Норми Користування Мережею (OFISP-008)

Мережа Інтернет є глобальним об'єднанням комп'ютерних мереж та інформаційних ресурсів, що належать безлічі різних людей і організацій. Це об'єднання децентралізоване, і єдиної загальнообов'язкової збірки правил (законів) користування мережею Інтернет не встановлено. Існують, проте, загальноприйняті норми роботи в мережі Інтернет, спрямовані на те, щоб діяльність кожного користувача мережі не заважала роботі інших користувачів. Фундаментальне положення цих норм таке: правила користування будь-якими ресурсами мережі Інтернет визначають власники цих ресурсів, і лише вони (тут і далі словом "ресурс" позначається будь-яка сукупність програмних і апаратних засобів, що становлять у тому або іншому значенні єдине ціле; ресурсом мережі Інтернет можуть вважатися, наприклад, поштова скринька, персональний комп'ютер, віртуальний або фізичний сервер, локальна обчислювальна мережа, канал зв'язку і т. д.).

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

Як показує практика, більшість користувачів мережі Інтернет чекає від інших користувачів виконання загальноприйнятих мережевих норм, оскільки їх порушення спричиняє серйозні ускладнення роботи в Мережі, як технічні, так і обумовлені людським чинником. Під час створення документа не ставилося за мету формулювання універсальних правил роботи в Мережі, дублювати положення законодавства тих або інших держав і т. п. Документ охоплює виключно внутрішньомережеві нормативи, що склалися в міжнародному мережевому співтоваристві як прояв самозбереження мережі Інтернет.

Автори документа сподіваються, що дана формалізація загальноприйнятих норм буде корисною як адміністраторам мереж під час розробки правил доступу для користувачів, так і кінцевим користувачам Мережі для уникнення конфліктних ситуацій у повсякденній роботі. Крім того, даний документ допоможе визначити, якої поведінки слід чекати користувачеві від інших учасників мережевої взаємодії і в яких випадках можна вважати себе потерпілим від неприпустимих дій.

1. ОБМЕЖЕННЯ НА ІНФОРМАЦІЙНИЙ ШУМ (СПАМ)

Розвиток Мережі спричинив одну з основних проблем користувачів – надлишок інформації. Тому мережеве співтовариство виробило спеціальні правила, спрямовані на захист користувача від непотрібної/незапитуваної інформації (спаму). Зокрема, є неприпустимими:

1.1. Масова розсилка повідомлень за допомогою електронної пошти та інших засобів персонального обміну інформацією (включаючи служби негайної доставки повідомлень, такі як SMS, IRC і т. п.), інакше як за явно і недвозначно вираженою ініціативою одержувач.

1.2. Відкрита публікація адреси електронної пошти або іншої системи персонального обміну інформацією не може служити підставою для залучення адреси до якого-небудь списку для масової розсилки повідомлень. Залучення адреси, одержаної будь-яким шляхом (через веб-форму, через підписного робота і т. п.), до списку адрес, за яким проводиться будь-яка розсилка, допускається тільки за умови наявності належної технічної процедури підтвердження або передплати, яка гарантує, що адреса не потрапить до списку інакше, ніж за бажанням власника адреси. Процедура підтвердження передплати повинна виключати можливість включення адреси до списку адресатів будь-якої розсилки (одноразової або регулярної) за ініціативою третіх осіб (тобто осіб, що не є власниками даної адреси

1.3. Обов'язкова наявність можливості для будь-якого замовника за його бажанням негайно покинути список розсилки без будь-яких ускладнень. При цьому власне можливість вилучення зі списку не може бути підставою для внесення адрес до списку не за бажанням власників адрес.

1.4. Відправка електронних листів та інших повідомлень, що містять вкладені файли та/або мають значний обсяг, без заздалегідь отриманого дозволу адресата.

1.5. Розсилка (інакше як за прямою ініціативою одержувача):

- електронних листів та інших повідомлень (зокрема одноразових) рекламного, комерційного або агітаційного характеру;
- листів і повідомлень, що містять грубі і образливі вирази і пропозиції;
- розсилка повідомлень, що містять прохання переслати дане повідомлення іншим доступним користувачам (chain letters);
- використання безособових ("ролевих") адрес не за їхнім прямим призначенням, встановленим власником адреси та/або стандартами.

1.6. 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.

1.7. 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 попередньо узгоджене з власниками чи адміністраторами даної конференції.

1.8. Розміщення в будь-якій конференції статті, що містить вкладені файли, окрім випадків, у яких вкладення явно дозволені правилами даної конференції або таке розміщення було попередньо узгоджене з власниками чи адміністраторами конференції.

1.9. Розсилка інформації одержувачам, що раніше висловили небажання одержувати цю інформацію, інформацію цієї категорії або інформацію від цього відправника.

1.10. Використання власних або наданих інформаційних ресурсів (поштових скриньок, адрес електронної пошти, веб-сторінок і т. д.) у якості контактних координат під час здійснення будь-якої з вищеописаних дій незалежно від того, з якої точки Мережі були вчинені ці дії.

1.11. Здійснення діяльності з технічного забезпечення розсилки спаму (spam support service), зокрема:

- цілеспрямоване сканування вмісту інформаційних ресурсів з метою отримання 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 в таку базу даних, явно виразили свою згоду на внесення адрес у цю конкретну базу даних; відкрита публікація адреси такою згодою вважатися не може).

2. ЗАБОРОНА НЕСАНКЦІОНОВАНОГО ДОСТУПУ І МЕРЕЖЕВИХ АТАК

Не допускається здійснення спроб несанкціонованого доступу до ресурсів Мережі, проведення мережевих атак і мережевого злому і участь у них, за винятком випадків, коли атака на мережевий ресурс проводиться з явного дозволу власника або адміністратора цього ресурсу. Зокрема заборонені:

1.1. Дії, спрямовані на порушення нормального функціонування елементів Мережі (комп'ютерів, іншого обладнання або програмного забезпечення), що не належать користувачу.

1.2. 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 користувачу, без узгодження з власниками цього програмного забезпечення або адміністраторами даного інформаційного ресурсу. Під несанкціонованим доступом розуміється будь-який доступ способом, відмінним від ресурсу, що передбачався власником.

1.3. Передача комп'ютерам або обладнанню Мережі безглуздої або непотрібної інформації, що створює паразитне навантаження на ці комп'ютери або обладнання, а також проміжні ділянки мережі в обсягах, що перевищують мінімально необхідні для перевірки зв'язності мереж і доступності окремих її елементів.

1.4. Цілеспрямовані дії зі сканування вузлів мереж з метою виявлення внутрішньої структури мереж, списків відкритих портів і т. п. інакше, ніж у межах, мінімально необхідних для проведення штатних технічних заходів, що не ставлять за мету порушення пунктів 2.1 і 2.2 цього документа.

3. ДОТРИМАННЯ ПРАВИЛ, ВСТАНОВЛЕНИХ ВЛАСНИКАМИ РЕСУРСІВ

3.2. 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 точці підключення до таких ресурсів і є обов'язковими для виконання всіма користувачами цих ресурсів. Правила повинні бути легкодоступними, написаними з урахуванням різного рівня підготовки користувачів.

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

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

3.4. У випадку якщо правила, встановлені власником ресурсу, суперечать тим або іншим пунктам цього документа, щодо цього ресурсу застосовуються правила, встановлені власником, якщо це не спричиняє порушення щодо інших ресурсів.

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

4. НЕПРИПУСТИМІСТЬ ФАЛЬСИФІКАЦІЇ

Значна частина ресурсів Мережі не вимагає ідентифікації користувача і допускає анонімне використання. Проте у деяких випадках від користувача вимагається надати інформацію, що ідентифікує його і використовувані ним засоби доступу до Мережі. 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, під час передавання даних в Мережу.

4.3. Використовувати неіснуючі зворотні адреси під час відправки електронних листів та інших повідомлень.

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

5. НАЛАШТУВАННЯ ВЛАСНИХ РЕСУРСІВ

5.1. Під час роботи 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 із такого налаштування своїх ресурсів, яка перешкоджала б недобросовісному використанню цих ресурсів третіми особами, а за виявлення випадків такого використання – вживати оперативних заходів з їхнього припинення.

5.2. 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 і т. п.);
- загальнодоступні широкомовні адреси локальних мереж, які дозволяють проводити за їхньою допомогою атаки типу smurf;
- електронні списки розсилки з недостатньою надійністю механізму підтвердження передплати або без можливості її скасування;
- web-сайти та інші подібні ресурси, що здійснюють відправку кореспонденції третім особам за анонімним або недостатньо аутентифікованим запитом.