальними цілями або з метою втягнення осіб до незаконної діяльності, на що неодноразово вказував В. Д. Гавловський [10].

Проаналізувавши все вищезазначене, можемо зробити **висновок** про фактичне існування в інформаційному просторі великої кількості соціальних мереж, залучення до них мільйонів користувачів, а, особливо, існування цих систем без належного законодавчого та практичного контролю з боку держави, що створює сприятливе середовище для проведення різноманітних дій злочинного характеру.

Отже, виникає негайна потреба у розробці та створенні належних заходів правового регулювання доступу до персональних даних у соціальних мережах, з чітким зазначенням статусу власників соціальних мереж, адміністраторів соціальних мереж, технічного персоналу стосовно використання, зберігання та захисту персональних даних у соціальній мережі; формуванні основних принципів юридичної відповідальності за незаконне розголошення відомостей персонального характеру; подальшої розробки та формулювання поняття "крадіжка особистості", а також характеристики цього діяння з точки зору кримінального закону; розробці системи заходів щодо обмеження прав користування соціальними мережами певними категоріями громадян (військовослужбовцями, особами, що мають доступ до державної таємниці).

Список використаних джерел

1. Гавловський В. Д. До питання захисту персональних даних у соціальних мережах / В. Д. Гавловський // Боротьба з організованою злочинністю і корупцією (теорія і практика) : наук.-практ. журнал. – 2001. – № 24. – С. 252–262.

2. Десять самых популярных социальных сетей / [Электронный ресурс]. – Режим доступа :
http://www. social-networking. ru/news/ten-biggest-social-networks.

3. Гавловський В. Д. Соціальні мережі і національна безпека / В. Д. Гавловський // Актуальні проблеми управління інформаційною безпекою держави : зб. мат-лів наук.-практ. конф. (Київ, 22 берез. 2001 р.) : [у 2 ч.]. – К. : Вид-во НАСБ України, 2011. – Ч. 2. – С. 16–18.

4. Про захист персональних даних : Закон України від 1 черв. 2010 р. № 2297-VI / [Електронний ресурс]. – Режим доступу :
http://zakon2. rada. gov. ua/laws/show/2297-17.

5. Кража личности / [Электронный ресурс]. – Режим доступа :
http://www. securitylab. ru/news/tags/.

6. Кража личности / [Электронный ресурс]. – Режим доступа :
http://rusfront. ru/1367-krazha-lichnosti. html.

7. Россиянин арестован за кражу личности / [Электронный ресурс]. – Режим доступа :
http://lifenews. ru/news/56272.

8. Погорецький М. А. Поняття кіберпростору як середовища вчинення злочину / М. А. Погорецький, В. П. Шеломенцев // Інформаційна безпека людини, суспільства, держави : наук.-практ. журнал. – К. : НАСБУ. – 2009. – № 2 (2). – С. 80–85.

9. Мельник С. В. До проблеми формування понятійно-термінологічного апарату кібербезпеки / С. В. Мельник, О. О. Тихомиров // Актуальні проблеми управління інформаційною безпекою держави : зб. мат-лів наук.-практ. конф., (Київ, 22 берез. 2001 р.) : [у 2 ч.]. – К. : Вид-во НАСБ України, 2011. – Ч. 2. - С. 43-48.

10. Гавловський В. Д. До питання несанкціонованого збору та систематизації персональних даних користувачів через соціальні мережі / В. Д. Гавловський // Боротьба з організованою злочинністю і корупцією (теорія і практика) : наук.-практ. журнал. – 2011. – № 25–26. – С. 312–319.

В статье исследуются проблемы информационной безопасности, которые связаны с новой угрозой для украинского информационного пространства, а именно с определением и общественной опасностью кражи личности в социальных сетях.

The article deal with the problems of the informative security, which are related to the new threat for the Ukrainian informative space, namely with the determination and public danger of the identity theft in the social networks.

Стаття надійшла до редакції журналу 1 червня 2012 року.