НКМ-2026

Норми користування Мережею

Чинна редакція документа OFISP-008: ті самі принципи мережевої взаємодії, приведені до сьогоднішніх технологій, загроз і українського правового поля.

ІДЕНТИФІКАТОР **НКМ-2026**	СТАТУС Чинна редакція
РЕДАКЦІЯ 13 вересня 2026	БАЗОВИЙ ТЕКСТ OFISP-008 від 20 вересня 2002
ПІДГОТОВЛЕНО Редакція ofisp.org.ua	МОВА ВИДАННЯ Українська

> Попередня редакція — OFISP-008 (2002) — публікується без змін. Перелік відмінностей — у розділі «Зміни щодо редакції 2002».

Преамбула

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 користування мережею Інтернет не існує.

Існують, проте, загальноприйняті норми роботи в мережі Інтернет, спрямовані на те, щоб діяльність кожного користувача не заважала роботі інших користувачів. Фундаментальне положення цих норм таке: правила користування будь-яким ресурсом мережі Інтернет визначає власник цього ресурсу, і лише він. Тут і далі словом «ресурс» позначається будь-яка сукупність програмних і апаратних засобів, що становить у тому чи іншому значенні єдине ціле; ресурсом можуть вважатися, наприклад, поштова скринька, обліковий запис, пристрій користувача, сервер, хмарний сервіс, локальна мережа, канал зв'язку, вебсайт, спільнота в месенджері чи соціальній мережі і т. п.

Цей документ є формальним описом загальноприйнятих норм мережевої взаємодії, які в більшості мереж вважаються обов'язковими для виконання всіма користувачами. Такі або аналогічні норми застосовуються до всіх доступних мережевих ресурсів, коли правила, встановлені власниками цих ресурсів самостійно, заздалегідь невідомі або встановлені лише частково.

Документ не дублює законодавство і не встановлює нових заборон: він фіксує внутрішньомережеві нормативи, що склалися в міжнародному мережевому співтоваристві як прояв самозбереження мережі Інтернет. Співвідношення цих норм із законодавством України описано в розділі 6.

Ця редакція є осучасненням документа OFISP-008, ухваленого Відкритим форумом інтернет-сервіс-провайдерів 20 вересня 2002 року. Форум припинив діяльність, тому редакцію підготувала й опублікувала редакція сайту ofisp.org.ua. Нумерацію розділів і пунктів збережено: пункт 1.1 базового тексту відповідає пункту 1.1 цієї редакції. Базовий текст 2002 року публікується без змін за адресою ofisp.org.ua/ofisp-008/, і документи, які посилаються саме на нього, можуть продовжувати це робити.

Автори сподіваються, що документ буде корисним як адміністраторам мереж і сервісів під час розроблення правил доступу для користувачів, так і кінцевим користувачам Мережі для уникнення конфліктних ситуацій у повсякденній роботі. Крім того, документ допоможе визначити, якої поведінки слід очікувати 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). Ці правила стосуються будь-якого каналу персонального обміну повідомленнями: електронної пошти, месенджерів, SMS, особистих повідомлень у соціальних мережах, push-сповіщень, коментарів, дзвінків через Мережу. Зокрема, є неприпустимими:

1.1. Масова розсилка повідомлень будь-яким засобом персонального обміну інформацією інакше, ніж за явно і недвозначно вираженою згодою одержувача.

Відкрита публікація адреси електронної пошти, номера телефону чи іншого ідентифікатора не може служити підставою для внесення його до будь-якого списку для масової розсилки. Внесення адреси, одержаної будь-яким шляхом (через вебформу, імпорт контактів, реєстрацію в сервісі і т. п.), до списку, за яким проводиться розсилка, допускається лише за наявності належної технічної процедури підтвердження підписки (double opt-in), яка гарантує, що адреса не потрапить до списку інакше, ніж за бажанням її власника. Попередньо проставлена позначка згоди, згода «за замовчуванням» або згода, отримана як умова доступу до не пов'язаної з розсилкою послуги, підтвердженням не вважається.

Кожен одержувач повинен мати можливість негайно й без ускладнень відмовитися від розсилки: однією дією, без входу в обліковий запис і без пояснення причин. Сама по собі наявність можливості відписатися не може бути підставою для внесення адрес до списку не за бажанням їхніх власників.

1.2. Надсилання електронних листів та інших повідомлень, що містять вкладені файли значного обсягу або посилання на них, без заздалегідь отриманої згоди адресата.

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

a) електронних листів та інших повідомлень (зокрема одноразових) рекламного, комерційного, політичного або агітаційного характеру;

b) листів і повідомлень, що містять грубі та образливі вирази або пропозиції;

c) повідомлень, що містять прохання переслати їх іншим користувачам (ланцюжкових листів);

d) повідомлень на безособові («рольові») адреси на кшталт abuse@, postmaster@, info@ не за їхнім прямим призначенням, встановленим власником адреси та/або стандартами.

1.4. Розміщення в будь-якій спільноті повідомлень, які не відповідають тематиці цієї спільноти (офтопік). Тут і далі під спільнотою розуміються форуми, чати, групи й канали в месенджерах, розділи коментарів, спільноти в соціальних мережах, списки розсилки та інші середовища групового обміну повідомленнями.

1.5. Розміщення в будь-якій спільноті повідомлень рекламного, комерційного або агітаційного характеру, крім випадків, коли такі повідомлення явно дозволені правилами цієї спільноти або їх розміщення було попередньо узгоджене з її власниками чи адміністраторами.

1.6. Розміщення у спільноті вкладених файлів, масових згадок (тегування) учасників або автоматизованих повідомлень (ботів), окрім випадків, у яких це явно дозволене правилами спільноти або було попередньо узгоджене з її власниками чи адміністраторами.

1.7. Надсилання інформації одержувачам, що раніше висловили небажання одержувати цю інформацію, інформацію цієї категорії або інформацію від цього відправника, зокрема тим, хто відписався від розсилки або заблокував відправника.

1.8. Використання власних або наданих ресурсів (поштових скриньок, адрес електронної пошти, номерів телефонів, облікових записів, вебсайтів, посилань 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.

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

- цілеспрямоване сканування вмісту інформаційних ресурсів з метою збирання адрес електронної пошти, номерів телефонів та інших ідентифікаторів служб доставки повідомлень;
- розроблення, розповсюдження або надання в користування програмного забезпечення та інфраструктури для масових розсилок в обхід згоди одержувачів;
- створення, верифікація, підтримка або розповсюдження баз даних адрес чи інших ідентифікаторів (за винятком випадку, коли власники всіх адрес, включених у таку базу, явно виразили згоду на внесення саме до цієї бази; відкрита публікація адреси такою згодою вважатися не може);
- масове створення або продаж облікових записів для розсилок, а також обхід засобів захисту від спаму (обмежень частоти надсилання, перевірок «я не робот», репутаційних фільтрів).

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 або перевірка захищеності мережевого ресурсу проводиться з явного, бажано письмового, дозволу власника або адміністратора цього ресурсу і в межах, ним визначених. Зокрема заборонені:

2.1. Дії, спрямовані на порушення нормального функціонування елементів Мережі (пристроїв, іншого обладнання, програмного забезпечення або сервісів), що не належать користувачу, зокрема атаки на відмову в обслуговуванні (DoS, DDoS) будь-яким способом, а також участь у таких атаках, у тому числі через надання власних ресурсів для їх проведення.

2.2. Дії, спрямовані на отримання несанкціонованого доступу до ресурсу Мережі (пристрою, іншого обладнання, облікового запису або інформаційного ресурсу), подальше використання такого доступу, а також знищення, модифікація, шифрування або витік програмного забезпечення чи даних, що не належать користувачу, без узгодження з власниками цього програмного забезпечення чи даних або адміністраторами даного інформаційного ресурсу. Під несанкціонованим доступом розуміється будь-який доступ способом, відмінним від того, що передбачався власником ресурсу, зокрема через підбір або використання чужих паролів, ключів і сесій, експлуатацію вразливостей, обхід автентифікації.

2.3. Передача пристроям або обладнанню Мережі безглуздої або непотрібної інформації, що створює паразитне навантаження на ці пристрої 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 зі сканування вузлів мереж з метою виявлення внутрішньої структури мереж, списків відкритих портів, версій програмного забезпечення, облікових записів 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.

2.5. Створення, розповсюдження або застосування шкідливого програмного забезпечення (вірусів, троянських і шпигунських програм, програм-вимагачів, засобів прихованого майнінгу і т. п.), керування зараженими пристроями (ботмережами), а також розміщення ресурсів, призначених для зараження пристроїв користувачів або для керування шкідливим програмним забезпеченням.

2.6. Перехоплення, підміна або втручання в чужі з'єднання і трафік без згоди їхніх учасників, зокрема підміна відповідей DNS, маршрутів або мережевих адрес, впровадження у з'єднання (атаки «людина посередині»), а також перехоплення чужих облікових даних.

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 у точці доступу до таких ресурсів (на вебсайті, в умовах надання послуги, у правилах спільноти) і є обов'язковими для виконання всіма користувачами цих ресурсів. Правила повинні бути легкодоступними, написаними з урахуванням різного рівня підготовки користувачів; про зміни правил користувачів повідомляють заздалегідь.

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 цього ресурсу застосовуються правила, встановлені власником, якщо це не спричиняє порушення щодо інших ресурсів.

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. Анонімність сама по собі не є порушенням; порушенням є фальсифікація. Користувач не повинен:

4.1. Використовувати ідентифікаційні дані (імена, адреси, телефони, облікові записи, домени, логотипи і т. п.) третіх осіб, крім випадків, коли ці особи уповноважили користувача на таке використання, а також видавати себе за іншу особу, організацію, сервіс або посадову особу, зокрема з метою виманювання облікових даних чи платежів (фішинг).

4.2. Фальсифікувати свою IP-адресу, а також адреси та ідентифікатори, що використовуються в інших мережевих протоколах, під час передавання даних в Мережу, зокрема адресу й домен відправника електронної пошти, номер телефону, що відображається під час дзвінка чи в SMS, ідентифікатори пристрою.

4.3. Використовувати неіснуючі або чужі зворотні адреси під час відправлення електронних листів та інших повідомлень.

4.4. Недбало ставитися до конфіденційності власних ідентифікаційних реквізитів (зокрема, паролів, ключів доступу, кодів двофакторної автентифікації, сесійних токенів та інших кодів авторизованого доступу), у тому числі передавати їх третім особам, що може призвести до використання тих або інших ресурсів третіми особами від імені даного користувача (із приховуванням, таким чином, справжнього джерела дій).

4.5. Створювати або використовувати підставні облікові записи та автоматизовані засоби для імітації дій багатьох осіб (накрутка, координована неавтентична поведінка) з метою спотворення оцінок, рейтингів, голосувань чи публічного обговорення.

5. Налаштування власних ресурсів

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, яке перешкоджало б недобросовісному використанню цих ресурсів третіми особами, а за виявлення випадків такого використання – вживати оперативних заходів з їхнього припинення.

Прикладами потенційно проблемного налаштування мережевих ресурсів є:

— відкриті ретранслятори електронної пошти (open relay) і поштові сервери, що приймають пошту від будь-кого без автентифікації;

— відкриті рекурсивні DNS-резолвери, сервери NTP, SNMP, memcached та інші служби, придатні для посилення (ампліфікації) атак на третіх осіб;

— відкриті проксі-сервери, VPN-вузли та інші засоби, що дозволяють третім особам неавторизовано приховати джерело з'єднання;

— маршрутизатори, камери, «розумні» пристрої та інше обладнання із заводськими або слабкими паролями, без оновлень безпеки або з інтерфейсом керування, відкритим у Мережу;

— бездротові мережі без шифрування або із застарілими протоколами захисту (WEP, WPA першої версії);

— пристрої, скомпрометовані шкідливим програмним забезпеченням, що беруть участь у ботмережах;

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

— вебсайти, форми та програмні інтерфейси, що здійснюють відправлення повідомлень третім особам за анонімним або недостатньо автентифікованим запитом;

— загальнодоступні сховища даних (хмарні сховища, бази даних, резервні копії) без контролю доступу, які містять чужі персональні дані.

Власник мережі, сервісу або домену повинен підтримувати доступний канал для повідомлень про зловживання (адресу abuse@ або її аналог, зазначений у реєстраційних даних) і реагувати на обґрунтовані звернення в розумний строк.

---

6. Співвідношення із законодавством

Ці норми є саморегулюванням мережевого співтовариства і не замінюють законодавства. При цьому:

6.1. Ці норми не скасовують і не обмежують вимог законодавства України, зокрема законів «Про електронні комунікації», «Про захист персональних даних», «Про захист суспільної моралі», «Про авторське право і суміжні права», а також положень Кримінального кодексу України про кримінальні правопорушення у сфері використання комп'ютерів, систем і мереж. У разі розбіжності між нормою цього документа і законом застосовується закон.

6.2. Обіг інформації, поширення якої заборонене законом (заклики до насильства, тероризм, виправдовування збройної агресії проти України, порушення суспільної моралі, дискримінація і т. п.), не є предметом цих норм: його регулюють закон і правила власників ресурсів. Водночас використання Мережі для поширення такої інформації провайдери й власники ресурсів зазвичай прирівнюють до порушення правил надання послуг.

6.3. Дотримання цих норм не звільняє від відповідальності за законом, а їх порушення може бути підставою для обмеження доступу до ресурсу його власником незалежно від того, чи є діяння правопорушенням за законом.

Зміни щодо редакції 2002

Нумерацію розділів і пунктів базового тексту OFISP-008 збережено; нові пункти додано в кінець розділів. Нижче перелічено, що саме змінено.

Преамбула. Оновлено приклади ресурсу (обліковий запис, хмарний сервіс, спільнота). Додано абзац про статус редакції та про те, що базовий текст 2002 року публікується без змін за окремою адресою.

Розділ 1. Перелік каналів спаму розширено з електронної пошти, SMS та IRC до месенджерів, соціальних мереж, push-сповіщень і коментарів (вступ, п. 1.1). У п. 1.1 уточнено, що не вважається згодою, і додано вимогу відписки однією дією. Поняття «телеконференції Usenet» замінено на «спільноту» (п. 1.4). У п. 1.6 замість вкладень у групи новин — файли, масові згадки й боти у спільнотах. У п. 1.9 додано масове створення облікових записів та обхід засобів захисту від спаму.

Розділ 2. У вступі уточнено, що перевірка захищеності допускається лише з дозволу власника і в його межах. П. 2.1 явно називає атаки на відмову в обслуговуванні та участь у них; п. 2.2 — підбір паролів, експлуатацію вразливостей, обхід автентифікації, шифрування даних. У визначенні несанкціонованого доступу виправлено перекладацьку помилку. Додано п. 2.5 (шкідливе програмне забезпечення, ботмережі) і п. 2.6 (перехоплення та підміна трафіку).

Розділ 3. Уточнено, де публікуються правила (вебсайт, умови надання послуги, правила спільноти), і додано вимогу повідомляти про їх зміни заздалегідь. Суть розділу без змін.

Розділ 4. До п. 4.1 додано видавання себе за іншу особу чи сервіс (фішинг); до п. 4.2 — підміну відправника пошти та номера телефону; до п. 4.4 — коди двофакторної автентифікації, сесійні токени й передавання реквізитів третім особам. Додано п. 4.5 про підставні облікові записи та накрутку.

Розділ 5. Приклади 2002 року (відкриті сервери новин, smurf-атаки на широкомовні адреси) замінено сучасними: служби, придатні для ампліфікації атак, пристрої із заводськими паролями, незахищені бездротові мережі, скомпрометовані пристрої, відкриті сховища даних. Додано вимогу мати канал для повідомлень про зловживання.

Розділ 6. Новий розділ про співвідношення норм із законодавством України.

Правопис. Написання приведено до чинного правопису: «вебсайт», «вебформа», «автентифікація».

НКМ-2026 — Норми користування Мережею. https://ofisp.org.ua/