

# Норми користування мережею Інтернет

Мережа Інтернет являє собою глобальне децентралізоване об'єднання комп'ютерних мереж та інформаційних ресурсів, що належать багатьом різним людям та організаціям, яке не має єдиного переліку правил (законів) користування Мережею. Однак, існують загальноприйняті норми роботи в мережі Інтернет, які скеровані на те, щоб забезпечити нормальну роботу кожного з користувачів, яка не заважає роботі інших користувачів.

Фундаментальним положенням цих норм є наступне:

**Правила користування будь-якими ресурсами мережі Інтернет (від поштової скриньки до каналу зв'язку) визначають виключно власники цих ресурсів і лише вони.**

Даний документ описує загальноприйняті норми роботи в мережі Інтернет, дотримання яких є обов'язковим для усіх без винятку користувачів. Дія цих норм розповсюджується на порядок використання ресурсів Мережі. Тут і надалі словом Мережа позначаються глобальна мережа Інтернет та доступні з неї інші мережі.

## 1. ОБМЕЖЕННЯ НА ІНФОРМАЦІЙНИЙ ШУМ (СПАМ)

Розвиток Мережі призвів до того, що однією з основних проблем користувачів став надлишок інформації. Через це спільнота Мережі розробила спеціальні правила, які направлено на захист користувача від непотрібної йому/незамовленої ним інформації (спама). Так, при користуванні Мережею є неприпустимим:

- 1.1 Масове розповсюдження попередньо не обумовлених електронних листів (unsolicited mass mailing)<sup>1</sup>. Під неузгодженим масовим розповсюдженням розуміється як розсилка множині адресантів, так і розсилка багатьох листів одному адресанту.
- 1.2 Не обумовлене раніше відправлення електронних листів більше однієї сторінки або наявність у листі вкладених файлів.
- 1.3 Не обумовлене розповсюдження електронних листів рекламного, комерційного або агітаційного характеру, а також листів, що містять грубі, нецензурні або принижуючі вирази чи пропозиції.
- 1.4 Розміщення в будь-якій конференції Usenet або в іншій конференції<sup>2</sup>, форумі або електронному списку розсилки публікацій, які не відповідають тематиці даної конференції чи списку розсилки (off-topic).
- 1.5 Розміщення в будь-якій конференції повідомлень рекламного, комерційного чи агітаційного характеру, окрім випадків, коли такі повідомлення явно дозволені правилами конференції або їх розміщення було попередньо обумовлене із власниками або адміністраторами конференції.
- 1.6 Розміщення в будь-якій конференції статті, що містить вкладені файли, окрім випадків, коли це є явно дозволено правилами конференції або їх розміщення було попередньо обговорене із власниками або адміністраторами конференції.
- 1.7 Розсилка інформації користувачам, які повідомили раніше явне небажання отримувати дану інформацію.
- 1.8 Використання власних або наданих інформаційних ресурсів (поштових скриньок, адресів електронної пошти, сторінок WWW, тощо) в якості контактних координат при скоєнні будь-якої з вище описаних дій, незалежно від того, з якої точки Мережі були скоєні ці дії.

<sup>1</sup> тут і надалі під електронними листами розуміються повідомлення електронної пошти, ICQ та інших подібних засобів особистого обміну інформацією

<sup>2</sup> тут і надалі під конференцією розуміється телеконференції (групи новин) Usenet та інші конференції, форуми та електронні списки розсилки

## **2. ЗАБОРОНА НЕСАНКЦІОНОВАНОГО ДОСТУПУ ТА МЕРЕЖЕВИХ АТАК**

Не допускається здійснення спроб несанкціонованого доступу до ресурсів Мережі, проведення або участь в атаках та зламів в Мережі, за виключенням випадків, коли атака на ресурс Мережі відбувається з явної згоди власника або адміністратора цього ресурсу. У тому числі заборонені:

- 2.1 Дії, направлені на порушення нормального функціонування елементів Мережі (комп'ютерів, іншого обладнання або програмного забезпечення), що не належать користувачу.
- 2.2 Дії, направлені на отримання несанкціонованого доступу, в тому числі привілейованого, до ресурсу Мережі (комп'ютера, іншого обладнання або інформаційного ресурсу), наступне використання такого доступу, а також знищення чи модифікація програмного забезпечення чи даних, які не належать користувачу, без узгодження із власниками цього програмного продукту чи даних або адміністраторами даного інформаційного ресурсу.
- 2.3 Передача комп'ютерам чи обладнанню Мережі беззмстовної чи шкідливої інформації, що створює паразитне навантаження на ці комп'ютери чи обладнання, а також проміжні відрізки Мережі, в об'ємах, що перевищують мінімально припустимі для перевірки зв'язку між мережами чи доступності окремих її елементів.

## **3. ДОТРИМАННЯ ПРАВИЛ, ЩО ВСТАНОВЛЕНІ ВЛАСНИКАМИ РЕСУРСІВ**

Окрім вище наведених правил, власник будь-якого інформаційного чи технічного ресурсу Мережі може встановлювати для цього ресурсу власні правила його використання.

Ці правила використання публікуються власниками або адміністраторами ресурсів. Вони або посилання на них є доступними при підключенні користувача до ресурсу.

Користувач зобов'язаний дотримуватися правил використання ресурсу, встановлених власником, або відмовитися від його використання.

Власник або адміністратор ресурсу (комп'ютерів, іншого обладнання або програмного забезпечення), що не належить користувачу, не несе відповідальності перед користувачем за будь-які збитки, які можуть бути завдані йому внаслідок невиконання ним зобов'язань, що регламентуються загальноприйнятими нормами користування мережею Інтернет.

Власник або адміністратор ресурсу, що не належить користувачу залишає за собою право заборонити виконання скриптів користувача, що можуть викликати перевантаження системи та/або нанести яку-небудь шкоду роботі серверного програмного забезпечення.

## **4. НЕПРИПУСТИМІСТЬ ФАЛЬСИФІКАЦІЇ**

Значна частина ресурсів Мережі не вимагає ідентифікації користувача та допускає анонімне використання. Однак, у ряді випадків користувач має надати інформацію, яка ідентифікує його та засоби доступу до Мережі, які він використовує. При цьому користувачу заборонено:

- 4.1 Використовувати ідентифікаційні дані (імена, адреси, телефони, тощо) третіх осіб, крім випадків, коли ці особи уповноважили користувача на таке використання.
- 4.2 Користувач має прийняти відповідні міри, щоб запобігти використанню ресурсів Мережі третіми особами від його імені (забезпечити надійне збереження паролів та інших кодів авторизованого доступу та управління своїми WEB-проектами).
- 4.3 Фальсифікувати свою IP-адресу, а також адреси, що використовуються в інших мережесих протоколах при обміні даними в Мережі.
- 4.4 Використовувати неіснуючі зворотні адреси при відправленні електронних листів.