

Астахов Даниїл Юрійович

*Національний університет «Одеська юридична академія»,
студент 2-го курсу факультету кібербезпеки та інформаційних
технологій*

ЗАСОБИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В МЕРЕЖІ ІНТЕРНЕТ

Сьогодні Інтернет є найбільш важливим ресурсом для спілкування та навчання. Це дуже великий крок для людства в цілому. В мережі інтернет є позитивні сторони, такі як багатий обсяг будь-якої інформації і про що завгодно, але звідси і виходять негативні сторони, тобто, переважна незахищеність персональних даних користувачів.

Базові способи захисту даних користувачів мережі інтернет?

Проблема з втратою персональних даних на користь зловмисника завжди була, є і буде. Персональними даними не обов'язково можуть бути ім'я чи прізвище, чи номер телефону, але і IP-адреса та будь-яка інша інформація, яка може ідентифікувати особистість користувача у цифровому просторі.

Є декілька порад для того, щоб максимально захистити користувача під час з'єднання з мережею інтернет:

1. Не підключатись до громадських мереж WI-FI, які не захищені паролем, тому, що вони можуть бути створеними мережами-двійниками для перехоплення даних користувачів.
2. Створювати складні паролі та змінювати їх як мінімум раз на місяць. Слід придумати багато різних та складних паролів, записати їх у блокнот для того, щоб максимально захистити особисті дані. Також є застосунки, які самі створюють складні паролі, прикладом такого застосунку є LastPass.
3. Використовувати двофакторну аутентифікацію – дуже важливий критерій для захисту даних. Кожен раз, коли користувач вводить свій пароль, він

має підтвердити, що це саме він через повідомлення. Це найголовніший засіб зупинення злочинця.

4. Слідкувати за адресним рядком. Краще використовувати захищені підключення, такі як HTTPS, а не HTTP.

5. Шифрувати повідомлення. В багатьох месенджерах вже давно є спеціальні системи, які допомагають захистити дані за допомогою шифрування повідомлень. Наприклад, в Фейсбуці є таємне листування. В системних налаштуваннях iPhone можна увімкнути функцію шифрування [1].

Методи захисту інформації, якими забезпечують розробники

У 2018 році в Європі було прийнято правила захисту персональних даних, а саме GDPR. За їх порушення прийдеться платити штраф.

GDPR – загальний регламент захисту персональних даних. Правила збору, зберігання, обробки, та розповсюдження даних дуже сильно змінено з цим регламентом, наприклад:

1. Право на доступ. Кожна людина має можливість отримати свої данні, і в даному випадку мова йде не тільки про ті дані, які представив сам користувач, а й дані, які збирає той чи інший сервіс про нього. Також користувач має право знати: для якої мети його дані було зібрано, скільки ці дані будуть зберігатися, чи має він право на видалення своїх даних тощо.

2. Право на уточнення. Користувач має право на змінення застарілих або недостовірних даних.

3. Право на компенсацію. Кожен користувач мережі інтернет має право на відшкодування збитку від втрати даних. Також сама організація має сплатити штраф за порушення GDPR [2].

Також є американський аналог, який було запущено в 2020 році. Називається він California Consumer Privacy Act, або CCPA. Це закон про захист персональних даних користувачів штату Каліфорнія, який на сьогодні є одним з найбільш регламентованих нормативних актів у сфері захисту персональних даних на території США [3].

Він розповсюджується саме на юридичні та фізичні особи саме в штаті Каліфорнія. За порушення правил, згідно ССРА, треба буде заплатити від 2500 до 7500 доларів, усе залежить від того, чи навмисно було порушення.

Розвиток йде дуже-дуже швидко, тому деякі користувачі просто не встигають зрозуміти, що треба зробити, щоб не віддати свої данні у руки зловмисників. Саме тому питання захисту даних в мережі інтернет є, мабуть, одним з найважливіших проблем сучасного світу. Кожного дня люди втрачають свої дані, чи за своєю провиною, чи за провиною розробників. Але треба зрозуміти, що наведені вище правила не зможуть захистити дані користувачів на 100%, але користувач зможе зробити усе можливе, що зловмиснику було дуже складно якось отримати про нього інформацію.

Тому, треба розповсюджувати інформацію, як захистити себе та користувачів додатків або сайтів, які використовують будь-які персональні дані.

Список використаних джерел:

1. 5 шляхів захисту особистих даних в інтернеті. : Веб сайт. URL: <https://beetroot.academy/blog/general/5-shlyahiv-zahistu-osobistih-danih-v-interneti> (Дата звернення: 1.11.2021).

2. Что такое GDPR и какие требования предъявляет. : Веб сайт. URL: <https://data-privacy-office.com/what-is-gdpr/> (Дата звернення: 1.11.2021).

3. California Consumer Privacy Act: новий тренд США із захисту персональних даних у 2020 році. : Веб сайт. URL: https://uz.ligazakon.ua/ua/magazine_article/EA013372 (Дата звернення: 1.11.2021).

Ключові слова: захист, персональні дані, користувач, розробник

Ключевые слова: защита, персональный данные, пользователь, разработчик

Keywords: security, personal data, user, developer

Науковий керівник: к.т.н., доц. Задерейко О.В.