ПРАВИЛА КОРИСТУВАННЯ МЕРЕЖЕЮ ІНТЕРНЕТ

Мережа Інтернет є глобальним об'єднанням комп'ютерних мереж та інформаційних ресурсів, що належать безлічі різних людей та організацій. Це об'єднання є децентралізованим, і єдиного загальнообов'язкового зведення правил (законів) користування мережею Інтернет не встановлено. Проте існують загальноприйнятні норми роботи в мережі Інтернет, спрямовані на те, щоб діяльність кожного користувача мережі не заважала роботі інших користувачів.

Фундаментальним положенням цих норм є таке: ПРАВИЛА ВИКОРИСТАННЯ БУДЬ-ЯКИХ РЕСУРСІВ МЕРЕЖІ ІНТЕРНЕТ ВИЗНАЧАЮТЬ ВЛАСНИКИ ЦИХ РЕСУРСІВ І ТІЛЬКИ ВОНИ (тут і далі словом "ресурс" позначається будь-яка сукупність програмних та апаратних засобів, що становлять в тому чи іншому значенні єдине ціле. Ресурсом мережі Інтернет можуть вважатись, наприклад, поштова скринька, персональний комп'ютер, віртуальний або фізичний сервер, локальна обчислювальна мережа, канал зв'язку тощо).

Як показує практика, більшість користувачів мережі Інтернет очікують від інших користувачів дотримання загальноприйнятних мережевих норм, оскільки їх порушення призводить до серйозних ускладнень роботи в Мережі, як технічних, так і зумовлених людським чинником.

1. ОБМЕЖЕННЯ НА ІНФОРМАЦІЙНИЙ ШУМ (СПАМ)

Розвиток Мережі призвів до того, що однією з основних проблем користувачів став надлишок інформації. Тому мережеве співтовариство виробило спеціальні правила, направлені на захист користувача від непотрібної /незапитаної інформації (спама). Зокрема, є неприпустимими:

1.1. Масове розсилання повідомлень електронною поштою та іншими засобами персонального обміну інформацією (включно зі службами негайної доставки повідомлень, такими як SMS, IRC і т.п.), інакше як за явно і недвозначно вираженою ініціативою одержувачів.

Відкрита публікація адреси електронної пошти чи іншої системи персонального обміну інформацією не може служити підставою для включення адреси в який-небудь список для масового розсилання
повідомлень.

Включення адреси, отриманої будь-яким шляхом (через веб-форму, через підписного робота і т.п.), в перелік адрес, за яким проводиться якесь розсилання, допускається лише за умови наявності належної технічної процедури підтвердження підписки, яка гарантує, що адреса не потрапить в список інакше, як за волею власника адреси.

Процедура підтвердження підписки повинна виключати можливість потрапляння адреси в список адресатів якоїсь розсилки (одноразової чи регулярної) за ініціативою третіх осіб (тобто осіб, які не є власниками даної адреси).

Обов'язково має бути можливість для будь-якого одержувача негайно залишити список розсилки без жодних утруднень, щойно у нього виникне таке бажання. При цьому наявність можливості залишити список сама по собі не може служити виправданням внесення адрес до списку не за волею
власників адрес.

1.2. Відправлення електронних листів та інших повідомлень, що містять вкладені файли (attachments) та/або мають значний об'єм, без попередньо отриманого дозволу адресата.

1.3. Розсилання (інакше, як за прямою ініціативою одержувача):

а) електронних листів та інших повідомлень (у тому числі одиничних) рекламного, комерційного або агітаційного характеру;

б) листів і повідомлень, що містять грубі і образливі вирази і пропозиції.

в) повідомлень, що містять прохання переслати дане повідомлення іншим доступним користувачам (ланцюгові листи - chain letters).

г) з використанням безособових ("ролевих") адрес інакше, як за їх прямим призначенням, встановленим власником адрес та/або стандартами.

1.4. Розміщення в будь-якій електронній конференції повідомлень, які не відповідають тематиці даної конференції (off-topic). Тут і далі під конференцією розуміються телеконференції (групи новин) Usenet та інші конференції, форуми і списки розсилки.

1.5. Розміщення в будь-якій конференції повідомлень рекламного, комерційного або агітаційного характеру, крім випадків, коли такі повідомлення явно дозволені правилами даної конференції або їх
розміщення було погоджено з власниками або адміністраторами даної конференції заздалегідь.

1.6. Розміщення в будь-якій конференції статті, що містить вкладені файли, крім випадків, коли вкладення явно дозволені правилами даної конференції або таке розміщення було погоджено з власниками або адміністраторами конференції заздалегідь.

1.7. Розсилання інформації одержувачам, які раніше в явному вигляді висловили небажання одержувати цю інформацію, інформацію даної категорії або інформацію від даного відправника.

1.8. Використання власних або наданих інформаційних ресурсів (поштових скриньок, адрес електронної пошти, сторінок WWW і т.д.) як контактних координат при здійсненні будь-якої з вищеописаних дій, незалежно від того, з якого місця Мережі були вчинені ці дії.

1.9. Здійснення діяльності з технічного забезпечення розсилання спама (spam support service), як то:

а) цілеспрямоване сканування вмісту інформаційних ресурсів з метою збору адрес електронної пошти та інших служб доставки повідомлень;

б) розповсюдження програмного забезпечення для розсилання спама;

в) створення, верифікація, підтримка або розповсюдження баз даних адрес електронної пошти чи інших служб доставки повідомлень (за винятком випадку, коли власники всіх адрес, включених до такої бази даних, в явному вигляді виказали свою згоду на включення адрес саме до цієї конкретної бази даних; відкрита публікація адреси такою згодою вважатися не може).

2. ЗАБОРОНА НЕСАНКЦІОНОВАНОГО ДОСТУПУ І МЕРЕЖЕВИХ НАПАДІВ

Неприпустимими є спроби несанкціонованого доступу до ресурсів Мережі, проведення мережевих нападів та мережевого зламу і участь в них, за винятком випадків, коли напад на мережевий ресурс проводиться з явного дозволу власника або адміністратора цього ресурсу. Зокрема, заборонені:

2.1. Дії, спрямовані на порушення нормального функціонування елементів Мережі (комп'ютерів, іншого устаткування або програмного забезпечення), які не належать користувачу.

2.2. Дії, направлені на отримання несанкціонованого доступу до ресурсу Мережі (комп'ютера, іншого устаткування або інформаційного ресурсу), подальше використання такого доступу, а також знищення або модифікація програмного забезпечення чи даних, що не належать користувачу, без узгодження з власниками чи адміністраторами даного інформаційного ресурсу. Під несанкціонованим доступом розуміється будь-який доступ способом, відмінним від

передбаченого власником ресурсу.

2.3. Передавання комп'ютерам або устаткуванню Мережі безглуздої або даремної інформації, що створює паразитне навантаження на ці комп'ютери чи устаткування та проміжні ділянки мережі, в об'ємах, що перевищують мінімально необхідні для перевірки зв'язності мереж і доступності окремих її елементів.

2.4. Цілеспрямовані дії по скануванню вузлів мереж з метою виявлення внутрішньої структури мереж, списків відкритих портів і т.п., інакше як в межах, мінімально необхідних для проведення штатних технічних заходів, що не ставлять метою порушення пунктів 2.1 і 2.2 цього документа.

3. ДОТРИМАННЯ ПРАВИЛ, ВСТАНОВЛЕНИХ ВЛАСНИКАМИ РЕСУРСІВ

Власник будь-якого інформаційного або технічного ресурсу Мережі може встановити для цього ресурсу власні правила його використання.

Правила використання ресурсів або посилання на них публікуються власниками або адміністраторами цих ресурсів в місці підключення до таких ресурсів і є обов'язковими до виконання всіма користувачами цих ресурсів.

Правила мають бути легко доступними, написаними з урахуванням різного рівня підготовки користувачів.

Правила використання ресурсу, встановлені власником, не повинні порушувати права власників інших ресурсів або приводити до зловживань щодо інших ресурсів.

Користувач зобов'язаний дотримуватись правил використання ресурсу або негайно відмовитись від його використання.

У випадку, якщо правила, встановлені власником ресурсу, суперечать тим або іншим пунктам цього документа, щодо даного ресурсу застосовуються правила, встановлені власником, якщо це не призводить до порушень щодо інших ресурсів.

У випадку, якщо власником групи ресурсів явно встановлені правила тільки для частини ресурсів, для інших застосовуються правила, сформульовані в даному документі.

4. НЕПРИПУСТИМІСТЬ ФАЛЬСИФІКАЦІЇ

Значна частина ресурсів Мережі не вимагає ідентифікації користувача і допускає анонімне використання. Проте у ряді випадків від користувача вимагається надати інформацію, що ідентифікує його та засоби доступу до Мережі, що він використовує. При цьому користувач не повинен:

4.1. Використовувати ідентифікаційні дані (імена, адреси, телефони і т.п.) третіх осіб, крім випадків, коли ці особи уповноважили користувача на таке використання.

4.2. Фальсифікувати свою IP-адресу, а також адреси, що використовуються в інших мережевих протоколах, при передачі даних в Мережу.

4.3. Використовувати неіснуючі зворотні адреси при відправленні електронних листів і інших повідомлень.

4.4. Недбало ставитись до конфіденційності власних ідентифікаційних реквізитів (зокрема, паролів та інших кодів авторизованого доступу), що може привести до використання тих чи інших ресурсів третіми особами від імені даного користувача.

5. НАЛАШТУВАННЯ ВЛАСНИХ РЕСУРСІВ

При роботі в мережі Інтернет користувач стає її повноправним учасником, що створює потенційну можливість для використання мережевих ресурсів, що належать користувачу, третіми особами. У зв'язку з цим користувач повинен вжити належних заходів з такого налаштування своїх ресурсів, яке перешкоджало б несумлінному використанню цих ресурсів третіми особами, а в разі виявлення випадків такого використання - вживати оперативних заходів щодо їх припинення.

Прикладами потенційно проблемної настройки мережевих ресурсів є:

- відкриті ретранслятори електронної пошти (open SMTP-relays);
- загальнодоступні для неавторизованої публікації сервери новин (конференцій, груп);
- засоби, що дозволяють третім особам неавторизовано приховати джерело з'єднання (відкриті проксі-сервери і т.п.);
- загальнодоступні широкомовні адреси локальних мереж, що дозволяють проводити з їх допомогою напади типу smurf;
- електронні списки розсилки з недостатньою надійністю механізму підтвердження підписки або без можливості її скасування;
- www-сайти та інші подібні ресурси, що здійснюють відправку кореспонденції третім особам за анонімним або недостатньо аутентифікованим запитом.