

## СУЧАСНІ МЕТОДИ БОРОТЬБИ ЗІ СПАМОМ

Є. А. Носков<sup>1</sup>, М. В. Коломицев<sup>1</sup>

<sup>1</sup>Національний технічний університет України «Київський політехнічний інститут»

### Анотація

В роботі розглядаються основні методи і правила для ефективної боротьби зі спамом. Описуються методи фільтрації поштових повідомлень як на стороні сервера, так і на стороні клієнта. Пропонуються варіанти протидії способам обходу методів фільтрації і захисту від рекламних повідомлень.

**Ключові слова:** спам, методи фільтрації, електронна пошта

### Вступ

СПАМ – це анонімна масова розсилка небажаної інформації людям, які не висловили бажання її отримувати, та не потребують її. Кількість користувачів в мережі Інтернет з кожним роком збільшується, в 2014 році – 3,01 мільярда, а в 2015 році вже 3,2 мільярда користувачів Інтернет [1]. Це пов'язано з багатьма факторами, такими як здешевлення обладнання (як результат – ціна доступу до мережі знижується), активне поширення планшетних комп'ютерів і смартфонів (користувачі мобільного інтернету).

Частка спаму в світовому трафіку становить майже 60 % за 2015 рік. На зростання спаму вплинула масова поява незахищених сайтів і форумів. Також люди, які розсилають спам, почали активно використовувати нелегальні методи, такі, як злом сайтів, зараження комп'ютерів користувачів для створення комп'ютерів-зомбі (заражених комп'ютерів і серверів, які використовуються зловмисниками з метою нанесення шкоди) для розсилки спаму. Значне зростання спровокувало також збільшення трафіку з Китаю – це пов'язано з просуванням підробок відомих брендів. З ростом популярності сервісів миттєвих повідомлень і соціальних мереж зростає кількість спаму в даних сервісах. Також відзначається зростання спаму в sms-повідомленнях.

### 1. Основні загрози від спаму

В наш час, можна виділити такі основні загрози від спаму:

- Навантаження комунікацій. Спам забиває канали зв'язку, створює трафік, оплачувати який доводиться або провайдеру, або користувачу.
- Втрата часу. Якщо спам дістався до кінцевої пошти, то її власник буде змушений вручну видаляти спам з пошти, а це призводить до значної втрати робочого часу.
- Невдоволення та роздратування. Видаляючи спам, користувач по суті займається видаленням сміття, що не входить до його обов'язків. Це не може його не дратувати.

- Втрата потрібного електронного листа. Часто серед спаму дуже важко, а іноді майже неможливо відшукати необхідний нам лист.
- Поширення програм-вірусів з потенційно небезпечними наслідками, здатними пошкодити комп'ютер або цілу мережу, знищити або викрасти інформацію, зупинити роботу організації.
- Щорічно зростає криміналізація спаму. Цьому сприяє анонімність спам-розсилки, так створюється помилкове враження повної безкарності, що є абсолютно неправдою.
- Потрапляння облікових даних користувача в базу розсилки спаму і подальше несанкціоноване використання цієї адреси.
- Втрата ділової репутації. Звичайно, за короткий проміжок часу репутацію компанії зруйнувати дуже складно. Але якщо не реагувати на спам-рекламу, розіслану недобросовісними партнерами або працівниками, і на спам-розсилки, спрямовані проти компанії або її клієнтів, в довгостроковій перспективі репутація може серйозно постраждати.

Все це призводить до фінансових втрат як організації, так і державних установ.

### 2. Методи боротьби зі спамом

Серед методів боротьби зі спамом немає методу, який гарантовано вирішує проблему спаму. Кожен метод має свої переваги і недоліки.

Тому, для ефективної протидії поширенню спаму необхідне об'єднання різних зусиль – технологічних (виробництво програмного забезпечення), політичних (прийняття законів), організаційних (правила використання email-адресів в Інтернеті) і соціальних (допомога суспільства).

#### 2.1. Організаційні методи

Найнадійніший метод боротьби зі спамом – це не допустити, щоб спамери дізнались вашу електронну адресу, проте досягти цього дуже важко. Існують такі методи які допоможуть вам у цьому:

- 1) Не реєструватись на ненадійних сайтах та службах. Якщо ж ситуація вимагає реєстрації, то можна створити спеціальну пошту, для реєстрації на таких сайтах та службах. Також можна використовувати спеціальні служби, що видають одноразові адреси електронної пошти, для використання у сумнівних ситуаціях.
- 2) Не залишати електронну адресу в групах чи на веб-сайтах. Якщо ж цього досягти не можливо і адресу доводиться залишати, то рекомендовано її видозмінити. Існують такі варіанти видозмінення електронної адреси:

- Перетворення адреси в картинку. Скріншот електронної адреси виставляється як контактна інформація на сайті замість текстового еквівалента. Користувач без проблем прочитає адресу що подана на картинці, проте спамерська програма-робот, що збирає електронні адреси – ні.
- Маскування адреси. Перший варіант маскування адреси полягає у додаванні сторонніх символів у адресу, наприклад, замість `user@domain.com` ми отримаємо `u_s_e_r_(a)_d_o_m_a_i_n_.c_o.m`. Іншим варіантом маскування являється прописання назв символів, наприклад, замість `ivan.ivanov@domain.com` отримуємо `ivan(dot)ivanov(at)domain(dot)com`. Проте, слід пам'ятати, що в найпростіших випадках замасковану адресу зможе розпізнати і програма-робот.

Головним недоліком видозмінення електронних адреси є те, що воно ускладнює доступ до поштової адреси реальним користувачам.

- 3) Необхідно обирати надійне ім'я електронної пошти. При створенні електронної пошти, необхідно, по можливості обирати максимально довге та незручне для вгадування ім'я, ще краще аби воно не мало жодного сенсу. Використання букв з різних алфавітів і цифр також значно ускладнить задачу спамерам. Однак усі ці методи проти вгадування ім'я електронної пошти мають значний недолік. Ускладнюючи ім'я, ми ускладнюємо його не лише для спамерів, а й для самих себе і інших користувачів. А якщо йдеться про ім'я електронної пошти якоїсь компанії, то хочеться щоб воно було простим, зрозумілим і легко запам'ятовувалось.
- 4) Ігнорувати та не відповідати на спам, не переходити за посиланнями в ньому, навіть якщо сказано що перейшовши за посиланням можна відмовитись від підписки. Цим ви підтвердите, що використовуєте свою електронну пошту і отримуватимете ще більше спаму.
- 5) Забороняти завантаження картинок. Зазвичай, якщо в отриманому листі містяться картинки, то поштовий клієнт робить запит на дозвіл їх завантаження. Рекомендується забороняти завантаження картинок, від ненадійних відправників, адже якщо користувач завантажує картинку, це означає, що

поштова адреса використовується. Іншими словами, сам факт завантаження картинок, вкладених у лист використовується для перевірки того, чи є електронна адреса активною, чи ні.

## 2.2. Соціальні методи

До соціальних методів боротьби можна віднести ті методи, які здатне здійснювати саме суспільство. До них входять:

- 1) Пропаганда. Спроба пояснити людям, а саме спамерам, що спам має негативний вплив.
- 2) Ідеологія. Очевидним фактом є те, що спам приносить певну матеріальну вигоду його замовникам. Виходячи з цього, можна зробити висновок, що недовлячись на всі негативні фактори спаму, деякі користувачі все ж таки використовують послуги, прорекламовані у спамі. Спам існуватиме до тих пір, поки дохід від спаму перевищує затрати на нього. Тобто одним із найдієвіших методів боротьби зі спамом є його ігнорування та відмова від послуг, прорекламованих в спамі.
- 3) Громадський осуд. Існує практика застосування громадського осуду, щодо осіб, які використовують прорекламовані у спамі послуги.
- 4) Допомога свідомих користувачів. Для цього користувач повинен виконати такі дії:
  - Визначити з якого саме поштового хостингу прийшло спам-повідомлення. Для цього досить поглянути на заголовки електронного листа From – там буде вказано IP-адреса та ім'я хоста відправника.
  - У разі якщо мова йде про великий поштовий хостинг: сервіс безкоштовної пошти з доброю репутацією, або про великий комерційний хостинг-провайдер має сенс перейти до наступного пункту, якщо ж спам поширює невеликий провайдер домашніх мереж – витрачати час на написання їм листів не слід.
  - Знайти на сайті оператора поштового хостингу форму зворотнього зв'язку або адресу електронної пошти для повідомлення про спам-розсилку.
  - Написати повідомлення про факт розсилки спаму службі підтримки. При цьому необхідно вказати вихідний текст повідомлення з усіма службовими заголовками (це допоможе знайти спамера або хоча б запобігти поточну розсилку спаму) і свої контактні дані (це чисто психологічно простимулює службу підтримки для якнайшвидшого розгляду іменованого, а не анонімного звернення).
  - Чекати отримання підтвердження про отримання повідомлення про спам-інцидент: більшість серйозних провайдерів поштового хостингу мають trouble ticket систему, яка в автоматичному режимі присвоїть унікальний номер заявці в службу підтримки і повідомить ініціатора про хід її рішення.

## 2.3. Технічні методи боротьби зі спамом

В результаті проведеного аналізу існуючих методів технічного захисту авторами обрано набір методів, найбільш ефективно фільтруючих спам при їх комплексному застосуванні.

Існують два основні технічні методи захисту від спаму: фільтрація надходження спаму на стороні сервера і на стороні клієнта.

### 2.3.1. Фільтрація спаму на стороні сервера

**Чорні списки** Вони ж DNSBL (DNS-based Blackhole Lists) [2]. Це один з найстаріших методів боротьби зі спамом. Принцип його роботи полягає у занесення до чорних списків IP-адресів комп'ютерів, з яких ведеться розсилання спаму.

Переваги: Чорні списки повністю відсікають пошту від ненадійних джерел.

Недоліки:

- 1) Високий рівень помилок.
- 2) За час, поки спамерів занесуть до чорного списку, вони встигають знаходити нові комп'ютери.
- 3) Кілька комп'ютерів, з яких відправляють спам, можуть скомпрометувати весь поштовий домен і багато користувачів не зможуть надсилати пошту на сервер, який використовує даний чорний список.

**Сірі списки** Принцип дії сірих списків базується на тактиці розсилки спаму, який як правило, розсилається в дуже короткий час.

Робота сірого списку полягає в навмисній затримці листів на деякий час. При цьому адреса і час пересилки заноситься в базу даних сірого списку. Якщо віддалений комп'ютер є справжнім поштовим сервером, то він повинен зберегти лист в черзі і повторювати пересилання протягом п'яти днів [3].

Спам-боти, як правило, листів в черги не зберігають, тому через нетривалий час, припиняють спроби переслати лист. Експериментальним шляхом встановлено, що в середньому час розсилки спаму складає трохи більше години. Якщо з моменту першої спроби пройшла необхідна кількість часу, то при повторному пересиланні листа з цієї ж адреси ваш поштовий сервер прийме його. При цьому IP-адреса поштового сервера-відправника, електронні адреси відправника і одержувача будуть внесені до білого списку на досить тривалий час, після чого листи будуть прийматись без затримок.

Переваги:

- 1) Сірі списки дозволяють відсіяти до 90 % спаму, при цьому ризик втрати важливих листів надзвичайно малий.
- 2) Налаштування сірих списків не потребує значної праці адміністратора сервера-отримувача.
- 3) Користувач не повинен нічого налаштовувати чи «навчати» систему.

Недоліки:

- 1) Можливість помилкового відсіювання листів з серверів, що не виконують рекомендації протоколу SMTP.
- 2) Затримка при доставці пошти може досягати години (можливо й довше), що є неприйнятним для багатьох користувачів.
- 3) Спамери можуть легко вдосконалювати свої програми, оскільки реалізація підтримки повторного надсилання повідомлення не є важким завданням.

**Перевірка адреси відправника** Приблизно 50 % спаму надходить із зазначенням неіснуючої адреси відправника. За замовчуванням поштові сервери визначають лише IP-адресу сервера, на якому нібито розташований електронний ящик відправника. Повна перевірка адреси відправника полягає в тому, що поштовий сервер користувача встановлює з'єднання з віддаленим поштовим сервером і починає діалог. Дійшовши до фази RCPT TO: і отримавши відповідь, поштовий сервер користувача має інформацію про наявність або відсутність адреси відправника.

Установка зворотних з'єднань і є слабким місцем перевірки адреси відправника. Зловмисник може змусити сервер користувача встановлювати величезну кількість з'єднань і викликати відмову в обслуговуванні. Тому фільтр, який виконує перевірку адреси відправника, не повинен використовуватися самостійно.

Переваги:

- 1) Один з найбільш ефективних фільтрів.
- 2) У випадку налаштування поштового сервера на ретрансляцію пошти всередину мережі, звіти про недоставлених повідомленнях будутьходити відправнику, а не надсилатися на локальний ящик.

Недоліки:

- 1) Багато автоматичних розсилок ведуться з неіснуючих адрес і не приймаються сервером.
- 2) Фільтр не повинен використовуватися самостійно: це робить поштову систему вразливою до DOS-атак.

### 2.3.2. Фільтрація спаму на стороні клієнта

**Фільтр Баєса** Метод фільтрації спама, в основі якого лежить застосування теореми Баєса. При навчанні фільтра, для кожного зустрінутого в повідомленнях слова розраховується і зберігається його «вага» – оцінка ймовірності того, що лист з цим словом – спам. У найпростішому випадку в якості оцінки використовується частота: «появ в спамі/появ всього». Фільтри Баєса не потребують постійних налаштувань, достатньо лише попередньо обучити фільтр. Після цього фільтр підлаштовується під тематику листів, типові для даного конкретного користувача. Переваги:

- 1) Ефективність для індивідуальної пошти (після навчання на досить великій вибірці відсікає до 95-97 % спаму, і в разі будь-яких помилок його можна довчити) [4]. Загалом, є всі показання

для його повсюдного використання, що і має місце на практиці – на його основі побудовані практично всі сучасні спам-фільтри.

- 2) Даний метод зручний, має індивідуальне налаштування.

Недоліки:

- 1) Метод працює тільки з текстом. Знаючи про це, спамери почали вкладати рекламну інформацію в картинку.
- 2) Не ефективний для корпоративної пошти.

**Контентна фільтрація** Метод полягає у перевірці повідомлення на наявність притаманних спаму слів, фрагментів тексту, картинок. В результаті аналізу можна підрахувати «спамерську вагу» повідомлення.

Переваги:

- 1) Гнучкість, можливість швидкого налаштування.
- 2) Помилки з розмежуванням спаму і нормальних повідомлень трапляються дуже рідко.

Недоліки:

- 1) Оскільки налаштуванням спам-фільтрів займаються цілі антиспам-лабораторії, то й вартість даних спам-фільтрів відповідна.
- 2) Спамери винаходять нові способи обходу цього методу – додають в спам випадковий «шум», тим самим ускладнюючи пошук спамерських характеристик у повідомленні.

### 2.3.3. Додаткові методи захисту

**Контроль масовості** Даний метод базується на виявленні в поштовому потоці масових повідомлень, які є абсолютно однаковими або відрізняються несуттєво. Щоб створити ефективний «масовий» аналізатор необхідні великі обсяги поштових повідомлень. Саме тому, даний метод пропонують великі виробники, що володіють величезними потоками пошти, яку можна піддати аналізу.

Переваги: При спрацюванні методу, гарантовано буде виявлено масову розсилку.

Недоліки:

- 1) Існують випадки, коли «велика» розсилка не являється спамом.
- 2) Спамери навчилися проходити такий захист за допомогою програм, які генерують різний кон-

тент у кожному спам-повідомленні, в результаті контроль масовості не спрацьовує.

## Висновки

В даній роботі, авторами запропоновані правила поведінки і технічні рішення, комбінація яких дасть значне зниження небажаних повідомлень, а також знизить навантаження на сервера і мережевий трафік, і не буде віднімати час у користувачів.

Проте, враховуючи те, що спам приносить вигоду замовникам, сподіватись на його зникнення найближчим часом не варто. Якщо підприємці будуть далі замовляти розсилку спаму, а користувачі відгукуватися на рекламні повідомлення, попит буде рости і обсяг спаму також буде збільшуватися.

Виконання простих правил поведінки в мережі Інтернет може значно знизити обсяг одержуваного спаму, тому можна стверджувати, що багато чого залежить від самого користувача. І за ним стоїть вибір, слідувати цим правилам чи ні.

Використання спеціального програмного забезпечення і методів підвищує ефективність фільтрації повідомлень. Але, як правило, всі методи вимагають постійного удосконалення, тому що практично всі, хто займається розсилкою спаму, вдосконалюють методи обходу систем захисту. Також бажано постійно проводити навчання систем для підвищення їх ефективності.

Не варто забувати про юридичні аспекти – в деяких країнах прийняті закони про кримінальну відповідальність за розсилку спаму.

## Перелік використаних джерел

1. Sanou Brahim. ICT Data and Statistics Division. — 2015. — P. 1–3.
2. Schryen Guido. Anti-Spam Measures: Analysis and Design. — Aachen : Springer, 2007. — P. 61–70.
3. Tan Ying. Anti-Spam Techniques Based on Artificial Immune System. — Boca Raton : CRC Press, 2016. — P. 5–7.
4. Zdziarski Jonathan A. Ending Spam: Bayesian Content Filtering and the Art of Statistical Language Classification. — San Francisco : No Starch Press, 2005. — P. 48–50.