Секція 1

АНАЛІЗ МЕТОДІВ ЗМЕНШЕННЯ ЦИФРОВИХ СЛІДІВ ДЛЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧІВ

Малєєва З.-Т.О.
Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ»
Науковий керівник Пєвнєв В.Я.

Актуальність. Згідно зі щорічним звітом про витік даних за 2021 рік, опублікованим ITRC, загальна кількість скомпрометованих даних зросла більш ніж на 68% порівняно з 2020 роком [1]. Одним із аспектів захисту від крадіжки цифрових даних є розуміння концепції цифрових слідів. Цей автоматичний слід реєструє звички, інтереси, події, спілкування в мережі Інтернет, і саме через цю інформацію можна провести паралель між віртуальним аватаром та реальною особою. Особисті дані про користувачів, які доступні в мережі Інтернет також містяться в таких джерелах, як: судові та майнові записи, реєстрації гарантій, сайти соціальних мереж і дані перепису населення. Отже, погано керований цифровий слід може розкрити конфіденційну інформацію особи.

Мета роботи полягає у аналізі методів зменшення цифрових слідів для захисту даних користувачів.

Основні положення. Серед багатьох визначень цифрового сліду найбільш влучним є, що це інформація про конкретну особу, яка існує в мережі Інтернет в результаті її онлайн активності, а саме: листування через сервіси електронної пошти, покупка в Інтернеті, поширення контенту (фото, відео, дописи, коментарі), відвідування веб-сайтів [2].

Дані про користувачів залишені в мережі Інтернет зберігаються у величезній кількості місць, тому зовсім видалити свій цифровий слід не вдасться. Але необхідно обережно поширювати інформацію про особу в мережі, бо[2]: поширення опублікованої інформації в мережі Інтернет неможливо повністю контролювати; цифрові сліди складно зробити знеособленими, за ними можливо виявити соціальні зв’язки, звички людей, знайти особисті дані.

Існують два основні типи цифрових слідів: пасивні та активні. Активний цифровий слід з'являється, коли користувач передає свої персональні дані самостійно, наприклад, майже для кожного створюваного онлайн-облікового запису потрібні особисті ідентифікатори, такі як ім'я, дата народження, адреса, тощо. Також таким слідом є електронні листи, пости, лайки, коментарі, які залишають користувачі.

Пасивний цифровий слід з'являється у мережі без відома користувача. Програми на смартфоні, сайти, розумний годинник та інші пристрої постійно збирають та передають на сервери компаній дані про користувачів, а саме: IP-адреси, історію пошуку, файли cookie та ін. Ця

інформація зберігається на серверах відповідних компаній та може бути використана комерційними організаціями, правоохоронними органами або злочинцями.

Активний цифровий слід користувач може мінімізувати самостійно. Для цього потрібно: регулярно перевіряти яка інформація доступна у відкритому доступі; налаштувати конфіденційність в соціальних мережах, що дозволить контролювати список користувачів, що «стежать» за профілем; обмежувати дані, що викладаються в мережу Інтернет; видалити старі акаунти; видаляти метадані та приховувати геолокацію; не під'єднуватись до загальнодоступної мережі Wi-Fi; не реєструватися на веб-сайтах за допомогою соціальних мереж; підтримувати програмне забезпечення у актуальному стані; скасувати підписку на сервіси розсилки; очищати файли cookie.

Пасивний цифровий слід скоротити досить складно, але "розмити" його можна різними методами. До базових відносять наступні: використання пошукових систем, які не зберігають інформацію про пошук, наприклад, DuckDuckGo, використання платних сервісів для видалення цифрового сліду, але вони можуть бути не досить ефективними; використовувати режиму «інкогніто» у браузері; користуватись розширеннями браузера для запобігання несанкціонованого стеження.

Висновки. Усе, що потрапляє в Інтернет зберігається, аналізується та використовується, тому методу повного видалення цифрових слідів не існує. Різні сервіси та платформи можуть бути корисні для пошуку та видалення інформації про людину, але вони не дають стовідсотковий результат. Проте, загалом, користувач може сам контролювати інформацію, яка доступна про нього в мережі та впроваджувати організаційні методи для зменшення свого цифрового сліду.

Список літератури

1. Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises. *ITRC*. URL: https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/ (дата звернення 28.10.2022);
2. Цуранов М.В. Методи та засоби боротьби з правопорушеннями в інформаційній сфері: навчальний посібник / М.В. Цуранов, В.М. Струков, В.Я. Пєвнєв. – Харків: ХНУВС, 2015. – 256 с.

Відомості про авторів

Малєєва Злата-Тіна Олександрівна, студентка кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 050-275-80-95, z.malieieva@student.csn.khai.edu

Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., доцент, v.pevnev@csn.khai.edu