ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

УДК354.42/44:343.9

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

Деякі аспекти незаконного збору персональних даних користувачів мережі Інтернет

У статті досліджуються питання, пов'язані з незаконним збором персональних даних і відслідковуванням користувачів мережі Інтернет, зокрема, соціальних мереж.

Ключові слова: мережа Інтернет, соціальні мережі, персональні дані, засоби збору інформації, спецслужби.

Прогрес науки і техніки, який впливає на процеси інформатизації, має як позитивні, так і негативні наслідки. З одного боку, людина отримує доступ до нових можливостей, з іншого – стикається з усе більш різноманітними ризиками, які несуть загрозу її безпеці, свободам, приватному життю. Одним із принципів інформаційного суспільства є прозорість суспільства. І, реалізовуючи його, "прозорою" в інформаційному відношенні стає і сама людина. Так, останнім часом у глобальних інформаційно-телекомунікаційних мережах усе більшого поширення набуває новий вид протиправної деструктивної діяльності – відслідковування осіб, збирання та аналіз персональних даних користувачів. Відбувається розголошення та протиправне використання конфіденційної інформації щодо сфери приватного життя особи, порушуються особисті конституційні права людей.

Найбільш суспільно небезпечною складовою є те, що, фактично, відслідковування, викрадення, збирання та аналіз персональних даних користувачів, їх зв'язки, психологічні та інші особливості можуть створювати передумови до цілеспрямованого зовнішнього чи внутрішнього інформаційного впливу, а також той факт, що 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.

Слід зазначити, що парадокс полягає в тому, що значна кількість користувачів надзвичайно відверті в онлайні, що робить збір інформації про них для професіоналів доволі нескладним. До того ж надмірна централізація персональних даних спрощує їх отримання.

До того ж особливе занепокоєння викликає те, що європейці та американці усвідомили ризики, пов'язані зі збором і збереженням інформації про своїх громадян, а українці в цьому сенсі більш безтурботні. В Україні на сьогодні переважають користувачі, які, навпаки, готові реєструватися в різних соціальних мережах, і залишати свої особисті, часом конфіденційні, дані абсолютно доступними, не контролюють своє електронне листування тощо.

Варто зауважити, що початок XXI століття охарактеризувався появою нового виду воєн – інформаційно-мережевих, за яких перемога досягається не за рахунок знищення збройних сил і економіки противника, а за допомогою впливу на його морально-психічний стан. Метою інформаційно-мережевої війни є закріплення більшої частини стратегічно важливих ресурсів країни за геополітичним агресором. При цьому "передача" цих ресурсів агресору здійснюється елітою країни-жертви в значній мірі добровільно, оскільки сприймається нею не як захоплення, а як шлях до розвитку. Це породжує складність у розпізнаванні технології та методів інформаційно-мережевої війни порівняно з традиційною, а також відсутність своєчасної реакції на дії агресора, так як жертвою не чиниться жодних заходів протидії їм [1].

Тому сьогодні спецслужби різних країн досить активно і масштабно проводять різного роду спецоперації щодо відслідковування, особливо з використанням мережі Інтернет, громадян, у першу чергу, осіб, які займають ключові місця в державі.

Останнім часом усе частіше почала з'являтися інформація про виявлення і розсекречення глобальних і добре спланованих операцій по "кібершпигунству". Низку таких операцій було викрито вже в цьому році. Так, на початку року фахівці "Лабораторії Касперського" виявили вірус, якому дали назву Red October (Красний Октябрь). За допомогою цієї програми, починаючи з 2007 року, викрадалася інформація з урядових, дипломатичних, військових, наукових установ, організацій, а також окремих об'єктів критичної інфраструктури на території СНД, Європи, США і Марокко. Викрадалися як особисті дані, так і службові, особливо конфіденційні. Для зараження систем використовувалися фішінгові листи, які адресувалися конкретним отримувачам, відповідно до їхніх індивідуальних особливостей, тобто попередньо вивчивши інформацію про потенційну жертву. Наразі розробники вірусу залишаються невідомими [2].

Крім того, у лютому п. р. було виявлено ще дві кібершпигунські мережі. Одну з них – MiniDuke – було виявлено спільними зусиллями "Лабораторії Касперського" та угорською компанією CrySys Lab (Лабораторія криптографії і системної безпеки). Серед жертв цього вірусу виявилося 59 державних установ із 23 країн світу, в тому числі й України. Вірус має надзвичайно малий розмір бекдора (20 Кб). Він проникав на комп'ютери користувачів через прогалини в додатках Adobe Reader з використанням PDF-файлів, які, до речі, досить ретельно підбиралися і були надзвичайно актуальними для потенційних жертв. Так, у них містилася інформація, що стосується семінарів про права людини (ASEM), дані про зовнішню політику України, плани держав-учасниць НАТО. Після проникнення програма зв'язувалася зі своїми розробниками через сервіс мікроблогів Twitter (а в разі, коли Twitter не працює чи відповідні облікові записи відключено, пошук командного сервера відбувається з використанням пошуковика Google) і завантажувала в декілька етапів основну частину вірусу, який відкривав зловмисникам доступ до даних, що містилися в комп'ютері жертви [3].

Наступну серію атак було організовано групою китайських хакерів. Про них стало відомо зі звіту американської компанії Mandiant "APT1 : Exposing One of China's Cyber Espionage Units". За даними експертів, APT1 має відношення до відділу 61398 2-го Бюро Третього Департаменту Генерального штабу Народно-визвольної армії Китаю. Вони, починаючи з 2006 року, займалися економічною розвідкою і викрали інформацію у 141 компанії та організації [4].

Наприкінці березня п. р. угорська компанія CrySys Lab спільно з Управлінням національної безпеки Угорщини опублікувала інформацію про викриту ними довготривалу (понад 10 років) кібероперацію, якій присвоїли назву TeamSpy. Її мета – викрадення паролів, ключів шифрування, документів, які містять таємні відомості, даних про натиснуті клавіші, копій екранів тощо з комп'ютерів політичних діячів і правозахисників високого рівня на всій території СНД і східноєвропейських країн.

За допомогою серії атак комп'ютери жертв заражали за принципом "водопій в засуху", коли віруси розміщували на веб-сайтах, які найчастіше відвідували потенційні потерпілі, тобто інтереси потерпілих попередньо ретельно вивчалися [5].

На початку червня "Лабораторія Касперського" розкрила нову мережу кібершпіонажу NetTraveler, в рамках якої цільовим атакам піддалися більше 350 комп'ютерних систем у 40 країнах світу. До числа потерпілих увійшли державні організації, посольства, компанії з нафтовидобувної та газової галузей, дослідницькі центри, військові структури та громадські активісти [6].

Зазвичай, потужні, довготривалі розвідувальні операції щодо збору інформації та відслідковування користувачів проводилися за підтримки розвинених країн.

Американська газета The Guardian повідомила про те, що державні органи США мають можливість стежити за повідомленнями електронної пошти, перевіряти соціальні мережі й чати в 150 країнах світу. І все це без відповідних на це судових санкцій. Об'єм інформації, що збирається, величезний. Дані про паролі користувачів можуть зберігатися на серверах агентства три дні, зміст Інтернет-листування – місяць [7].

Підтвердженням того, що інформація про громадян незаконно збирається з використанням державних програм стало повідомлення одного з колишніх програмістів компанії Booz Allen Hamilton (є підрядником Агентства Національної Безпеки США, АНБ) Едварда Сноудена. За його словами, існуюча в США державна програма PRISM не тільки дозволяє владі збирати інформацію про користувачів дев'яти великих Інтернет-компаній і соціальних мереж (Microsoft, Yahoo, Google, Facebook, Paltalk, YouTube, AOL, Skype, Apple), але й відкриває прямий доступ до комп'ютерних систем цих організацій, що є порушенням права на приватне життя з боку американського уряду.

До речі, про збір персональних даних рядових користувачів Агентством національної безпеки США шляхом збору електронної пошти, листування користувачів у мікроблозі Twitter, пошукових запитів, які потім використовувалися для створення баз даних і пошуку в них, повідомлялося і раніше. Так, наприклад, у минулому році про

несанкціонований збір даних говорив колишній співробітник АНБ США Уільям Бінні [8].

Відповідно до нещодавно опублікованого газетою The Washington Post повідомлення, Агентство національної безпеки США за останні п'ять років багаторазово порушувало свої повноваження у сфері збору інформації. Так, тільки в період з травня 2011 р. по травень 2012 р. було зафіксовано 2776 порушень. Більшість цих порушень стосувалася незаконного спостереження за громадянами США та іноземними спецслужбами, причому ці порушення відбувалися як свідомо, так і в результаті випадкових помилок.

АНБ було опубліковано документ, в якому зазначалося, що агентство аналізує тільки 0,00004 % від усього обсягу даних, що передаються в мережі Інтернет. Так, згідно з документом, АНБ "стосується" тільки 1,6 % із 1826 петабайт даних, що передаються в мережі Інтернет щодня, причому тільки 0,025 % цих даних відбирається для аналізу [9].

Екс-співробітник спецслужб Сноуден заявив, що АНБ було створено інфраструктуру, яка дозволяє перехоплювати практично все – електронну пошту, паролі, дані про телефонні розмови, кредитні картки, а електронне відслідковування урядом США громадян країни за масштабами перевищує аналогічні операції по відношенню до Росії.

Правозахисні організації і значна частина громадян США вбачають у цьому порушення громадянських прав і недоторканості приватного життя. Про це говориться в Біллі про права і Четвертій поправці до Конституції США, які гарантують народу право на недоторканість особи, помешкання, особистих паперів і майна від необґрунтованих обшуків і арештів.

У свою чергу, директор Національної Розвідки США Джеймс Клеппер піддав різкій критиці витік секретної інформації. Він заявив, що стеження ведеться тільки з санкції суду, відстежується невелика частина комунікацій, і роблять це тільки фахівці з боротьби з тероризмом, а уряд не бере участі "у програмах одностороннього збору інформації" та не проводить "безрозбірного збору даних" у комп'ютерних компаній. На його переконання, "PRISM – це не секретна програма для пошуку і збору інформації. Це внутрішньоурядова система, призначена для задоволення інформаційних потреб у рамках вже розпочатих розслідувань, що проводяться під наглядом суду. За законністю збору даних завжди стежили всі три гілки влади" [10].

Президент США Барак Обама також виступив на захист цієї програми, заявивши, що вона являє собою незначне втручання в приватне життя, яке необхідне для захисту громадян від нападів терористів. На думку Президента США, неможливо отримати 100 % безпеку, зберігаючи 100 % приватність – це миттєво спровокує активність з боку терорис-

тів і злочинців. Завдання держави полягає в тому, щоб забезпечити прийнятний баланс між приватністю і безпекою громадян.

У свою чергу, компанії Apple, Google і Facebook спростовують інформацію про те, що уряд мав доступ до їхніх серверів. Так, головний юридичний консультант пошукового гіганта Девід Драммонд (David Drummond) заявив, що у влади немає і не було "ні прямого, ні інженерного" доступу до внутрішніх комп'ютерних мереж Google, а запити про користувачів надаються індивідуально і нерідко отримують відмову.

Голова сенатського комітету з розвідки Дайен Файнстайн заявила, що робота програми здійснюється на законних підставах. Вона підкреслила, що таким чином вдалося розкрити щонайменше дві терористичні змови, в тому числі підготовку вибухів у нью-йоркському метро в 2009 році [11].

Відносно цього скандалу влада США неодноразово підкреслювала, що в рамках проекту проводилося "акуратне" стеження, коли стеження за громадянами США було виключено повністю або проводилося в значно меншій мірі. І це насправді так, оскільки Конституція США захищає права громадян тільки своєї країни. По суті, громадяни інших країн у рамках американської глобальної системи стеження не мають жодних прав на недоторканність приватного життя [11].

Тому уряди багатьох країн світу, правозахисні організації та окремі відомі діячі висловили занепокоєння ситуацією і назвали PRISM програмою, що посягає на приватне життя громадян. Так, Європейська комісія стурбована наслідками відслідковування особистого життя громадян ЄС. Співробітниця прес-служби Єврокомісії М. Андрєєва відмітила, що питання національної безпеки входять до компетенції держав-членів ЄС. Ситуація, що виникла, не передбачена союзним регламентом про захист даних. Але коли зачіпаються права громадян держав-членів Європейського Союзу, національна юстиція вирішує, чи відповідає національному, європейському або міжнародному законодавству такий збір даних [12].

Гучний скандал викликало відслідковування громадян через мережу Інтернет у Великобританії, де представники спецслужб на вимогу палати общин повинні підготувати доповідь і, тим самим, відповісти на запитання, на якій підставі Управління урядового зв'язку збирало інформацію на британців через американську програму відслідковування. Попередньо міністр МВС Уільям Хоуг в інтерв'ю сказав, що законослухняним британцям боятися не потрібно. Відслідковування, якщо й ведеться, то лише за порушниками законів і тільки в рамках закону та права громадян на недоторканість приватного життя британський уряд не порушує. Тобто, міністр власне не підтвердив і не спростував інфо-

рмацію щодо її надання Агентством національної безпеки США і ФБР британським спецслужбам [13].

До речі, Британські спецслужби також активно займаються відслідковуванням громадян. Так, наприклад, Сноуденом було викрито секретну базу на Близькому Сході, яку створили Британські спецслужби. З неї здійснювалося перехоплення електронної переписки, Інтернет-трафіку та інформації про телефонні дзвінки регіону. Інформацію отримували завдяки підключенню до оптоволоконних кабелів. Зібрані дані про Інтернет-користувачів Близького Сходу направляються в Центр урядового зв'язку Великобританії, який потім ділиться інформацією з Агентством національної безпеки США [14].

Стурбована масштабами відслідковування і влада Індії. Прессекретар МЗС Саід Акбаруддін заявив, якщо факт порушення індійських законів щодо недоторканості інформації про приватне життя підтвердиться, для індійського уряду, без сумніву, це буде неприпустимим. До речі, за даними британської газети Guardian, Індія займає п'яте місце, після Ірану, Пакистану, Йорданії та Єгипту, за кількістю зібраних Агентством національної безпеки США "одиниць розвідінформації" – 6,3 млрд [15].

Естонське Інтернет-співтовариство (Eesti Intemeti Kogukond) підозрює, що спецслужби США збирали інформацію про жителів Естонії і передавали її естонським спецслужбам, що, в свою чергу, є порушенням конституційних прав громадян Естонії, де для таємного збирання інформації про приватне життя потрібен дозвіл суду [16].

Варто наголосити, що одним із ключових чинників досягнення перемоги у військовому конфлікті майбутнього стане правильний розподіл пріоритетів впливу на цілі та об'єкти противника. Систему таких пріоритетів було розроблено полковником ВПС США Дж. Уорденом майже два десятки років тому. Основні зусилля у військовому конфлікті повинні бути спрямовані на знищення політичних лідерів країни противника, причому в цьому контексті під знищенням необов'язково розуміється фізична ліквідація, а й акції за ідейною, політичною та моральною дискредитацією [17].

Отже, необхідно зазначити, що, фактично, ми можемо вести мову саме про системне використання іноземними організаціями та спецслужбами мережі Інтернет, 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 мережі Інтернет персональних даних користувачів. Це, в свою чергу, зумовлює об'єктивну необхідність негайного вироб-

лення на державному рівні принципово нових підходів до забезпечення захисту інтересів особи, суспільства та держави у цій сфері.

Список використаних джерел

1. Когда нация становится жертвой: Концептуальные основы информационно-сетевых войн / [Электронный ресурс]. – Режим доступа : http://flot2017.com/posts/new/kogda_nacija_stanovitsja_zhertvoj__koncept ualnye_osnovy_informacionnosetevyh_vojn.

2. “Лаборатория Касперского” взломала шпионскую сеть “Красный Октябрь” миру / [Электронный ресурс]. – Режим доступа : http://russian.rt.com/article/3020.

3. MiniDuke – новая вредоносная программа для кибершпионажа в государственных структурах по всему миру / [Электронный ресурс]. – Режим доступа : http://www.kaspersky.ru/news?id=207733960.

4. APT1: разоблачение китайской организации, занимавшейся промышленным кибершпионажем / [Электронный ресурс]. – Режим доступа : http://habrahabr.ru/company/eset/blog/170285/.

5. Атаки TeamSpy Crew – незаконное использование TeamViewer в целях кибершпионажа / [Электронный ресурс]. – Режим доступа : http://www.securelist.com/ru/blog/207764533/Ataki_TeamSpy_Crew_nezak onnoe_ispolzovanie_TeamViewer_v_tselyakh_kibershpionazha.

6. Во втором квартале число мобильных зловредов еще больше возросло [Электронный ресурс] // InternetUA. – 2013. – 17 авг. – Режим доступа : http://internetua.com/vo-vtorom-kvartale-csislo-mobilnih-zlovredov-esxe-bolshe-vozroslo.

7. Купченко А. Слежка за пользователями сети: Украина набирает обороты [Электронный ресурс] // InternetUA. – 2013. – 22 авг.– Режим доступа : http://internetua.com/slejka-za-polzovatelyami-seti–ukraina-nabiraet-oboroti).

8. Уильям Бинни АНБ США собирает конфиденциальные данные граждан [Электронный ресурс] / Уильям Бинни. – Режим доступа : http://www.securitylab.ru/news/427859.php.

9. АНБ уличили в незаконной слежке за американцами [Электронный ресурс] // Левый берег. – 2013. – 16 авг. – Режим доступа : http://world.lb.ua/news/2013/08/16/220182_anb_ulichili_nezakonnoy_slezh ke.html.

10. Раскрыт факт существования американской программы PRISM – инструмента слежения за пользователями Сети / [Электронный ресурс]. – Режим доступа : http://www.securitylab.ru/news/441387.php.

11. Американский сенатор предложил изменить закон, позволяющий спецслужбам собирать данные о телефонных разговорах и интернет-трафике / [Электронный ресурс]. – Режим доступа : http://pd.rsoc.ru/press-service/subject1/news2216/?print=1.

12. ЕС спросит США за слежение в Интернете / [Электронный ресурс]. – Режим доступа : http://podrobnosti.ua./power/2013/06/10/910220.html.

13. Британский парламент возмущен слежкой за гражданами / [Электронный ресурс]. – Режим доступа :
http://radiovesti.ru/article/show/article_id/94972.
14. Сноуден рассекретил британскую базу интернет-слежки на Ближнем Востоке [Электронный ресурс] // InternetUA. – 2013. – 23 авг.– Режим доступа :
http://internetua.com/snouden-rassekretil-britanskuua-bazu-internet-slejki-na-blijnem-vostoke.
15. Индия обеспокоена масштабами электронной слежки США за ее гражданами / [Электронный ресурс]. – Режим доступа :
http://ria.ru/world/20130611/942824764. html.
16. Эстонское интернет-сообщество подозревает спецслужбы в нарушении прав граждан Эстонии / [Электронный ресурс]. – Режим доступа :
http://rus.err.ee/estonia/64f0d98b-6eb2-481c-b3f9-819522609ae7.
17. Попов И. Технологическая революция в "традиционной" войне [Электронный ресурс] / Игорь Попов. – Режим доступа :
http://nvo.ng.ru/concepts/2013-04-12/1_conflicts. html.

Статья посвящена исследованию вопросов, связанных с незаконным сбором персональных данных и отслеживанием пользователей сети Интернет, в частности, социальных сетей.

The article is devoted to the research of questions concerning the illegal data collection and tracing of the Internet users, in particular, of the social networks.

Стаття надійшла до редакції журналу 25 вересня 2013 року.