д.п.н., професор, професор кафедри
суспільно-політичних наук
Вінницького національного
технічного університету
Денисюк С. Г.

ПРОБЛЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ГРОМАДЯН В СУЧАСНИХ УМОВАХ

Розвиток сучасних методів і технологій передачі інформації вражає своїми масштабами і можливостями. Зокрема, мережа Інтернет сьогодні активно використовується як державними і недержавними організаціями та установами, так і окремими особами, зокрема, для повсякденної комунікації, надання послуг, обробки певної інформації, реалізації електронного урядування тощо.

Проте нині через активізацію терористичних загроз, сепаратистських настроїв, воєнних конфліктів, збільшення рівня злочинності як в Україні, так і у світі, спостерігається підвищення контролю з боку влади над громадянами, їх комунікацією. Часто об'єктивне існування таких загроз використовується не тільки для захисту держави, але й виступає приводом для слідкування за громадянами, збору приватної інформації про них.

Наприклад, в Україні введені іменні залізничні квитки, громадяни надають свої паспортні дані, ідентифікаційні коди у різні державні інституції, які контролюють буквально кожний крок людини. 6 грудня 2012 р. набрав чинності Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус». Відповідно до цього Закону в Україні розпочато роботи із запровадження оформлення і видачі паспорта громадянина України, що містить безконтактний електронний носій із біометричними даними власника документу. Але чи надаються чіткі гарантії збереження особистих даних, і чи визначено відповідальність за просочування інформації? Мабуть, що ні.

Спроби тотального контролю здійснюється не лише в Україні та інших пострадянських державах. Зокрема, відомими є відкриття Wikileaks та їх партнерами таємної інформації, яка стосувалась діяльності органів державної

влади. Так, Е. Сноуден розкрив правду про збирання персональної інформації органами національної безпеки США. Стало очевидним, що, починаючи з 2007 року США спостерігали за кожним користувачем Інтернету, який використовував сервіси розташовані в Сполучених штатах [1]. Такий спосіб і мета використання Інтернету є пріоритетними для влади. За приблизними підрахунками на такі дії уряд США витрачає мільярди доларів [2].

Цікаво, що спецслужби збирають дані про дзвінки, електронне листування, передані файли, інформацію із соціальних мереж, дані про місце розташування користувача, IP адресу тощо [2].

Головними способами одержання інформації органами влади є: перехоплення інформації з волоконно-оптичних кабелів; офіційні звернення до сайтів з метою отримання доступу до персональних даних користувачів; прямий доступ до центральних серверів; використання третіх сторін для отримання доступу [3].

За даними ЗМІ влада США та її союзники співпрацюють з такими інтернет-компаніями: Microsoft, Yahoo, Google, Facebook, AOL, PalTalk, Skype, Apple, YouTube [4]. Стосовно інтернет-компаній, які найбільш популярні серед українських користувачів, то такими є Facebook, Google, Vkontakte. Проаналізувавши політику їх конфіденційності, можна зробити висновок, що існує надмірне збирання інформації державними структурами. Досить важко зрозуміти, чому Facebook збирає і розкриває органам влади такий великий обсяг даних, які прямо не допомагають розслідуванням, таких як налаштування оголошень, політичні уподобання, сімейний стан, відвідані сторінки користувачів тощо [5].

Контроль над громадянами та їх діяльністю не обмежується лише Інтернетом. Наприклад, у США всюди встановлюються автоматичні сканери номерних знаків автомобілів. Їх розташовують на патрульних автомобілях, іноді на стаціонарнах об’єктах (мостах або дорожніх знаках). Такі автоматичні сканери щодня збирають неймовірну кількість інформації про маршрути мільйонів звичайних американців.

За даними CNN, сканери райдужної оболонки ока вже впроваджуються в школи по всій країні, і незабаром їх будуть використовувати в банках,

аеропортах і банкоматах. Промислові інсайдери стверджують, що у 2016 р. ця технологія буде застосовуватися абсолютно скрізь. А це означає, щоб отримати доступ до банкомата, не потрібно людині вводити ПІН-код, все, що буде потрібно – це просто подивитися. Використовувана в аеропорту система буде аналізувати райдужну оболонку ока, поки людина проходить контроль, ідентифікуючи і вітаючи її по імені.

Як може громадянин подбати про своє приватне життя, про те, щоб інформація про нього не була використана з метою маніпуляції чи зловживання з боку влади?

Звичайно, це зробити важко. Проте одним із шляхів розв'язання проблеми перевищування повноважень з боку влади є прозорість її дій і контроль з боку суспільства. Важливим є те, що громадяни повинні бути не лише об'єктом, але й суб'єктом інформаційного контролю.

Відомо, що тотальне слідкування за людьми не унеможливлює діяльності злочинців, адже останні використовують різні інтернет-ресурси і кодують таємну інформацію. Нині інтернет-злочинність є бізнесом, який швидко розвивається, і приносить мільярдні прибутки.

Однак отримання інформації владою про громадян іноді сприяє безпеці суспільства і держави, викриттю злочинців, сепаратистів, терористів. Однак важливо визначити чіткі межі та цілі у процесі отримання інформації про громадян аби не перевищувати повноваження. Нині спостерігається певний зсув у бік збільшення контролю над громадянами, що не сприяє демократичному розвитку будь-якого суспільства. Сучасні технології відкривають нові можливості для можновладців слідкувати за людьми, і, враховуючи економічну і політичну ситуацію в Україні, рівень культури політиків, недосконалу нормативно-правову базу, використовувати інформацію для власного збагачення і утвердження влади.

Список використаної літератури

1. Glance D. The death of privacy through the PRISM of the US Government [Електронний ресурс] / D. Glance // Business Spectator. – Режим

доступу : http://www.businessspectator.com.au/article/2013/6/10/technology/death-privacy-through-prism-us-government.

2. NSA slides explain the PRISM data-collection program [Електронний ресурс] // The Washington Post. – Режим доступу : https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

3. «Великий брат» стежить за тобою [Електронний ресурс] // Euronews. – Режим доступу : http://ua.euronews.com/2013/06/07/us-intelligence-chief-responds-to-internet-tapping-claims.

4. Gellman B. British intelligence mining data from nine U.S. Internet companies in broad secret program [Електронний ресурс] / B. Gellman, L. U. S. Poitras// The Washington Post. – Режим доступу : https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

5. Facebook’s Data Pool [Електронний ресурс] // Europe-v-facebook.org. – Режимдоступу :http://europe-v-facebook.org/EN/Data_Pool/data_pool.html.