Правила користування

Компанія Jamzo вживає всіх необхідних заходів, щоб і абоненти тарифних планів серії «для дому» і «для бізнесу» отримували якісні сервісні послуги. Мережа Інтернет являє собою глобальне об'єднання комп'ютерних мереж та інформаційних ресурсів, що належать безлічі різних людей і організацій. Це об'єднання є децентралізованим, і єдиного загальнообов'язкового зведення правил (законів) користування мережею Інтернет не встановлено.

Існують, однак, 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 використання будь-яких ресурсів мережі Інтернет визначають власники цих ресурсів і лише вони (тут і далі словом ресурс позначається будь-яка сукупність програмних і апаратних засобів, складових в тому чи 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 тощо)

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

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 фактором. При створенні документа не ставилося за мету формулювати універсальні правила роботи в Мережі, дублювати положення законодавства тих чи 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 виявиться корисною як адміністраторам мереж при розробці правил доступу для користувачів, так і кінцевим користувачам Мережі для уникнення конфліктних ситуацій в 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 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 (спама). 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 одержувачів.
Відкрита публікація адреси електронної пошти або іншої системи персонального обміну інформацією не може служити підставою для включення адреси в який-небудь список для масової розсилки повідомлень. Включення адреси, отриманої будь-яким шляхом (через веб-форму, через підписного робота і т.п.), в список адрес, за яким проводиться будь-яка розсилка, допускається тільки за умови наявності належної технічної процедури підтвердження підписки, яка гарантує, що адреса не потрапить в список інакше, як з волі власника адреси. Процедура підтвердження підписки повинна виключати можливість потрапляння адреси в список адресатів будь-якої розсилки (одноразової або регулярної) за ініціативою третіх осіб (тобто осіб, які не є власниками даної адреси).

Обов'язкова наявність можливості для будь-якого передплатника негайно покинути список розсилки без будь-яких ускладнень при виникненні у нього такого бажання. При цьому наявність можливості покинути список саме по собі не може служити виправданням внесення адрес в список не по волі власників адрес.
1.2. Відправлення електронних листів та інших повідомлень, що містять вкладені файли та / або мають значний об'єм, без попередньо отриманого дозволу адресата.
1.3. Розсилка (інакше як за прямою ініціативою одержувача)
а) електронних листів та інших повідомлень (зокрема одноразових) рекламного, комерційного або агітаційного характеру;
б) листів і повідомлень, що містять грубі і образливі вирази і пропозиції.
в) Розсилка повідомлень, що містять прохання переслати дане повідомлення іншим доступним користувачам (chain letters).
г) Використання безособових (рольових) 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 і 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 узгоджене з власниками чи адміністраторами даної конференції заздалегідь.
1.6. Розміщення в будь-якій конференції статті, що містить прикладені файли, крім випадків, коли вкладення явно дозволені правилами даної конференції або таке розміщення було узгоджене з власниками чи адміністраторами конференції заздалегідь.
1.7. Розсилка інформації одержувачам, 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-якого з вищеописаних дій, незалежно від того, з якої точки Мережі були вчинені ці дії.
1.9. Здійснення діяльності з технічного забезпечення розсилки спаму (spam support service), як то:
- Цілеспрямоване сканування вмісту інформаційних ресурсів з метою збору 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, в явному вигляді виразили свою згоду на включення адрес в дану 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 в них, за винятком випадків, коли атака на мережевий ресурс проводиться з явного дозволу власника або адміністратора цього ресурсу. У тому числі заборонені:
2.1. Дії, спрямовані на порушення нормального функціонування елементів Мережі (комп'ютерів, іншого обладнання або програмного забезпечення), не належать користувачу.
2.2. Дії, спрямовані на отримання несанкціонованого доступу до ресурсу Мережі (комп'ютера, іншого устаткування або інформаційного ресурсу), подальше використання такого доступу, а також знищення чи модифікація програмного забезпечення чи даних, які не належать користувачеві, без узгодження з власниками цього програмного забезпечення чи даних або адміністраторами даного інформаційного ресурсу. Під

несанкціонованим доступом розуміється будь-який доступ способом, відмінним від передбачався власником.
2.3. 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.
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 своєю метою порушення пунктів 2.1 та 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 чи адміністраторами цих ресурсів у точці підключення до таких ресурсів і є обов'язковими до виконання всіма користувачами цих ресурсів. Правила повинні 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 відносно інших ресурсів.
Користувач зобов'язаний дотримуватися правил використання ресурсу або негайно відмовитися 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 веде 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 потрібно 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, використовувані в інших мережевих протоколах, при передачі даних в Мережу.
4.3. Використовувати неіснуючі зворотні адреси при відправці електронних листів і інших повідомлень.
4.4. Недбало ставитися 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 (із приховуванням, таким чином, справжнього джерела дій).

5. Налаштування власних ресурсів
При роботі в мережі Інтернет користувач стає її 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 із такого налаштування своїх ресурсів, яка перешкоджала б недобросовісному використанню цих ресурсів третіми особами, а при виявленні випадків такого використання приймати оперативні заходи по їх припиненню.
Прикладами потенційно проблемної настройки мережевих ресурсів є:
- Відкриті ретранслятори електронної пошти (open SMTP-relays);
- Загальнодоступні для неавторизованої публікації сервери новин (конференцій, груп);

- Кошти, 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 атаки 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.