УДК 004.773.3

Загороднюк С.П.[1], к.ф.-м.н
Мар'яновський В.А.[1], к.т.н
Олейніков А.Ю.[1],
Циба А.В.[1]

Моніторинг фактів перебування серверів електронної пошти підприємства у чорних списках

[1] Київський національний університет імені Тараса Шевченка, 03680, м. Київ, пр-т. Глушкова 4г, e-mail: kola@univ.net.ua

S.P. Zagorodniuk [1], PhD
V.A. Marianovskyi [1], PhD
O.Y. Oleynikov[1],
O.V. Tsyba[1]

Monitoring the facts of finding enterprise E-mail servers in the DNS blacklist servers

[1] Taras Shevchenko National University of Kyiv, 03680, Kyiv, Glushkova st., 4g, e-mail: kola@univ.net.ua

В статті розглядається програмна реалізація моніторингу фактів перебування поштових серверів підприємства в централізованих всесвітньо доступних сховищах негативної інформації про джерела поширення небажаних повідомлень і своєчасного сповіщення адміністратора. Крім того, стаття пропонує алгоритм пошуку джерел розсилки повідомлень, які своєю поведінкою демонструють бажання відгадати або підібрати адресу електронної пошти користувача і направити йому потік небажаних повідомлень. Представлено результати тестування і впровадження програмної служби в мережі Київського університету імені Тараса Шевченка.

Ключові слова: електронна пошта, служба SMTP, RBL-сервер, DNSBL-сервер, небажані повідомлення.

The article discusses the software implementation to monitor the facts of finding E-mail servers in the centralized global storage of negative information about the sources of the unwanted messages spread. The the comparative characteristics of the most popular and relevant world-wide DNSLB servers are given and the procedure of urgent admin notification via short message services is described in detail. In addition, the article offers algorithm to search the sources whose behavior demonstrated a willingness to guess or pick up E-mail address of the user and send him a stream of unwanted messages. The results of the testing and deployment of software service in a network of Kyiv Taras Shevchenko National University are also present in the article.

Key Words: E-mail, SMTP service, RBL server, DNSBL server, unwanted messages.

Статтю представив д.т.н., проф. Погорілий С.Д.

Поширення небажаних повідомлень рекламного або непристойного змісту є глобальною загальносвітовою проблемою використання електронної пошти та систем миттєвих повідомлень. Незважаючи на серьйозний прогрес [1] у подоланні цієї проблеми, вона залишається далекою від її остаточного вирішення [2]. Головною причиною цього явища є комерційний інтерес системних адміністраторів, які володіють потужними обчислювальними кластерами поштових серверів і пропонують послуги такого агресивного рекламного бізнесу.

Головними споживачами таких послуг, як це не парадоксально, є підприємства, що ведуть цілком законну діяльність і легальний бізнес, але при цьому не нехтують дешевою рекламою своїх товарів або послуг, яка поширюється на велике коло потенційних клієнтів. При цьому небажані повідомлення можуть насторожити і відвернути певну частину потенціальних клієнтів, але на практиці на це не звертають увагу рекламодавці. Інший прошарок споживачів - це компанії та фізичні особи, які пропонують нелегальні товари або послуги, адже пропонувати ці товари і послуги у більш відкритий спосіб неетично або небезпечно [3].

Очевидно, що адміністратор системи електронної пошти повинен захищати користувачів своєї поштової системи від повені небажаних повідомлень. Для цього він може використовувати стандартні загальноприйняті

фільтри небажаних повідомлень [4], або, крім того, розробити і впровадити свої власні фільтри. Але для адміністратора не менш важливою задачею також є постійний контроль за тим, щоб повідомлення електронної пошти, сформовані користувачами його власної поштової системи були успішно доставлені до користувачів інших поштових систем і не були при цьому розпізнані фільтрами цих віддалених поштових систем як небажані. Для досягнення цієї мети адміністратору потрібно знати принципи роботи основних стандартних фільтрів і постійно виконувати умови, які він нього вимагають ці фільтри.

Вищезгаданий глобальний характер проблеми змушує фахівців з різних країн світу об'єднатись і спільно її вирішувати. Коли адміністратор поштової системи фіксує систематичну розсилку небажаних повідомлень з конкретного вузла або мережі, у нього виникає природнє і свідоме бажання попередити про цю небезпеку не тільки своїх знайомих колег, але й адміністраторів інших країн, які потенційно також можуть стати об'єктом зловмисників.

Очевидно, що найкращим способом організації такої співпраці є створення центрального загальнодоступного глобального сховища для накопичення негативної інформації про вузли і мережі як джерела поширення небажаних повідомлень. Дійсно, такі інформаційні сховища створені і називаються «чорними списками», RBL серверами (англ. Realtime Black List - чорний список, що змінюється в реальному часі) або DNSBL-серверами (англ. DNS Black List - DNS-сервер в ролі чорного списку) [2-4].

Остання назва пов'язана з тим, що для перевірки факту перебування того чи іншого вузла в чорному списку поштовий адміністратор або його фільтруюче програмне забезпечення повинні надіслати до служби DNS (англ. Domain Name System - система доменних імен [1,2]) спеціалізований DNS-запит і дочекатись на нього відповідь. Період часу між DNS-запитом і DNS-відповіддю складає, як правило від 0 до 3 секунд. Коли сервер поштової системи відправника встановлює сеанс зв'язку з приймаючим сервером поштової системи отримувача, саме в цей час приймаючому серверу слід виконати цей DNS-запит до DNSBL-сервера і перевірити факт перебування сервера-відправника в чорному списку. Якщо в результаті DNS-запита з'ясовується, що сервер-відправник перебуває в чорному списку, приймаючий сервер може зробити вигляд, що нічого особливого не відбулось, або може негайно розірвати сеанс зв'язку, пояснивши серверу-відправникові істинні мотиви свого рішення або, нарешті, навмисно нічого не пояснюючи.

Таблиця 1

Порівняльна характеристика ефективності серверів чорних списків [5].

	Заблоковано небажаних листів	**Пропущено небажаних листів**	**Ефективність, %**
bl.spamcop.net	2855	4150	40,76
cbl.abuseat.org	4994	2011	71,29
dnsbl.sorbs.net	2601	4404	37,13
dul.nsbl.sorbs.net	1845	5160	26,34
dul.ru	39	6966	0,56
sbl-xbl.spamhaus.org	5007	1998	71,48
zen.spamhaus.org	6657	348	95,03

Сервери чорних списків розташовані в різних країнах, але користуватись ними можуть будь-які поштові системи світу, яким варто обрати для себе приблизно від трьох до десяти серверів чорних списків [6].

Якщо таких серверів буде менше - результат фільтрації може виявитись неточним; якщо більше зазначеного діапазона, то виконання DNS-запитів може зайняти надто багато часу і мережевого трафіку. Найбільш популярні в світі сервери чорних списків та статистика їх роботи наведена в таблиці 1.

Нажаль, доволі часто до чорних списків потрапляють не тільки поштові системи зловмисників, але і поштові системи порядних користувачів [6]. Причин для цього більш ніж достатньо [3,4].

Серед великої кількості користувачів поштової системи з високою репутацією може виявитись один зловмисник з палаючими очима та невпинним бажанням покращити своє матеріальне становище. Такими зловмисниками доволі часто стають працівники комерційних структур, що проходять процедуру свого примусового звільнення. Чимало недбалих користувачів стають жертвами вірусів або шпигунського програмного забезпечення, що періодично потрошить адресну книгу поштової клієнтської програми користувача, такої як Microsoft Outlook, та виконує розсилку за знайденими адресами від імені цього користувача.

Нарешті, молодий адміністратор поштової системи за браком досвіду може ненавмисно налаштувати надмірні права доступу до поштового сервера, перетворивши його на

відкритий ретранслятор [6,7]. Так називають поштовий сервер, що дозволяє анонімно надсилати листи не тільки своїм власним користувачам, але і користувачам усього світу.

Коли трапляється така, щойно описана, неприємність, то вкрай важливо, щоб адміністратор поштової системи дізнався про неї першим і негайно приступив до процедури вилучення поштового сервера з чорного списку. Ця процедура є різною для різних серверів чорних списків [3,6,7], її суть виходить за межі даної статті. Потрапляння серверів до чорного списку не є ганебною подією для адміністратора поштової системи і йому не варто це приховувати від користувачів. Наприклад, популярна поштова система від корпорації Google під назвою GMAIL.COM регулярно потрапляє до чорних списків, але не стає від цього менш популярною. Навпаки, адміністратору буде соромно, коли він почує про цю подію від своїх користувачів і не зможе точно визначити як давно ця подія відбулась. Дана стаття пропонує алгоритм постійно працюючої моніторингової служби, впровадженої в Київському університет імені Тараса Шевченка, яка фіксує факти перебування поштових серверів в чорних списках і своєчасно інформує про це адміністраторів.

Блок-схему циклічного алгоритму моніторингової служби показано на рис. 1. Після запуску служби виконується наступна послідовність дій:

1. Перевіряється існування розділу і параметрів реєстру, в якому зберігаються початкові параметри налаштування для коректної роботи служби. Якщо такий розділ або параметри

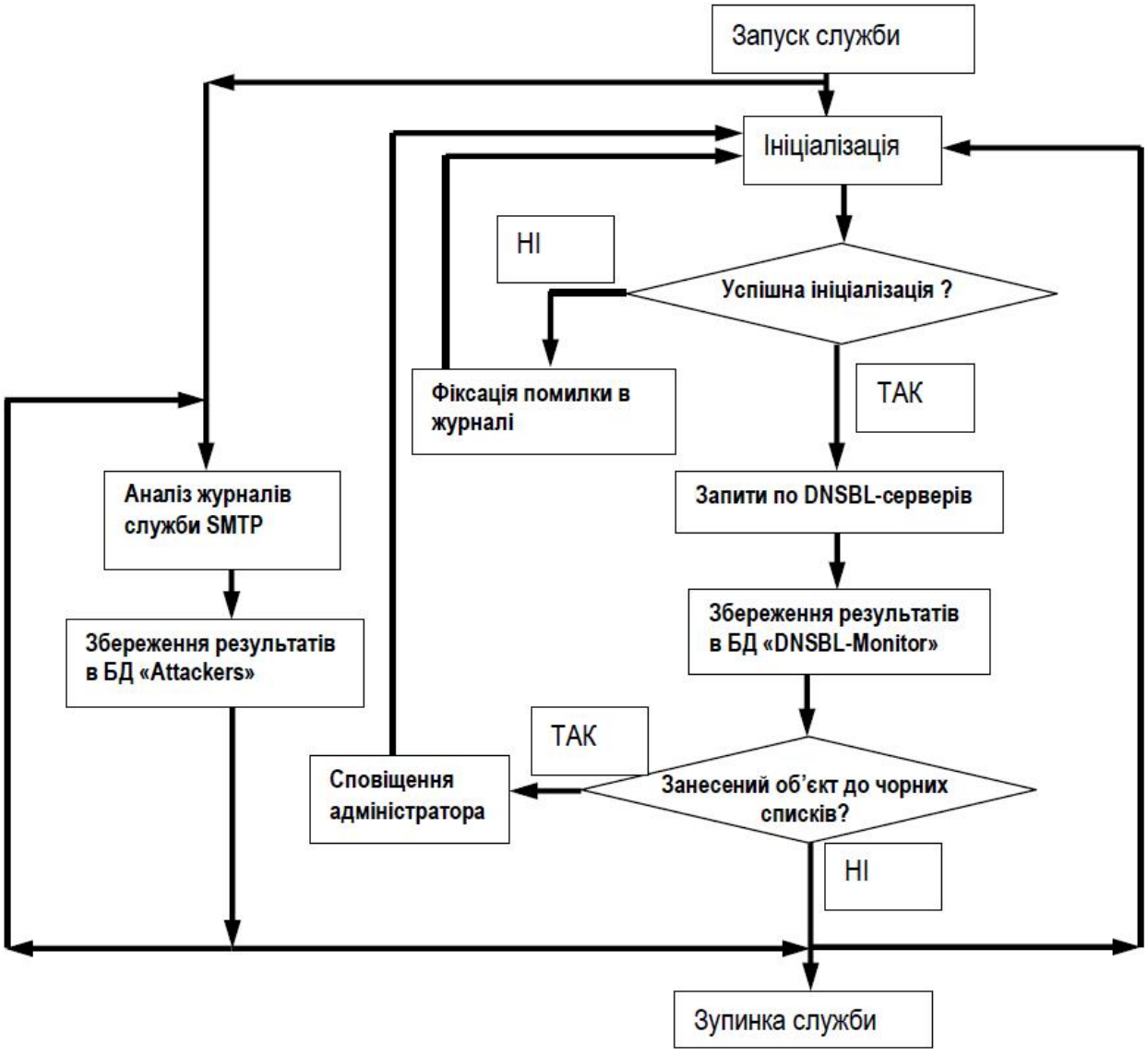

Рис. 1. Блок-схема функціонування моніторингової служби.

відсутні – вони створюються.

2. Перевіряється наявність робочого каталогу, в якому буде зберігатися база даних та текстовий журнал подій роботи служби. Якщо такий каталог відсутній – він створюється.

3. Перевіряється наявність створеної бази даних "DNSBL-Monitor" з усіма необхідними таблицями (таблиця IP-адрес (англ. Internet Protocol, протокол адресацій і маршрутизації мережі Інтернет [1]), DNSBL-серверів та таблиця з результатами роботи служби). Якщо така база даних відсутня або має не всі таблиці – створюється нова база або нові таблиці відповідно.

4. Виконується запит до DNSBL-серверів: по кожній IP-адресі з таблиці IP-адрес як по об'єкту моніторингу формується запит до кожного DNSBL-сервера з таблиці DNSBL-серверів. Якщо, наприклад, підприємство має два сервера з IP-адресами 20.30.40.1 і 20.30.40.2, що тільки відправляють повідомлення в інші поштові системи і три сервера з адресами 20.30.40.3, 20.30.40.4 і 20.30.40.5, що тільки приймають повідомлення від інших поштових систем, то в табліцю IP-адрес слід занести лише IP-адреси 20.30.40.1 і 20.30.40.2. Якщо, в свою чергу, таблиця DNSBL-серверів містить чотири адреси, то за кожен цикл буде виконуватись вісім DNS-запитів. Зокрема, для того, щоб перевірти чи входить IP-адреса 20.30.40.1 до чорного списку dnsbl.sorbs.net, потрібно запросити ресурсні записи будь-якого типу (тип ANY) для вузла:

`1.20.30.40.dnsbl.sorbs.net`

Якщо у відповідь від служби DNS прийде повідомлення, що жодного ресурсного запису не знайдено, це означатиме, що IP-адреса 20.30.40.1 не перебуває в чорному списку dnsbl.sorbs.net. Навпаки, якщо служба DNS у відповідь повертає ресурсний запис будь-якого типу, як правило, типу TXT - це означає, що IP-адреса перебуває в чорному списку.

5. Всі відповіді від DNSBL-серверів зберігаються в таблиці результатів бази даних.

6. Відбувається аналіз результатів, отриманих під час останнього запиту до DNSBL-серверів. Якщо серед результатів зустрічається позитивна відповідь, що означає перебування IP-адреси поштового сервера в чорному списку) виконується повідомлення відповідальної особи за допомою SMS (англ. Short Message Service - служба коротких повідомлень). Зокрема, для направлення SMS-повідомлення абоненту з номером 067-1234567 українського оператора стільникового зв'язку «Київстар» абонент повинен заздалегідь перевірити увімкнення послуги Email2SMS, після чого він може вручну або програмно надсилати Email-повідомлення за адресою 380671234567@sms.kyivstar.net , які від отримає як SMS-повідомлення на свій мобільний засіб зв'язку.

7. З бази даних вилучаються застарілі записи, для запобігання значного збільшення об'єму бази даних і зберігання вже неактуальних записів. Через певний період часу весь цикл повторюється з початку.

Окрім своєї основної функції контролю і інформування адміністратора, дана стаття також пропонує алгоритм аналізу журналу служби SMTP (англ. Simple Mail Transfer Protocol - простий протокол передачі пошти), яка є частиною будь-якої самодостатньої повнофункціональної поштової системи, з метою пошуку і виявлення в цьому журналі таких джерел відправлення повідомлень, які за своєю поведінкою демонструють явне і невпинне бажання відгадати адресу електронної пошти існуючого користувача і одразу надіслати йому шквал небажаних листів. Фрагмент такого журналу, проаналізований за тримісячний період роботи служби SMTP, наведено на рис. 2. Строка, в якій міститься символ «<» є SMTP-командою клієнта-зловмисника, а строка з символом «>» є відповіддю приймаючого поштового сервера.

```
.....................................................
88.198.39.130:4307,<,MAIL FROM:<dell@timose.com.ua>,
88.198.39.130:4307,<,RCPT TO:<ambulance@univ.net.ua>
88.198.39.130:4307,>,250 2.1.0 Sender OK,
88.198.39.130:4307 ,>,550 5.1.1 User unknown,
88.198.39.130:4307,<,DATA,
88.198.39.130:4307,*,Tarpit for '0.00:00:05',
.....................................................
```

Рис. 2. Фрагмент журналу служби SMTP з зафіксованою помилкою "550 User unknown".

Порушником слід вважати таку IP-адресу, яка за короткий час багато разів намагається надіслати повідомлення і отримує помилку "550 User unknown". Алгоритм виявлення таких порушників також реалізований в моніторинговій службі у вигляді окремої циклічної фонової програми, яка паралельно працює з основною програмним циклом. При цьому IP-адреси порушників та статистика їх роботи накопичується в окремій таблиці, або навіть в

окремій базі даних “Attackers”, оскільки її об’єм може суттєво відрізнятись в більшу сторону від об’єму бази даних “DNSBL Monitor” основного алгоритму служби. Ця інформація будь-коли може бути використаною для оформлення скаргової заявки на блокування відповідного вузла або усієї IP-підмережі, до якої цей вузол належить.

Блок-схему алгоритму виявлення порушників показано на рис. 2. Він складається з наступних кроків:

1. Перевіряється існування бази даних “Attackers” і відповідних таблиць в ній. Якщо база або таблиці відсутні - вони створюються.

2. Сканується останній журнал подій з метою знаходження SMTP-сеансів, в яких зафіксовані спроби відгадування адрес скриньок, тобто відправка пошти на неіснуючі поштові скриньки.

3. Виділити з сеансу корисні дані: IP-адресу відправника та фрагмент SMTP-сеансу, що підтверджує факт відправки пошти на неіснуючі поштові адреси.

4. Зберегти IP-адресу в базі даних “Attackers”, звірити її на подібність з кожною IP-адресою, яка вже занесена в базу даних “Attackers”, нарахувати цій адресі, а також усім подібним адресам «штрафні» бали. Оскільки IP-адреса являє собою послідовність тридцяти двох бітів, то для двох подібних IP-адрес, розкладених побітно, ліва частина бітів є однаковою і спільною, а права частина бітів є різною. Наприклад, якщо дві IP-адреси 91.202.128.21 і 91.202.131.21 розкласти побітно і порівняти (рис.), то видно, що перші 22 біті у них однакові, а інші 10 бітів є різними.

```
01011011.11001010.10000000.00010101
01011011.11001010.10000011.00010101
|                        ||       |
<==========22==========><====10===>
```

Рис. 2. Фрагмент журналу служби SMTP з зафіксованою помилкою “550 User unknown”.

Згідно синтаксису CIDR (англ. Classless InterDomain Routing - безкласова міждоменна маршрутизація [1]), ці дві IP-адреси належать одній спільній IP-підмережі з маскою /22. В статті пропонується визначати рівень подібності IP-адрес саме за довжиною маски підмережі, до якої ці IP-адреси належать і нараховувати штрафні бали відповідно до таблиці 2.

5. Зберегти фрагмент SMTP-сеансу, що підтверджує факт відправки пошти на неіснуючу поштові адресу. Вилучити з бази даних “Attackers” всі IP-адреси, що мають 100 і більше штрафних балів і занести ці адреси до власного приватного чорного списку IP-адрес поштової системи. Дані цього списку можуть бути вручну оформлені і надсилані у вигляді скаргового звернення до публічних DNSBL-серверів, кожен з яких передбачає власний формат такого звернення і процедуру його розгляду.

Таблиця 2

Нарахування штрафних балів для IP-адрес, що перебувають в базі даних “Attackers”

Рівень подібності IP-адрес	Кількість нарахованих штрафних балів
/22 /23 /24 /25	2
/26	3
/27	4
/28 /29 /30 /31	5
/32	10

6. Вилучити з бази даних записи старші за певний тривалий період, наприклад, 2 роки.

На фрагменті журналу порушників, що інтенсивно вгадували адресу отримувачів, добре видно (рис. 3), що в одному випадку для поширення небажаних повідомлень зловмисник використовує один поштовий сервер (72.29.73.123), в іншому випадку кластер поштових серверів (31.41.219.211-31.41.219.213), для які належать IP-підмережі /29.

```
.....................................................................
72.29.73.123     2014-02-21  <D2600123@univ.net.ua>
72.29.73.123     2014-02-21  <D2600107@univ.net.ua>
72.29.73.123     2014-02-21  <2600121@univ.net.ua>
199.59.150.88    2014-02-21  <victor@univ.net.ua>
31.41.219.212    2014-02-25  <ambulance@univ.net.ua>
31.41.219.211    2014-02-25  <ambulance@univ.net.ua>
31.41.219.213    2014-02-25  <ambulance@univ.net.ua>
.....................................................................
```

Рис. 3. Характерна зміна IP-адреси порушника, що підбирає поштову адресу існуючого користувача.

Висновки

1. Тривале перебування поштових серверів сучаних підприємств у чорних списках може негативно вплинути на репутацію поштової системи цього підприємства, користувачі якого не зможуть вчасно і без перешкод відправити необхідну кореспонденцію користувачам іншої

поштової системи, яка під час отримання листів виконує перевірку тих самих чорних списків.

2. Запропонований в статті підхід, впроваджений в поштовій системі КНУ імені Тараса Шевченка, дозволяє вчасно інформувати поштових адміністраторів про факти потрапляння вузлів поштової системи до чорних списків за допомогою електронної пошти або служби коротких повідомлень (SMS).

3. Аналіз журналу служби SMTP, що приймає повідомлення від інших поштових систем, дозволяє отримати статистику IP-адрес порушників, які займаються підбором поштових адрес існуючих користувачів та автоматично помістити IP-адреси цих порушників до приватного чорного списку поштової системи з можливим оприлюдненням інформації цього списку, наприклад, у вигляди скаргового звернення до глобального DNSBL-сервера з проханням заблокувати ці IP-адреси.

Список використаних джерел

1. *Олифер В. Г.* Компьютерные сети. Принципы, технологии, протоколы 4-е издание: учебник для ВУЗОВ / В.Г. Олифер, Н.А. Олифер – С.Петербург. Питер, – 2010. – 505 С.
2. *Бохан К.А.* Сетевые информационные технологии: Часть 1: Протоколы обмена электронной почтой. Учебное пособие / К.А. Бохан, А.В. Волковой, Г.А. Кучук, А.А. Сиора; МНО Украины ; Национальный. аэрокосмический университет им. М.Е. Жуковского " Харьковский авиационный институт". – Харьков : НАУ "ХАИ". – 2008. – 172 С.
3. *Блам Р.* Система электронной почты на основе Linux : Учебное пособие / Блам Р., – Киев : Вильямс., – 2001. – 448 С.
4. *Зайцев О.* Технологии рассылки спама и методы защиты от него [электронный ресурс] / О. Зайцев. – КомпьютерПресс, – 2007. – 6 С. (http://compress.ru/article.aspx?id=17269)
5. Независимое тестирование различных АнтиСпам решений (коммерческие и свободные продукты) [электронный ресурс]. - HabraHabr.Ru, – 2009. – 14 р. (http://habrahabr.ru/post/56779)
6. RBL: вред или польза? [электронный ресурс]. - Лаборатория Касперского. - 2003.: (http://www.securelist.com/ru/analysis/22/RBL_vred_ili_polza)
7. Борьба со спамом [электронный ресурс]. - Проект Центров учебных ресурсов (ЦУР), - 2005.: (http://tools.ietf.org/pdf/rfc2505.pdf)

References

1. OLIFER V.G. (2010) *Kompyuterniye seti. Principy, Tekhnologii, protokoly* 4 Ed.: Uchebnik dlya VUZOV. Sankt-Peterburg: Piter.
2. BOKHAN K.A. et al. (2008) *Seteviye informatsionniye tekhnologii, Part 1: Protokoli obmena pochtoy.* Uchebnoye posobiye. MNO Ukrainy; Natsionalniy aerokosmicheskiy universitet imeni M.E.Zhukovskogo "Kharkovskiy aviatsionniy institute". Kharkov: NAU "KAI".
3. BLAM P. (2001) *Systema elektronnoy pochti na osnove Linux*: Uchebnoye posobiye. Kyiv: Williams.
4. ZAYTSEV O. (2007) *Teknologii rassylki spama i methody zashchity ot nego.* KompyuterPress. [Online] Available from: http://compress.ru/article.aspx?id=17269
5. *Nezavisimoye testirovaniye razlichnikh AntiSpam resheniy (kommercheskie i svobodniye producty)* (2009) HabraHabr.Ru. [Online] Available from: http://habrahabr.ru/post/56779
6. *RBL: vred ili zashchita?* (2003) Laboratoriya Kasperskogo. [Online] Available from: http://www.securelist.com/ru/analysis/22/RBL_vred_ili_polza
7. *Borba so spamom* (2005) Proekt Tsentrov uchebnih resursov (TUR). [Online] Available from: http://tools.ietf.org/pdf/rfc2505.pdf

Надійшла до редколегії 10.04.14