

ПРОБЛЕМА ЗАБЕЗПЕЧЕННЯ ПРИВАТНОСТІ ТА КОНФІДЕНЦІЙНОСТІ ДАНИХ КОРИСТУВАЧІВ В СУЧАСНИХ ІНТЕРНЕТ СЕРВІСАХ

Царіков М. С., ст. (гр. КП-81мп, ФПМ КПІ ім. Ігоря Сікорського)

Анотація: Проблема забезпечення приватності та конфіденційності користувацьких даних є актуальною проблемою при створенні та підтримці інформаційних систем. Тези присвячені розгляду проблеми відстеження дій користувачів регулюючими органами влади.

Ключові слова: база даних, інформаційна безпека, захист даних, приватність даних, конфіденційність даних.

Abstract: Problem of privacy and confidentiality of user data remain an unsolved problem, that takes part during the process of creating and supporting the information system. The paper is devoted to the problem of monitoring the user's activity by government.

Keywords: database, information security, vulnerability, data protection, data privacy, data confidentiality.

Приватність в мережі Інтернет – це право на зберігання, передачу іншим особам та підприємствам та відображення інформації деяким сторонам через мережу Інтернет. Проблеми приватності та конфіденційності даних в обраній тематиці були сформульовані ще в час зародження та популяризації обміну даних за допомогою комп'ютерів.

Приватність даних може стосуватись інформації, що ідентифікує персону, або не ідентифікує, як приклад: поведінка відвідувача веб-сайту. Приватною інформацією може бути будь-яка інформація, за якою можна ідентифікувати персону (наприклад фізична адреса та вік є достатніми критеріями для того, аби ідентифікувати людину, оскільки обидва фактори є достатньо точними для визначення конкретної особистості [1].

Експерти з дослідження справ конфіденційності в мережі Інтернет вважають, що конфіденційності більше не існує, оскільки більшість онлайн-сервісів під час своєї роботи звертаються до приватної інформації користувачів.

Однак відстеження дій користувачів в Інтернет має об'єктивно позитивний вплив. Так, експерт з питань безпеки в мережі Інтернет Брюс Шнаєр, висловив популярну серед його колег думку: «Відстеження конфіденційних даних захищає нас від зловживань влади, навіть якщо ми не робимо нічого поганого».

Спроби уникнути збору приватної інформації користувачів, та уникнути впливу влади та органів кримінальних та адміністративних справ спричинили розширення Інтернет. Наразі за допомогою загальнодоступних пошукових системам можна відвідати лише близько 20 % сайтів та веб-сервісів в мережі Інтернет, оскільки видимий Інтернет – це лише 20 % від всіх веб-джерел.

Решта – DeepWeb, DarkNet містять інформацію, що часто заборонена для розголошення (продаж наркотиків, зброї, послуги сфери проституції,

праворадикальні нацистські форуми і т.п.). Відвідування таких джерел, навіть у виключно дослідницьких намірах, може притягнути користувача до відповідальності перед законом [2].

Саме тому Інтернет конфіденційність розглядається окремо від конфіденційності інших даних людей.

Користувачі в Інтернет не повинні досягати повної анонімності. Вони можуть захищати свою інформацію використовуючи механізми контролюючі розкриття особистості (IP адреси стало таким компромісом).

З іншого боку, деякі користувачі хочуть більш високого ступеня конфіденційності. У цьому випадку вони можуть спробувати домогтися повної анонімності в Інтернеті для забезпечення конфіденційності – використовувати Інтернет, котрі дають третім особам можливість зв'язати дії в Інтернеті з особистими даними користувача Інтернету. Варто пам'ятати, що коли ви заповнюєте форми для реєстрації або купуєте товар, це відстежується, і оскільки інформація не є приватною, деякі компанії відправляють Інтернет-користувачам рекламу про аналогічні продукти.

Розміщення чогось в Інтернеті може бути шкідливим або навіть небезпечним (можливість для зловмисної атаки). Деяка інформація, яка потрапляє в Інтернет, залишається там назавжди, в залежності від умов обслуговування і політик конфіденційності певних послуг, пропонованих в Інтернеті. Деякі роботодавці можуть досліджувати потенційного співробітника шляхом пошуку в Інтернеті подробиць його поведінки, що може вплинути на успіх кандидата. Як приклад, в Китаї за участю «Alibaba Group» була створена система соціального рейтингу, яка масово аналізує дані про людей зібрані в мережі Інтернет та інших джерелах, оцінювала людей за різними параметрами. Наразі дана система введена в низці підприємств, проте планується її глобальне розширення. Вона була неодноразово розкритикована через свою схожість з поширенням диктатури в країні.

Існують цілі компанії, що спеціалізуються на зборі інформації про відвідувачів Інтернет-сайтів, відправляючи рекламу на основі зібраних даних. Є багато способів надати особисту інформацію про себе, наприклад, через соцмережі або відправляючи інформацію про банк та кредитну картку на різні веб-сайти.

Більш того, відслідковується і безпосередньо поведінка користувача через історію перегляду, пошукові запити і активність в соцмережах. Все більше і більше Інтернет засобів використовують механізми аналізу кліків користувачів та часу, за який ці кліки були здійснені для покращення свого інтерфейсу, що забезпечує збір даних про користувачів навіть якщо ті нічого не публікують, і не відправляють жодних повідомлень (як приклад комерційні сервіси, які продають програмне забезпечення, що є надбудовою на Інтернет за стосунком, та створюють мапи кліків користувачів). Все це допомагає зібрати найбільш небажані деталі про особу, такі як: сексуальна орієнтація, політичні та релігійні погляди, раса, пристрасть до наркотиків і рівень інтелекту. Але навіть і без цього існують способи відстежувати взаємодію користувача з сайтом,

отримуючи інформацію про поштовому індексі, ім'я та адресу місцезнаходження. Перелічені вище факти автоматично створюють проблему того, що при повній відмові від приватності та конфіденційності даних користувачів є ризик того, що значно збільшиться коло людей, які володітимуть даними про користувача, якими володіти не повинні з точки зору моралі, етики та цілей використання за стосунків, з яких була зібрана інформація. Це зумовлює порушення свободи людини.

Водночас зберігання всієї інформації, і не надання доступу до неї жодним правоохоронним органам провокує та захищає користувачів, які порушують закон. Як доказ, відмова компанії «Apple» на початку 2016 року співпрацювати з Федеральним Бюро Розслідувань: спецслужби не отримали підтримки від «Apple» у справі розшуку вбивці Саїда Фарука, оскільки вимагали надати дані з телефону розшукуваного, що суперечило принципу забезпечення приватності та конфіденційності даних користувачів. Дана ситуація описує пошук зловмисника вже після вчиненого злочину. Проте аналіз користувацької інформації міг би не дати здійснитися злочинам. Як приклад: масове вбивство в школі «Колумбайн» 20 квітня 1999 року штат Колорадо, США, в результаті якого загинуло 13 людей. Двоє підлітків протягом року у своїх блогах публікували відео, в якому погрожували «розправитися» з усіма людьми, що завдавали їм клопоти. Після того, як дана трагедія сталася, правоохоронні органи передивилися їх блог, який став предметом дослідження для багатьох психіатрів. Варто також зазначити, що хоч зняті відео були публічно доступні, в 1999 році мережа Інтернет лише починала активно розвиватися, та не була предметом масового вжитку, як сьогодні. Проте з історії листувань підлітків (яке було приватним) можливо було зрозуміти, що планується вбивство, і можна було б вжити заходів, щоб запобігти злочину.

Висновок. Питання забезпечення приватності та конфіденційності даних користувачів в сучасних інтернет сервісах є актуальним. Забезпечення цілковитої приватності даних людей може призвести до негативних наслідків, у разі якщо йдеться про дані людей, що порушують законодавство. Водночас відмова від приватності та конфіденційності порушує права та свободи людини. Дана проблема перетинається з проблемами моралі та етики, а також проблемами устрою суспільства й вимагає компромісного вирішення.

Науковий керівник: Землянська О. В., ст. викл. (каф. ОППЦБ КПІ ім. Ігоря Сікорського)

Література

1. Matthew Bailey. Complete Guide to Internet Privacy, Anonymity & Security // Nerel — 2011 — ISBN 395030930.
2. Miyazaki, A. D. (2001). «Consumer Perceptions of Privacy and Security Risks for Online Shopping». Journal of Consumer Affairs 35 (1): 38–39.