БЕЗПЕКА В ІНТЕРНЕТІ ТА ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Землянська О. В., ст. викл. (каф. ОППЦБ КПІ ім. Ігоря Сікорського);
Редін К. А., ст. (гр. КП-81мп, ФПМ КПІ ім. Ігоря Сікорського)

Анотація: Безпека інформації та персональних даних в Інтернеті є дуже важливим питанням на сьогоднішній день, адже з кожним днем росте кількість людей, які користуються глобальною мережею. Тези присвячені визначенню основних проблем захисту інформації в Інтернеті та їх вирішенню.

Ключові слова: Інтернет, всесвітня мережа, безпека персональних даних, конфіденційність, захист даних, проблеми захисту інформації.

Abstract: The security of information and personal data on the Internet is a very important issue because the number of people using World Wide Web is growing day by day. The paper is devoted to the main problems of the data protection on the Internet and possible solutions.

Keywords: Internet, World Wide Web, personal data security, privacy, data protection, information security.

На сьогоднішній день сфера інформаційно-обчислювальних технологій торкається майже усіх аспектів нашого життя. В Інтернеті щодня здійснюються тисячі різноманітних операцій, платежів, розмов, листувань та багато інших дій, що потребують конфіденційності користувача та захисту його персональних даних [1].

Саме поняття інформаційної безпеки означає стан інформацій, при якому система нормально функціонує та забезпечується цілісність, конфіденційність та захищеність персональних даних, а також забезпечення доступу до них.

Можна виділити три основні принципи, які відносяться до інформаційної безпеки:

– доступ до конфіденційних даних має бути лише у авторизованих користувачів;

– повнота та достовірність інформації означають її цілісність;

– доступність інформації означає, що при виникненні потреби авторизованим користувачам може бути забезпечений доступ до певних ресурсів, на яких розміщена ця інформація.

З появою всесвітньої мережі з’явились і проблеми захисту інформації в ній, адже Інтернет і інформаційна безпека несумісні за своєю природою. Відомо, що чим легший доступ в мережу, тим гіршою є її інформаційна безпека. Користувач може навіть не дізнатися, що його дані були скопійовані, змінені або навіть зіпсовані [2].

Існують антропогенні, техногенні та стихійні джерела загрози персональним даним.

До антропогенних джерел відносяться випадкові, або навмисні дії деяких суб’єктів. Існує два види таких дій:

– зовнішні – коли відбувається незаконне проникнення третьої особи зі сторони зовнішньої мережі;

– внутрішні – коли відбувається порушення інформаційної безпеки зсередини, наприклад працівником певної компанії.

До техногенних джерел відноситься все, що може призвести до відмови роботи програмного забезпечення або апаратної частини. Це можуть бути як застаріла система, під’єднанні до неї прилади, серверні проблеми, збої в кабельній або дисковій системі, так і програмні помилки, несправність операційної системи.

До стихійних джерел відносяться різноманітні природні катаклізми. Злива може викликати проблеми з електромережею, хуртовина проблеми зі зв`язком, а буревії можуть пошкодити або знищити необхідне для збереження або доступу до інформації обладнання [3].

Коли мова йде про захист персональних даних в мережі Інтернет, найчастіше мається на увазі антропогенні джерела загрози. Оскільки при передачі даних, вони мають пройти велику кількість різноманітних роутерів та серверів. На цьому шляху інформацію можуть перехопити, пошкодити, змінити, перенаправити, або «заразити» комп’ютерним вірусом, адже вже на рівні архітектури Інтернет не має засобів захисту від злодіїв.

Захист даних насамперед необхідний для компаній та організацій, таких як банкові системи, оператори, державні організації тощо.

Ще однією проблемою при забезпеченні захисту корпоративної мережі є ефективність роботи, адже при підвищенні рівня безпеки, знижується швидкість доступу, що може негативно вплинути на продуктивність роботи.

Робота звичайного користувача у всесвітній мережі також потребує захисту, як зі сторони організацій, що надають доступ до Інтернету, так зі сторони сервісів, що зберігають персональні дані. Але, найважливішим є розуміння небезпеки самим користувачем, свідоме використання мережі, а також внесення у неї своєї інформації.

Не зважаючи на те, що з самого заснування Інтернет не був захищеним, сьогодення внесло свої корективи і зараз існує необхідність удосконалювати засоби захисту.

Усі існуючі засоби захисту можна класифікувати наступним чином:

– апаратні;
– програмні;
– змішані;
– засоби організаційного характеру.

До групи апаратних засобів відносяться електронні або механічні засоби, що забезпечують захист від фізичного проникнення, або у випадку, якщо доступ все ж був отриманий, замаскувати дані для їх збереження.

Програмні засоби можуть ідентифікувати користувачів для контролю доступу, шифрувати або видаляти інформацію, тестувати контроль системи захисту даних. Рівень захисту цієї групи менший за апаратний, але більш гнучкий та дешевий, що спрощує використання та зменшує фінансові витрати на захист.

Змішані засоби захисту поєднують в собі апаратні і програмні розробки для підвищення ефективності та надійності системи. Ці засоби є найпоширенішими у використанні.

До засобів організаційного характеру відносяться як контроль доступу до приміщення, так і складання та вивчення правил користування комп'ютерною мережею, а також свідоме використання власних даних у ній.

Провайдери забезпечують максимальний захист інформації своїх користувачів завдяки апаратно-програмним засобам, а сучасні операційні системи мають вбудовані програмні засоби захисту, такі як брандмауер.

Крім того, існує безліч антивірусів, що збільшують захищеність системи від зловмисників, завдяки своєчасному оновленню вірусних баз. Усі сервіси, що оперують персональними даними, зобов'язують користувачів до створення облікових записів для подальшої аутентифікації, що забезпечує доступ до даних лише авторизованим у системі користувачам.

Висновки

Незважаючи на всі заходи безпеки, користувач має і сам розуміти ризики користування мережею, адже в більшості випадків зловмисник розраховує не лише на прогалину в системі, а й на людський фактор. При дотриманні всіх правил користування мережею, ризик втрати, ушкодження або викрадення даних значно знижується, але не зникає. Саме тому при доступі в Інтернет важливо уникати надмірного розповсюдження персональних даних.

Література

1. Зацарний В. В. Безпека життєдіяльності: навч. посіб. / В. В. Зацарний, Н. А. Праховнік, О. В. Землянська, О. В. Зацарна – Київ : НТУУ «КПІ» ІЕЕ, 2016. – електронне видання. URL: http://ela.kpi.ua/kandle/123456789/18263.

2. Безпека в мережі інтернет [Електронний ресурс]. – Режим доступу: http://svitppt.com.ua/informatika/osnovni-ponyattya-zahistu-informacii.htmll

3. Технології захисту інформації [Електронний ресурс]. – Режим доступу: https://www.uzhnu.edu.ua/uk/infocentre/get/4186.