**УДК 004.056.53**

***магістр О.І. Дмитрук, ст. викладач С.О. Галушко***
*ДВНЗ «Національний гірничий університет»*

# ФІЛЬТРАЦІЯ ЕЛЕКТРОННОЇ ПОЧТИ ВІД СПАМУ

*В даній статті йде мова про спам та захист від нього з допомогою фільтрації електронної почти. Розглядаються такі методи фільтрації, як чорні списки, авторизація поштових серверів, сірі списки, статистичні методи фільтрації спаму та декілька інших.*

Спам (англ. spam) – масова розсилка кореспонденції рекламного чи іншого характеру людям, які не висловили бажання її одержувати. Передусім термін «спам» стосується рекламних електронних листів.

В даний час використовується кілька методів фільтрації електронної пошти:

*Чорні списки*

У чорні списки [1] заносяться IP-адреси комп'ютерів, про які відомо, що з них ведеться розсилання спаму. Також широко використовуються списки комп'ютерів, які можна використовувати для розсилання – «відкриті релеї» і «відкриті проксі», а також – списки «dial-up» – клієнтських адрес, на яких не може бути поштових серверів. Можна використовувати локальний список або список який підтримує хтось інший. Завдяки простоті реалізації, широке поширення одержали чорні списки, запит до яких здійснюється через службу DNS. Вони називаються DNSBL (DNS Black List). В даний час цей метод не дуже ефективний. Спамери знаходять нові комп'ютери для своїх цілей швидше, ніж їх встигають заносити в чорні списки. Крім того, кілька комп'ютерів, що відправляють спам, можуть скомпрометувати весь поштовий домен і тисячі законослухняних користувачів на невизначений час будуть позбавлені можливості відправляти пошту серверам, що використовують такий чорний список.

*Авторизація поштових серверів*

Були запропоновані різні способи для підтвердження того, що комп'ютер, що відправляє лист, дійсно має на це право (Sender ID, SPF, Caller ID, Yahoo DomainKeys), але вони поки не розповсюджені.

*Сірі списки*

Метод сірих списків базується на тому, що «поведінка» програмного забезпечення, призначеного для розсилання спаму відрізняється від поведінки звичайних поштових серверів, а саме, спамерські програми не намагаються повторно відправити лист при виникненні тимчасової помилки, як того вимагає протокол SMTP.

Спочатку всі невідомі сервери заносяться в "сірий список" і листи від них не приймаються. Серверові відправника повертається код тимчасової помилки, тому, звичайні листи (не спам) не втрачаються, а тільки затримується їхня доставка (вони залишаються в черзі на сервері відправника і доставляються при наступній спробі). Якщо сервер поводиться так, як очікувалося, він автоматично переноситься в білий список і наступні листи приймаються без затримки.

Цей метод на даний час дозволяє відсіяти до 90 % спаму, практично без ризику втратити важливі листи. Однак він теж не бездоганний.

– Можуть помилково відсіватися листи з серверів, які не виконують рекомендації протоколу SMTP, наприклад, розсилки з сайтів новин;

– Затримка при доставці листа може досягати півгодини (а іноді й більше), що неприйнятно для термінової кореспонденції. Цей недолік компенсується тим, що затримка вноситься тільки при відправці першого листа з раніше невідомої адреси;

– Великі поштові служби використовують кілька серверів, з різними IP-адресами, більш того, можлива ситуація, коли кілька серверів по-черзі намагаються відправити той самий лист. Це може привести до дуже великих затримок при доставці листів;

– Спамерські програми можуть удосконалюватися. Підтримка повторної посилки повідомлення реалізується досить легко і цілком нівелює даний вид захисту.

*Статистичні методи фільтрації спаму*

Ці методи [2] використовують статистичний аналіз змісту листа для прийняття рішення, чи є він спамом. Найбільшого успіху удалося досягти за допомогою алгоритмів, заснованих на теоремі Байеса. Для роботи цих методів

потрібно «навчання» фільтрів, тобто потрібно використовувати розсортовані вручну листи для виявлення статистичних особливостей нормальних листів і спаму. Після навчання на досить великій вибірці, вдається розпізнати до 95-97 % спаму.

*Інші методи*

– Жорсткі вимоги до листів і відправників, наприклад відмова прийому листів із заздалегідь неправильною зворотною адресою (листи, з неіснуючих доменів), перевірка доменного імені за IP-адресою комп'ютера, з якого прийшов лист тощо Дані заходи застаріли, відсівається тільки найпримітивніший спам – невелика кількість повідомлень. Але не нульова, тому застосування все ще має сенс;

– Системи типу Виклик-Відповідь;

– Настроювання вибіркового скачування листів у TheBat «на льоту».

**Перелік літератури:**

1. http://best-free-soft.at.ua/publ/spam_vidi_spamu_i_borotba_zi_spamom/1-1-0-33.
2. http://uk.wikipedia.org/wiki/%D1%EF%E0%EC.