УДК: 316.472.4:342.7:001.103-027.552:004.451.5

Муха А. В.
науковий керівник: Павлюх М. В.,
кандидат наук із соціальних комунікацій, асистент кафедри міжнародної інформації, Національний університет «Львівська політехніка»

ЗАГРОЗИ ВИКОРИСТАННЯ ПЕРСОНАЛЬНИХ ДАНИХ У МЕРЕЖІ ІНТЕРНЕТ

У статті розглянуто популярні випадки використання персональних даних соціальними мережами. Досліджено маркетингову політику багатьох компаній, які часто використовують персональні дані своїх клієнтів задля постійного контролю та нав'язування своїх товарів чи послуг. З'ясовано, що кібершахрайство постійно використовує персональні дані осіб задля афер та збагачення.

Ключові слова: *маркетинг, персональні дані, юридичний захист, кіберзлочинці.*

Mukha A. V.

THREATS OF USE OF PERSONAL DATA ON THE INTERNET

The article deals with popular cases of personal data usage by social networks. It explores the marketing policies of many companies that often use their customers' personal information to constantly monitor and link their products or services. It has been found that cyber fraud constantly uses personal data of individuals for scams and enrichment.

Key words: *marketing, personal data, legal protection, cybercriminals.*

У процесі глобалізації світу та розвитку інформаційних технологій людина отримує доступ до нових можливостей. Але ці можливості стикаються із ризиками, які є загрозою для її безпеки, свободи та приватного життя. На сьогодні, найбільш поширеним видом протиправної деструктивної діяльності в мережі Інтернет є збір та аналіз персональних даних користувачів, які використовуються для несанкціонованого використання.

Проблема загроз персональним даним та витоку конфіденційної інформації зафіксована у всіх країнах світу. За різними джерелами, від 70% до 90% даних, що викрадаються, становлять персональні дані. За даними дослідження «Інформаційна безпека бізнесу 2012» [3], загроза витоку персональних даних посідає друге місце серед основних загроз бізнесу.

Сьогодні проблема викрадення персональних даних перетворюється у кримінальний вид комерційної діяльності, метою якого є продаж викрадених персональних даних. Активна обробка персональних даних проводиться на віддалених серверах, до яких користувачі не мають прямого доступу. Користувачі, які здійснюють покупку через мережу Інтернет, змушені повідомляти свої персональні дані. Саме ці Інтернет-магазини, як правило, зацікавлені в отриманні даних від покупців, адже так вони можуть аналізувати ринок та відтворювати продукцію за системою попиту та пропозиції. Але не завжди Інтернет-магазини забезпечують належний захист персональних даних користувача, деякі із них навіть можуть збирати та пропонувати персональні дані для продажу й отримання прибутку.

Темі захисту персональних даних у мережі Інтернет присвячено чимало наукових статей та публікацій, закордонних та українських. Темі викрадення персональних даних у соціальних мережах присвячені статті: D. Solove у журналі Американської науки; виступ C. Lampe на конференції, присвяченій новітнім технологіях, зокрема мережі Фейсбук, та співзвучна стаття M. Gebel, присвячена цій популярній мережі. Ці проблеми також порушують українські вчені: І. Березовська і В. Брижко, які досліджують викрадення і загрози використання персональних даних у популярних мережах та кіберзлочинах.

Мета статті – дослідити ступень загрози використання персональних даних у мережі Інтернет у різних сферах (маркетології, інтернет-продажах, бізнесі).

Мета передбачає такі завдання:

– з'ясувати, які існують загрози використання персональних даних в мережі Інтернет;

– дослідити інформаційну та комп'ютерну безпеку у сфері персональних даних;

– знайти шляхи забезпечення захисту персональних даних;

– вивчити європейський досвід правового поля «персональних даних»;

– проаналізувати законодавство України щодо правового регулювання персональних даних;

– зіставити європейське і українське законодавства у сфері персональних даних.

Серйозну загрозу для персональних даних становлять маркетологи різних комерційних компаній. Збір та пошук відомостей, таких як: діяльність, оточення, погляди, стосунки, характер, інтереси, поведінка, фінансова забезпеченість та багато інших даних, які є персональними даними, становлять комерційно важливу інформацію для маркетологів. Відомо, що за допомогою мережі Інтернет набагато легше збирати великі обсяги різної інформації, адже правильне використання цієї інформації приведе до збільшення прибутків [9, 31].

Проглядаючи веб-сторінки протягом тривалого часу, можна помітити, що реклами прямують за користувачем із сайту на сайт. Зміст цієї реклами заповнюється продуктами або послугами, які користувач міг переглядати раніше. Для відстеження дій користувача в мережі Інтернет використовуються файли-cookie, які і є персональними даними. Але це не єдиний спосіб відстеження персональних даних. Маркетологи компаній також використовують MAC-адресу та обліковий запис користувача для відстеження дій в Інтернеті. Як правило, більшість користувачів не заперечують, коли реклама обслуговує їхні інтереси, але, оскільки персональні дані стають більш важливими для компаній, розробників і рекламодавців, то за замовчуванням відбувається набагато більше відстеження.

У цей момент, коли стеження може прямувати за користувачем у режимі реального часу, різноманітні компанії та служби можуть збирати персональні дані користувача та обмінюватися MAC-адресою комп'ютера або маршрутизатора користувача з рекламодавцями та компаніями третіх сторін. В такому випадку у користувача немає прямої взаємодії з цими компаніями, що не мають контролю за власними персональними даними. Згодом відстеження поширюється на мобільні додатки користувача, які для того, щоб запропонувати свої послуги, просять доступ до номеру телефона, контактів та інших функцій телефона користувача.

Існує багато служб у мережі Інтернет, які відстежують та використовують персональні дані користувача. Наприклад, Google Maps відстежує місце розташування користувача в режимі реально часу та хронологію його пересування. Інший сервіс під назвою Glancee від Facebook може відстежувати місцеперебування конкретного користувача у пасивному режимі. Тобто, цей сервіс може показувати користувачу, де знаходяться його «друзі», а також показує користувачів мережі зі схожими інтересами поблизу користувача. На відміну від Google Maps, Glancee не вимагає реєстрації і працює у «тіні»,

проводячи моніторинг даних геолокації. Маркетологи рекламують цей сервіс, як «спосіб виявити навколо себе приховані зв'язки», але насправді це сервіс, який збирає персональні дані користувачів і використовує у своїх комерційних цілях [11].

Веб-сайти та Інтернет служби, які не мають нової та надійної системи безпеки, можуть залишити інформацію, яка містить персональні дані користувача, і дані, що передаються між комп'ютером користувача і веб-сервером на ризик від хакерів. Наприклад, веб-сайти, які використовують застарілий стандарт HTTP для веб-комунікації, а не більш надійний HTTPS, позбавлені зашифрованого з'єднання між комп'ютером або смартфоном та веб-сайтом, до якого він підключений. Це означає, що дані, що існують між двома точками, можуть контролюватися іншими компаніями або потенційно підхоплені та викрадені хакерами для більш небезпечних цілей.

Сучасні Smart телевізори, холодильники із системою оновлення через мережу Інтернет, навушники з підтримкою Wi-Fi також можуть становити загрозу витоку персональних даних. Відсутність стандартів безпеки в Інтернеті, речі, колективне ім'я, пов'язане із підключеними та інтелектуальними пристроями означає, що деякі пристрої можуть не мати зашифрованих з'єднань із серверами, які керують їхніми розумними функціями, або можуть бути вразливими до простих методів злому, що перетворює їх на мішені для кіберзлочинців.

Використання громадських точок доступу до мережі Інтернет через Wi-Fi також може бути загрозою викрадення персональних даних користувача. Проблема полягає в тому, що вони часто мають слабку систему захисту або взагалі відсутня система безпеки чи шифрування, а це означає, що хакери можуть перехоплювати персональні дані, що передаються між пристроєм користувача і точкою доступу до мережі Інтернет. Деякі точки доступу мають веб-портал, який вимагає надати електронну пошту або ввійти через Facebook або Twitter, тобто користувач повинен надати певні персональні дані.

В деяких країнах державні уряди проводять онлайн-спостереження за користувачами мережі Інтернет. У Великобританії Investigatory Powers Act [4] дозволяє державним органам юридично шпигувати за переглядом та використанням Інтернету британськими громадянами. Таким чином, уряд може безпосередньо використовувати персональні дані, якщо вони підозрюють, що користувач можете бути причетним до злочинної діяльності.

Investigatory Powers Act змушує Інтернет компанії збирати персональні дані своїх клієнтів і тримати їх протягом дванадцяти місяців,

які згодом можуть бути вилучені урядовим органом і використані для боротьби із тероризмом або зупинки організованої злочинності. Це означає, що персональні дані, можуть бути використані та оброблені групою правоохоронних органів, навіть якщо користувач не має жодного відношення до розслідування.

Розвиток соціальних мереж становить глобальну проблему захисту персональних даних в мережі Інтернет. Соціальні мережі дозволяють користувачу завантажувати персональну інформацію на загальний огляд іншим користувачам, створювати мережу онлайн друзів та переглядати персональну інформацію різних користувачів. Багато осіб передають свої персональні дані до мереж задля спілкування в Інтернеті. Більшість користувачів викладають деталі свого особистого життя, в тому числі і фото на загальний огляд. Лідером у сфері соціальних мереж є Facebook. Він посідає друге місце за відвідуваністю у світі і є Інтернет-ресурсом світу, що поступається популярністю лише пошуковій системі Google. У грудні 2018 року кількість активних користувачів мережі Facebook нараховує більше 2,3 мільярди людей [2]. Більшість цих користувачів відвідують свою сторінку щоденно; у середньому проводять у мережах близько години.

Таким чином, соціальні мережі отримали змогу відстежувати дії користувачів та контролювати дані для майбутнього використання, тому становлять потенційну загрозу персональним даним [5, 167].

Дослідження 45-ти соціальних мереж, проведене організацією Physorg у 2009 р., виявило «значну тривогу» самих учасників, так і з боку захисту персональних даних. Близько 90 % сайтів, наприклад, для надання дозволу приєднатися до них необґрунтовано вимагають вказувати прізвище, ім'я або дату. 85 % веб-сайтів не можуть використовувати стандартні протоколи шифрування для захисту даних користувачів від атак кібер-злочинців. 72 % сайтів у своїй політиці залишають за собою право на передачу даних про користувачів стороннім особам [1].

Поширення персональних даних через соціальну мережу відбувається значно швидше, ніж у реальному житті. Шкідливими для користувача є ті випадки, коли персональні дані надходять до людей, яким це зовсім не призначено. Часто користувачам соціальних мереж не цілком відомо, що вони можуть змінити персональні параметри конфіденційності, і якщо цього не зроблять, то їхні персональні дані будуть відкриті іншим користувачам. На сьогодні, вже існує багато випадків негативних наслідків зайвої відвертості у соціаль-

них мережах, наслідком якої є: звільнення з роботи, розголошення інтимних подробиць життя, крадіжка фінансів та інше.

За даними дослідження Careerbuilder.com, 53% роботодавців використовують соціальну мережу для перегляду інформації про кандидата на роботу. «У наш час межа між особистим і професійним стирається», – стверджує англійський дослідник Луі Купер. Він вважає, що резюме перетвориться на певний гібрид файлів людини у мережах Facebook та Linkedin, відео й записи на Twitter, що мають відношення до майбутнього кандидата» [13, 35].

На думку американського вченого Д. Солова, у зв'язку із тим, що молодь ділиться інтимними подробицями свого життя у соціальних мережах відбувається стирання кордонів між приватним і публічним [6, 104]. Тобто він вважає, що соціальні мережі стають смертельно небезпечними для персональних даних.

Цей висновок підтверджений одним випадком, який трапився у США. Меган Меєр, дівчина із міста Сент-Луїс, покінчила життя самогубством відразу після того, як її 16-річний «хлопець» у спілкуванні у мережі MySpace, написав: «З тобою світ поганий». Проте, як виявилось, «16-річний хлопець» був насправді групою кількох осіб, які жили неподалік і створили фейковий профіль. Участь у цій діяльності взяла й Лорі Дру – мати однокласника Меган, яка була притягнута до кримінальної відповідальності за звинуваченням у порушенні Закону «Про комп'ютерне шахрайство і зловживання» за декількома статтями: створення фейкових профілів, відправка образливих повідомлень і вимагання даних від неповнолітніх [7].

Сьогодні важливо контролювати персональні дані, які завантажуються у соціальні мережі. Адже особа не може контролювати: хто і як використає ці дані. Персональні дані, які розміщені на сторінці користувача, можуть використати злочинці для так званого «викрадення особистості».

Варто виділити три основні групи ризиків у соціальних мережах при використання персональних даних: повна інформація про особу; повідомлення персональних даних злочинцям; відсутність у користувача реального контролю над персональними даними.

Існує ціла низка вторинної інформації, яку збирає та обробляє соціальна мережа без згоди користувача; та, яку використовують у маркетингових цілях або передають своїм партнерам. Також цю інформацію із соціальних мереж можуть збирати державні органи. Наприклад, державні органи Російської Федерації мають повне право збирати персональні дані користувачів із соціальних мереж, таких як: ВК та Одноклассники. Ці соціальні мережі функціонують для

прикриття, розвідувально-пошукової діяльності спецслужб щодо збору придатної для наступного аналітичного дослідження особистісної інформації. За оцінкою співробітників спецслужб, соціальна мережа Одноклассники є прикладом збору та обробки розвідувальної інформації, яка містить персональні дані. Величезна база даних, яка систематизована у різних містах, навчальних закладах, заводах, військових частинах із зазначенням дати служби, персональних даних громадян із фото, такими розділами, як: «мої друзі», «друзі друзів», «групи», відсутня навіть у спецпідрозділів. Вона є великим довідником для різних спецслужб [8, 185].

За даними британської газети «The Guardian», на замовлення військових США компанія Raytheon розробила систему під назвою RIOT. Система може отримувати персональні дані підозрюваних осіб із соціальних мереж. Дані отримуються із EXIF заголовків, фото, які були опубліковані у особистих альбомах на різних сайтах [10].

Збір інформації про користувача мережі Інтернет проводиться також через IP-адресу, з якої користувач заходив на пошту. За даними розслідування, співробітники Інституту Планка у Німеччині протягом 2008–2011 років стежили за кореспонденцією 43-х мільйонів користувачів поштової адреси Yahoo!

Відстеження персональної інформації користувача також можливе через кнопку «Like» у мережі Facebook. Такого висновку дійшли німецькі правозахисники у сфері захисту персональних даних. Оскільки, як наслідок викрадаються дані про користувача: інтереси, діяльність на тій чи іншій сторінці, здійснення переходу з одного сайту на інший надходить до США, де згодом, використовується для тартенгування реклами, аналізу поведінки користувачів на сайті тощо. Це підтвердили і представники мережі [14].

Система візуального розпізнавання, яка застосовується у мережі Facebook, може розпізнавати обличчя користувачів і відмічати друзів на фото. Аналогічна програма була розроблена для поліції США – вона швидше ідентифікує обличчя злочинця, адже порівнює із базою біометричних даних. База даних із обличчями людей може наштовхнути до зловживання з боку зацікавлених осіб. У низці європейських країн ця технологія була заборонена [12].

Отже, можна зробити висновок, що при використанні мережі Інтернет, користувачі наражають на небезпеку свої персональні дані. Ці загрози можуть призвести до різного ступеня серйозності наслідків.

Соціальні мережі та Інтернет є потенційною загрозою для багатьох користувачів, які наражають свої персональні дані на небезпеку. Незнання, як захистити себе та свої персональні дані, – є дуже важливим викликом сучасності для людини XXI століття. Тому тема особистої безпеки у мережі залишається дуже актуальною. Ці та інші теми досліджуватимемо у наступних наукових працях.

Джерела та література

1. Ganslandt M. Social network privacy standards. *Talkstandards*. 2010. URL: http://www.talkstandards.com/social-network-privacy-standards (дата звернення: 25.05.2019).

2. Gebel M. In 15 years Facebook has amassed 2.3 billion users – more than followers of Christianity. Business Insider. URL: http https://www.businessinsider.com/facebook-has-2-billion-plus-users-after-15-years-2019-2 (дата звернення: 25.05.2019).

3. Infobez-expo – международная выставка-конференция. URL: http://infobez-expo.ru/ (дата звернення: 25.05.2019).

4. Investigatory Powers Act 2016: веб-сайт. URL: http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted (дата звернення: 25.05.2019).

5. Lampe C. A face(book) in the crowd: social searching versus social browsing. *Proceedings of the 20-th anniversary conference on computer supported cooperative work*. Banff, Alberta, Canada, 2007. P. 167–170.

6. Solove D. J. Do social networks bring the end of privacy? *Scientific American*. 2008. Vol. 299. P. 100–106.

7. Who's the bully? *Los Angeles Times*. 2008. 19 may.

8. Березовська І. Протиправне використання персональних даних, що містяться у соціальних мережах як загроза інформаційній та національній безпеці України. *Вісник Львівського університету. Серія юридична.* 2014. Вип. 60. С. 185.

9. Брижко В. М. Захист персональних даних: реалії та практика сучасності. *Інформація і право*. 2013. № 3 (9). С. 31.

10. Владу США звинуватили у шпигунстві за громадянами за допомогою соціальних мереж. URL: http://svit24.net/technology/67-vladusshazvynuvatyly-u-shpygunstvi-za-gromadjanamy-za-dopomogoju-socialnyh-merezh (дата звернення: 25.05.2019).

11. Интернет-паноптикум Facebook URL: http:// www.sostav.ua/news/2012/10/02/127/52214 (дата звернення: 25.05.2019).

12. Лицевая идентификация может помогать преступникам. URL: http://www.infox.ru/hi-tech/tech/2011/08/02/Licyevaya_idyentifik_print.phtml (дата звернення: 25.05.2019)

13. Мечетная Н. Общая раздевалка. *Корреспондент.* 10.09.2010. С. 35.

14. Німецькі поборники приватності угледіли загрозу в соціальній мережі Facebook, а точніше в улюбленій користувачами кнопці like. URL: http://briz.if.ua/9590.htm (дата звернення: 25.05.2019).