

НАДІЙНІСТЬ ЗБЕРЕЖЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ В МЕРЕЖІ ІНТЕРНЕТ

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

Анотація: Нині кількість користувачів мережі Інтернет становить 4 мільярди, більшість реєструються на різноманітних сайтах, де вводять особисту інформацію. Таким чином, виникає ризик, що цими даними можуть скористатись шахраї. Тези присвячені проблемі захисту персональних даних в мережі Інтернет та способам, як уберегти свої дані.

Ключові слова: Інтернет, персональні дані, захист даних, безпека даних, шифрування, кібербезпека.

Abstract: Today, the number of Internet users is 4 billion, the majority register on various sites where they enter personal information. Thus, there is a risk that these data can be used by fraudsters. Abstracts are devoted to the problem of personal data protection in the Internet and how to protect your data.

Keywords: internet, personal data, data protection, data security, encryption, cyber security.

Інтернет – глобальна всесвітня телекомунікаційна мережа, яка забезпечує зв'язок для передачі файлів, отримання доступу до інформації, пересилання повідомлень електронної пошти, з'єднання з іншими комп'ютерами. Була розроблена в 60-70-х рр. XX ст. для службовців Міністерства оборони США, яка потім перетворилась в масове соціальне явище.

Іншими словами, Інтернет – це глобальна система взаємопов'язаних комп'ютерів, що використовують «набір протоколів Інтернет» в якості загального засобу комунікації один з одним.

Ця велика мережа сформована з незліченної кількості більш дрібних мереж, які використовують окремі установи, університети, приватні компанії та урядові органи. Їхні мережі пов'язані за допомогою оптоволоконних кабелів, телефонних ліній та бездротових технологій.

Відмінність між мережею Інтернет та іншими глобальними мережами полягає у змісті інформації та умовам доступу до неї. Порівнявши мережу Інтернет з іншими комп'ютерними мережами, можна зробити висновок, що перша не має єдиних правил доступу до інформації.

Нині мережа Інтернет має велику кількість користувачів. Тому мережу Інтернет справедливо вважати універсальним засобом до збереження та передачі інформації. З розвитком інформаційних технологій (а саме мережі Інтернет), набуло нового змісту право на захист та конфіденційність персональних даних [1]. Під час використання мережі Інтернет виникає проблема незаконного доступу до персональних даних. Тобто, доволі часто особисті дані користувачів передаються та обробляються без їх відома (користувачі можуть бути непроінформовані або не дають згоди на такі маніпуляції з їх даними). Для наглядної демонстрації цієї ситуації, розглянемо пошукову систему. Якщо користувач виконував пошук певних товарів або

послуг в мережі, то через деякий час на інших сайтах буде з'являтися реклама з товарами або послугами, які шукав користувач. З одного боку таке відслідковування є зручним, проте з іншого – має багато негативних аспектів. Використовуючи цільову рекламу можна просто визначати зміст інформації або ж маніпулювати інформацією, яку бачить користувач в Інтернеті, що призводить до впливу на людську свідомість, як споживача.

Доступ, розміщення, передача інформації в мережі Інтернет відбувається за допомогою провайдерів – компаній, які є постачальниками послуг Інтернет. Кожен провайдер має можливість встановлювати свої правила на використання мережею для своїх клієнтів. Тобто може контролювати інформацію, що передається або отримується користувачами в мережі Інтернет [2]. Контролювати діяльність провайдерів може держава за допомогою різних юридичних організацій. Також режим інформаційного обміну з використанням мережі Інтернет може бути предметом міжнародно-правового регулювання.

У зв'язку з активним розвитком інформаційних технологій врегулювання кібербезпеки відбувається на національному рівні. Нещодавно було розроблено новий Закон України «Про основні засади забезпечення кібербезпеки України». Сутність цього закону полягає в тому, що необхідно створити національну систему кібербезпеки, що відповідатиме за збереження даних громадян і держави взагалом.

Отже, основною вимогою є те, що персональні дані в мережі повинні зберігатись з високим рівнем захисту. Користувачі повинні мати змогу редагувати та видаляти свої особисті дані, а також повинні давати згоду на передачу та збереження наданої інформації.

За використання не за призначенням чужої конфіденційної інформації законодавством передбачена кримінальна відповідальність. У випадку незаконної обробки персональних даних та втручання в особисте життя необхідно звернутися до розпорядника персональних даних з вмотивованою вимогою:

- заборонити таку обробку;
- внести зміни до своїх персональних даних (у випадку їх недостовірності);
- вимагати їх видалення (знищення).

Якщо дана вимога не буде виконана, то вказані дії чи бездіяльність розпорядника персональних даних можуть бути оскаржені в Уповноваженого Верховної Ради України з прав людини та/або в суді. За Кримінальним кодексом, особи, які незаконно збирають, зберігають, знищують та поширюють конфіденційну інформацію можуть бути притягнуті до кримінальної відповідальності. За статтею про «Порушення недоторканості приватного життя» зловмисники повинні виплатити штраф від 8500 до 17000 гривень, а за повторні злочини – позбавлені волі терміном від 3 до 5 років.

Декілька порад для захисту особистих даних в Інтернеті.

Не підключатися до громадського WiFi. Зазвичай доступ до громадської мережі можна отримати переглянувши рекламу. Проте необхідно бути

обережним, оскільки зловмисники можуть створити мережу-двійника з такою самою назвою і таким чином перехоплювати введені користувачем дані.

Необхідно створювати складні паролі для соціальних мереж, поштових скриньок та ін. Якщо важко придумати та запам'ятати складний пароль, існують такі додатки, як менеджери паролів, що можуть вирішити дану проблему.

Необхідно слідкувати за адресним рядком. Для передачі введених користувачем даних на сервер використовується протокол HTTP. Проте браузер має використовувати протокол HTTPS, який є розширенням протоколу HTTP з надбудовою шифрування. Тобто дані, що передаються по протоколу HTTP не захищені, а HTTPS забезпечує конфіденційність інформації шляхом її шифрування [4].

Використовувати шифрування повідомлень. Тобто, лише отримувач повідомлення бачить його на своєму пристрої у доступному для читання вигляді. Нині цей спосіб захищення даних є дуже популярним серед сучасних користувачів. Окрім того, пропонуються секретні чати, які мають більш складні алгоритми шифрування. Головне – не використовувати СМС-повідомлення для передачі важливої інформації, оскільки цей канал зовсім незахищений [5].

Висновки

Таким чином, захист персональних даних на сьогоднішній день – тематика досить актуальна, що пов'язано не тільки зі швидким розвитком Інтернет технологій і глобалізацією в цілому, але і з необхідністю захистити право громадян на приватне життя.

Науковий керівник: Прокопенко І. Д., асистент каф. електропостачання

Література

1. Акопов Г. Л. Інформаційне право / Г.Л. Акопов. – М.: Фенікс, 2008. – 348с.
2. Харчук В. Запровадження правового регулювання відносин у глобальній мережі Інтернет / В. Харчук // Юридичний журнал. – 2010.– № 12. – С. 80-82.
3. Захист особистих та персональних даних в Інтернеті: проблеми законодавчого врегулювання [Електронний ресурс]. – Режим доступу: http://ukrainepravo.com/scientific-thought/legal_analyst/zakhist-osobistikh-ta-personalnikh-danikh-v-interneti-problemi-zakonodavchogo-vregulyuvannya/.
4. Ера Інтернету [Електронний ресурс]. – Режим доступу: https://www.prointernet.in.ua/files/mod_1.pdf.
5. П'ять шляхів захисту особистих даних в Інтернеті [Електронний ресурс]. – Режим доступу: <https://beetroot.academy/uk/blog/5-shlyahiv-zahistu-osobistih-danikh-v-interneti/>.