Норми користування Мережею

Даний документ є одним з можливих формальних описів загальноприйнятих норм мережевої взаємодії, що вважаються в більшості мереж (як входять до мережі Інтернет безпосередньо, так і доступних з мережі Інтернет тим чи іншим опосередкованим чином) обов'язковими до виконання всіма користувачами. Такі або аналогічні норми застосовуються до всіх доступних мережевих ресурсів, коли заздалегідь не відомі правила, встановлені власниками цих ресурсів самостійно.

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, спрямовані на захист користувача від непотрібної/незапитаної інформації (спаму). Зокрема є неприпустимими:

- Масове надсилання повідомлень за допомогою електронної пошти та інших засобів персонального обміну інформацією (включаючи служби негайної доставки повідомлень, такі як SMS, IRC тощо), інакше як за явно і недвозначно вираженою ініціативою одержувачів. Відкрита публікація адреси електронної пошти або іншої системи персонального обміну інформацією не може бути підставою для включення адреси до будь-якого списку для розсилки повідомлень. Включення адреси, отриманої будь-яким шляхом (через веб-форму, через підписного робота тощо), до списку адрес, за якою проводиться будь-яке розсилання, допускається лише за умови наявності належної технічної процедури підтвердження підписки, яка гарантує, що адреса не потрапить у список інакше, як з волі власника адреси. Процедура підтвердження підписки повинна унеможливлювати попадання адреси до списку адресатів будь-якої розсилки (поодинокою або регулярною) за ініціативою третіх осіб (тобто осіб, які не є власниками цієї адреси). Обов'язково наявність можливості для будь-якого передплатника негайно залишити список розсилки без будь-яких труднощів при виникненні такого бажання. При цьому наявність можливості залишити список сама по собі не може бути виправданням внесення адрес до списку не з волі власників адрес.

- Надсилання електронних листів та інших повідомлень, що містять вкладені файли та/або мають значний обсяг, без попереднього дозволу адресата.

- Розсилка (інакше як за прямою ініціативою одержувача):

  - електронних листів та інших повідомлень (у тому числі поодиноких) рекламного, комерційного чи агітаційного характеру;

  - Листів та повідомлень, що містять грубі та образливі вирази та речення.

  - Розсилання повідомлень, що містять прохання надіслати це повідомлення іншим доступним користувачам (chain letters).

  - Використання безособових ("рольових") адрес інакше, як за їх прямим призначенням, встановленим власником адрес та/або стандартами.

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

- Розміщення в будь-якій конференції повідомлень рекламного, комерційного чи агітаційного характеру, крім випадків, коли такі повідомлення явно дозволені правилами цієї конференції або їхнє розміщення було узгоджено з власниками або адміністраторами цієї конференції попередньо.

- Розміщення у будь-якій конференції статті, що містить прикладені файли, крім випадків, коли вкладення явно дозволені правилами даної конференції або таке розміщення було узгоджено з власниками або адміністраторами конференції попередньо.

- Розсилання інформації одержувачам, які раніше у явному вигляді висловили небажання отримувати цю інформацію, інформацію даної категорії або інформацію від даного відправника.

- Використання власних або наданих інформаційних ресурсів (поштових скриньок, адрес електронної пошти, сторінок WWW і т.д.) як контактні координати при виконанні будь-якої з вищеописаних дій, незалежно від того, з якої точки Мережі були виконані ці дії.

- Здійснення діяльності з технічного забезпечення розсилки спаму (spam support service), як то:

  - цілеспрямоване сканування вмісту інформаційних ресурсів з метою збирання адрес електронної пошти та інших служб доставки повідомлень;

  - розповсюдження програмного забезпечення для розсилки спаму;

  - створення, верифікація, підтримка або розповсюдження баз даних адрес електронної пошти або інших служб доставки повідомлень (за винятком випадку, коли власники всіх адрес, включених до такої бази даних, явно висловили свою згоду на включення адрес в цю конкретну базу даних; відкрита публікація адреси (такою згодою вважатися не може).

2 Заборона несанкціонованого доступу та мережевих атак

Не допускається здійснення спроб несанкціонованого доступу до ресурсів Мережі, проведення мережевих атак та мережного злому та участь у них, за винятком випадків, коли атака на мережевий ресурс проводиться з явного дозволу власника або адміністратора цього ресурсу. У тому числі заборонено:

- Дії, спрямовані на порушення нормального функціонування елементів Мережі (комп'ютерів, іншого обладнання або програмного забезпечення), які не належать користувачеві.

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

- Передача комп'ютерів або обладнання Мережі безглуздої або непотрібної інформації, що створює паразитне навантаження на ці комп'ютери або обладнання, а також проміжні ділянки мережі в об'ємах, що перевищують мінімально необхідні для перевірки зв'язності мереж та доступності окремих її елементів.

- Цілеспрямовані дії щодо сканування вузлів мереж з метою виявлення внутрішньої структури мереж, списків відкритих портів тощо, інакше як у межах, мінімально необхідних для проведення штатних технічних заходів, які не мають на меті порушення пунктів 2.1 та 2.2 цього документа.

3 Дотримання правил, встановлених власниками ресурсів

Власник будь-якого інформаційного чи технічного ресурсу Мережі може встановити для цього ресурсу власні правила використання. Правила використання ресурсів або посилання на них публікуються власниками або адміністраторами цих ресурсів у точці підключення до таких ресурсів та 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 призводити до зловживань щодо інших ресурсів.

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

У випадку, якщо правила, встановлені власником ресурсу, суперечать тим чи іншим пунктам цього документа, щодо цього ресурсу застосовуються правила, встановлені власником, якщо це не призводить до порушень інших ресурсів. У разі, якщо власником групи ресурсів явно встановлені правила лише частини ресурсів, інших застосовуються правила, сформульовані у цьому документі.

4 Неприпустимість фальсифікації.

Значна частина ресурсів мережі не потребує ідентифікації користувача та допускає анонімне використання. Однак у ряді випадків від користувача потрібно надати інформацію, що ідентифікує його та використовувані ним засоби доступу до Мережі. При цьому користувач не повинен:

- Використовувати ідентифікаційні дані (імена, адреси, телефони тощо) третіх осіб, за винятком випадків, коли ці особи уповноважили користувача на таке використання.

- Фальсифікувати свою IP-адресу, а також адреси, що використовуються в інших мережевих протоколах під час передачі даних до мережі.

- Використовувати неіснуючі зворотні адреси для надсилання електронних листів та інших повідомлень.

- Недбало ставитися до конфіденційності власних ідентифікаційних реквізитів (зокрема паролів та інших кодів авторизованого доступу), що може призвести до використання тих чи інших ресурсів третіми особами від імені цього користувача (з приховуванням, таким чином, справжнього джерела дій).

5 Налаштування власних ресурсів

При роботі в мережі Інтернет користувач стає повноправним учасником, що створює потенційну можливість для використання мережевих ресурсів, що належать користувачеві, третіми особами. У зв'язку з цим користувач повинен вжити належних заходів щодо такого настроювання своїх ресурсів, який перешкоджав би недобросовісному використанню цих ресурсів третіми особами, а при виявленні випадків такого використання вживати оперативних заходів щодо їх припинення.

Прикладами потенційно проблемного налаштування 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 тощо);
- загальнодоступні широкомовні адреси локальних мереж, що дозволяють проводити за допомогою атаки типу smurf;

- електронні списки розсилки з недостатньою надійністю механізму підтвердження підписки або без можливості її скасування;

- www-сайти та інші подібні ресурси, які надсилають кореспонденцію третім особам за анонімним або недостатньо автентифікованим запитом.