«Системні технології» 4 (129) 2020 «System technologies»
DOI 10.34185/1562-9945-4-129-2020-10
УДК 004.773.3; 004.056

В.В. Гнатушенко, О.М. Певзнер, О.Л. Блат

# АНАЛІЗ ПРОБЛЕМ КІБЕРБЕЗПЕКИ ПОШТОВИХ СИСТЕМ, ЯКІ ФУНКЦІОНУЮТЬ В УМОВАХ НАЯВНОСТІ СУЧАСНОГО СПАМ-ТРАФІКА

*Анотація. Світова глобалізація та всебічна діджиталізація суспільства створюють умови для поглиблення електронних комунікацій. У той самий час існуючі комунікаційні технології уразливі до мережних загроз, однією з яких є поштовий спам. Системне дослідження небезпек, що може приносити спам-трафік, являє собою дуже актуальну та важливу проблему, якій присвячена робота авторів. Метою їх дослідження став системний аналіз кібербезпеки вузлу електронної пошти, який функціонує в умовах наявності активного спам-трафіка. Спираючись на дані авторитетних міжнародних джерел та результати власних спостережень, автори роблять висновок про необхідність фільтрації спама, але через певну невизначеність самого поняття «спам-трафік» та, враховуючи швидкість еволюції спама та технологій його розповсюдження, проблема точного розпізнавання спама та його блокування виявляється досить нетривіальною і потребує розробки спеціальних математичних алгоритмів. Ці питання передбачається розглянути в наступних роботах авторів.*

*Ключові слова: діджиталізація, електронна пошта, спам, трафік, кібербезпека, фільтр спаму, поштовий кладж, log-файл.*

**Постановка проблеми.** У сучасних умовах глобалізації світових процесів та всебічної діджиталізації світового суспільства різко зростає рівень електронних комунікацій. У той самий час разом з підвищенням рівня комунікаційних здібностей людства збільшується й рівень небезпек та загроз, які несуть з собою сучасні комунікаційні технології. Тому висвітлення таких кібернебезпек та їх класифікація являє собою дуже важливу і актуальну проблему.

**Метою дослідження** авторів статті став аналіз проблем мережної безпеки, які виникають під час розповсюдження спам-трафіка за допомогою технологій електронної пошти.





ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

**Аналіз останніх досліджень і публікацій.** Взагалі проблема безпеки систем електронного листування не нова та досліджується протягом більш ніж 20 років. Цим дослідженням присвячені, наприклад, роботи [1-6]. У той самий час спам швидко еволюціонує: змінюється його зміст та цільова аудиторія, змінюються технології доставки поштової кореспонденції тощо. Разом з еволюційними процесами, які супроводжують спам-трафік, змінюється й характер загроз, які він несе. Ще кілька десятиріч тому, коли канали передачі даних були досить вузькі, а трафік коштував великих грошей, основні ризики від спама полягали у можливому перевантаженні зовнішніх каналів користувачів паразитним трафіком. Сьогодні через появу нових швидкісних мережних технологій частка таких ризиків зникаюче мала, а на перші позиції виходять інші ризики, пов'язані зі значною криміналізацією спама та технологій його доставки. Сьогодні спам – не просто паразитний трафік, це – дуже вигідний та прибутковий бізнес, який має економічну та технічну бази для свого розвитку і функціонування. Водночас це, як правило, – кримінальний бізнес, і саме в цьому полягає основний характер загроз та небезпек, який він несе користувачам.

Головна проблема ідентифікації сучасного спама полягає в тому, що його дуже важко відрізнити від звичайної чесної електронної кореспонденції. Спам вдало маскується, застосовуючи різноманітні методи та прийоми, включаючи соціальну рекламу, психологію та соціальну інженерію. Тому, для ефективної протидії таким атакам конче необхідні всебічні системні дослідження сучасного спама та проблем, до яких він може призвести. Найбільш детальні дослідження у цьому напрямку наведено, наприклад, у [7] та [8]. Ці джерела являють собою дуже авторитетні міжнародні дослідницькі центри. Також слід звернути увагу на актуальність даних цих джерел, які поновлюються майже щомісячно.

**Аналіз та класифікація сучасного спама.** Розглянемо деякі результати, опубліковані в матеріалах [7] та [8]. За даними інтелектуальної платформи аналізу кіберзагроз Cisco Talos [9], частка спаму у загальному світовому поштовому трафіку у 2019 році становила близько 85% (див.

таблицю 1). Також проаналізовано загальний розподіл спаму за країнами світу [8] (див. таблицю 2).

Таблиця 1

Динаміка зміни частки спаму у загальному обсязі електронної кореспонденції у 2019 р

| | Загальна кількість e-mail, млрд. | Кількість спам-листів, млрд. | Частка спама, % | | Загальна кількість e-mail, млрд. | Кількість спам-листів, млрд. | Частка спама, % |
|---|---|---|---|---|---|---|---|
| Січень | 339,27 | 289,71 | 85,4 | Липень | 496,11 | 422,49 | 85,2 |
| Лютий | 239,22 | 204,19 | 85,4 | Серпень | 488,2 | 416,04 | 85,2 |
| Березень | 346,64 | 295,67 | 85,3 | Вересень | 478,41 | 409,51 | 85,6 |
| Квітень | 489,34 | 416,78 | 85,2 | Жовтень | 496,76 | 427,44 | 86,0 |
| Травень | 430,96 | 366,51 | 85,0 | Листопад | 482,88 | 412,19 | 85,4 |
| Червень | 539,22 | 459,40 | 85,2 | Грудень | 383,79 | 326,49 | 85,1 |

Таблиця 2

Рейтинг країн світу за спам-активністю у 2019 році

| Країна | Частка спаму | Країна | Частка спаму | Країна | Частка спаму |
|---|---|---|---|---|---|
| Китай | 20,43% | Туреччина | 2,42% | Південна Корея | 1,48% |
| США | 13,37% | Сінгапур | 2,24% | Великобританія | 1,42% |
| Росія | 5,60% | В'єтнам | 2,15% | Польща | 1,23% |
| Бразилия | 5,14% | Україна | 1,76% | Японія | 1,04% |
| Франція | 3,35% | Нідерланди | 1,68% | Колумбія | 1,04% |
| Німеччина | 2,95% | Індонезія | 1,65% | Інші країни | 26,92% |
| Індія | 2,65% | Аргентина | 1,48% | | |

Окреме місце посідає аналіз такого негативного явища, як спам-фішинг. Саме цей різновид спама являє собою сьогодні одну з найнебезпечніших загроз в Інтернеті та формує базу для кримінальної діяльності – електронного шахрайства, крадіжок, підробки персональних даних тощо. Такий спам часто застосовує методи соціальної інженерії та різноманітні гнучкі психологічні прийоми, через що дуже легко приймається



ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

довірливими користувачами за реальні вигідні пропозиції, що й становить одну з головних його загроз.

Ще один найнебезпечніший засіб використання спаму – розповсюдження за його допомогою небезпечних вірусів та мережних хробаків. Якщо колись такі «подарунки» були лише неприємністю, то сьогодні подібні технології застосовуються, наприклад, для розсилки вірусів-шифрувальників даних або вірусів-вимагачів. Атаки таких вірусів здатні нанести колосальної шкоди та досить відомі у світі. Так, річний звіт з кібербезпеки Cisco [7] наводить приклади випадків, що сталися у 2017 році. Серед них – масштабна атака, спрямована на персональні дані користувачів Gmail [10], злам енергетичних систем Ірландії [11], розповсюдження програми-вимагача Jaff великою бот-мережею Necurs [12] тощо. Більш детальну класифікацію відомих сьогодні загроз від спама можна знайти у вказаних працях [7-9].

**Проблеми захисту від спаму – технічний аспект.** Очевидно, що спам – дуже шкідливе явище, з яким потрібно вести безкомпромісну боротьбу. Але, як вже зазначалося вище, спам-листи, з технічної точки зору, нічим не відрізняються від звичайних листів, які спамом не являються. Більш того, саме поняття «спам» немає точного визначення: інформація, яку хтось буде сприймати як шкідливу та паразитну, для іншого може опинитися реально корисною. Тому, виходимо з того, що під «спамом» будемо розуміти, насамперед, такий поштовий трафік, який або спроможний навмисно порушувати нормальну роботу інших поштових систем (серверів), або може причинити шкоду системам користувачів.

Розглянемо загальну структуру поштового листа. Будь-який електронний поштовий лист завжди має технічні заголовки (кладжі), які автоматично формуються проміжними серверами, через які цей лист проходив, та безпосередньо тіло листа, яке містить основну інформацію для користувача. У різних за своєю специфікою листах кладжі можуть істотно відрізнятися, у той самий час вони та особливо їх набір мають бути несуперечливі та повністю відповідати стандартам поштових протоколів. Так, наприклад, у найпростішому випадку, лист, який має єдиного відправника та адресований єдиному отримувачу, може мати мінімум кла-

джей, серед яких найчастіше бачимо кладжі <From: >, <To:> та <Received:>, серед яких немає жодного обов'язкового за стандартами. Будь-який з цих кладжей може бути легко підроблений спамерами, завдяки чому спам-лист легітимізується й легко проходить крізь різноманітні спам-пастки та фільтри.

Розглянемо більш складний випадок, коли йдеться про масові розсилки. Існує багато легальних розсилок, які мають вільно проходити крізь фільтри й доходити до отримувачів. Головна технічна особливість листа, що являє собою елемент масової розсилки, – наявність у складі кладжів певних розпізнавальних елементів, насамперед, таких, як PRECEDENCE: Bulk та DKIM- і SPF-записів. Застосування таких засобів захисту репутації – непоганий шлях, але слід розуміти, що вони також мають уразливості, пов'язані з можливою підробкою, хоча підробка такої технічної інформації значно складніша за, наприклад, підробку даних про відправника або отримувача листа. Нижче наведені зразки повних заголовків листів, один з яких – простий лист:

***Received:*** *from olga ([195.24.140.206]) by omp.dp.ua with SMTP id 26757 for <admin@omp.dp.ua>; Tue, 3 Dec 2019 20:12:36 +0200*
***Message-ID:*** *<000701c71898$fc9e5900$ce8c18c3@olga>*
***Reply-To:*** *"Olga L. Blat" <olga@omp.dp.ua>*
***From:*** *"Olga L. Blat" <olga@omp.dp.ua>*
***To:*** *"Oleg M. Pevzner" <admin@omp.dp.ua>*
***Subject:*** *=?koi8-r?B?89TSwc7J3svB?=*
***Date:*** *Tue, 3 Dec 2019 20:12:55 +0200*
***Organization:*** *ISP "OMP", Dnepr*
***MIME-Version:*** *1.0*
***Content-Type:*** *text/plain; charset="koi8-r"*
***Content-Transfer-Encoding:*** *8bit*
***X-Priority:*** *3*
***X-MSMail-Priority:*** *Normal*
***X-Mailer:*** *Microsoft Outlook Express 6.00.2800.1807*
***X-MimeOLE:*** *Produced By Microsoft MimeOLE V6.00.2900.5579,*

а інший – елемент масової розсилки (Subscribe.ru):

***Return-Path:*** *<gluck@mail.subscribe.ru>*
***X-Envelope-To:*** *omp@omp.dp.ua*



ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

***X-Spam-Status:*** *No, hits=0.0 required=5.0 tests=CUSTOM_RULE_RECEIVED: -5.00,CUSTOM_RULE_FROM: ALLOW,TOTAL_SCORE: -5.000*

***X-Spam-Level: Received:*** *from gato121.sndsy.ru ([185.138.182.121]) by mail.lanservice.net (using TLSv1/SSLv3 with cipher AES256-SHA (256 bits)) for omp@omp.dp.ua; Wed, 26 Feb 2020 11:42:57 +0200*

***Received:*** *id 0955EACD6FC-1582710144*

***Return-Path:*** *gluck@mail.subscribe.ru*

***Precedence:*** *Bulk*

***DKIM-Signature:*** *v=1; a=rsa-sha256; c=relaxed/relaxed; d=subscribe.ru; s=felis.201206; t=1582710144; bh=axT1SXOp4Yg3Uhdn7ADn2A7532uOa4f4G0tb0f+4ZA4=; h=List-Id:List-Help:List-Subscribe:List-Unsubscribe:List-Archive: List-Owner:List-Post:Message-Id:Date:From:To:X-Mailru-Msgtype: Subject:MIME-Version:Content-Type; b=vb/4/tCG25g6DsNDt2LECwbkM/VCmE/YKlQrlThldAbaG26ohzjUK2qjLDBr vidk/ 3IvnlgP9+/+6ebO8Kstf9eXU6MizQC+0S30ZPQGFNFKnZjrCGHaoxgdd3jsT4k sQ13 rVROAh5+09S9fzBbUSUueleWCDpg/vXJBtJ*

***List-Id:*** *<news.citycat.subscribe.ru>*

***List-Help:*** *<https://subscribe.ru/catalog/news.citycat>*

***List-Subscribe:*** *<mailto:news.citycat-sub@subscribe.ru>*

***List-Unsubscribe:*** *<mailto:news.citycat-unsub@subscribe.ru>*

***List-Archive:*** *<https://subscribe.ru/archive/news.citycat>*

***List-Owner:*** *<mailto:news.citycat-owner@subscribe.ru>*

***List-Post:*** *NO*

***Message-Id:*** *20200226122011.hui.940416@940416.news.citycat.subscribe*

***Date:*** *Wed, 26 Feb 2020 12:20:11 +0300*

***From:*** *=?utf-8?Q?=22Subscribe=2ERu=22?= <namma940416@subscribe.ru>*

***To:*** *=?utf-8?Q?=22news=2Ecitycat=22?= <omp@omp.dp.ua> (940416)*

***X-Mailru-Msgtype:*** *news.citycat*

***Subject:*** *=?utf-8?Q?=D0=9D=D0=BE=D0=B2=D0=BE=D1=81=D1=82=D0=B8=20?= =?utf-8?Q?Subscribe=2ERu=20?= =?utf-8?Q?26=2F02=2F2020?*

***MIME-Version:*** *1.0*

***Content-Type:*** *multipart/related; boundary="=felis-related=20200226124131=633227*

Найбільш ефективними, з точки зору досягнутого ефекту блокування, можуть бути «чорні» та «сірі» списки, коли спамери блокуються за IP-адресою сервера-відправника спама. Сьогодні фільтри за «чорними» та «сірими» списками присутні майже на всіх відомих серверних платформах, але такі фільтри мають великий негативний побічний ефект – вони неінтелектуальні самі по собі, тому не спроможні приймати рішення і просто виконують свої фільтруючі завдання, незалежно від можливої зміни обставин. Істотно кращим рішенням у цьому разі виглядає фільтрація спаму за RBL/DNSBL-списками. Головні переваги цих сервісів – в їх динамічності. Сьогодні саме цей метод фільтрації дає, за різними джерелами, відсіч від 60% до 80% жорсткого спаму, але, враховуючи величезні загальні обсяги глобального спаму, навіть ті 20%-40% «поганої» пошти, які залишаються активні після RBL/DNSBL-фільтрації, являють собою дуже серйозну загрозу. Крім того, нині для розсилки спама звичайно застосовуються величезні мережні спам-боти, проти яких навіть динаміка RBL/DNSBL-систем виявляється не досить ефективною.

Таким чином, можна зробити висновок про те, що суто технічними засобами поштових технологій організувати ефективну відсіч спам-трафіка сьогодні неможливо. Водночас для розв'язання цієї проблеми існують додаткові можливості, пов'язані з розробкою інтелектуальних систем фільтрації, які базуються на аналізі не стільки технічної інформації поштових відправлень, скільки їх змісту. Іншими словами, йдеться про розробку автоматичних читачів пошти, які отримують доступ до тіла кожного листа, що проходить крізь поштову систему, та за власними інтелектуальними алгоритмами самостійно приймають рішення, чи вважати той чи інший лист за спам-відправлення. Цей підхід є дуже перспективний і нині активно розвивається, але його теж неможна вважати безпроблемним. Одна з проблем цього підходу криється в самій його суті – необхідності відкрити доступ до чужої кореспонденції, нехай і не людині, а програмі-обробнику. Ця проблема виходить за рамки технічної та лежить у суто юридичній площині. Залишаються також і проблемі технічного характеру. Вони, головним чином, пов'язані з великим різноманіттям вмісту поштових відправлень та їх постійною зміною. Саме ці при-



ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

чини призводять до необхідності постійно шукати нові автоматичні алгоритми для інтелектуального блокування сучасного спам-трафіка. Автори активно працюють у цьому напрямку, але детальний розгляд цих питань виходить за рамки нашої статті.

Наведені вище дані свідчать про те, що боротьба зі спамом – дуже гнучкий та складний процес, ефективність якого може бути високою лише тоді, коли заходи щодо блокування шкідливого трафіка мають всебічний, сумісний, комплексний характер. Також слід звернути увагу на ще один аспект сучасної спам-діяльності – її високу економічну привабливість. Масові спам-розсилки – один з найдешевших шляхів рекламної, маркетингової діяльності. У сукупності з можливою кримінальною інтеграцією такий бізнес може давати гігантські надприбутки. Тому до проблеми комплексної боротьби зі спам-трафіком слід обов'язково, крім технічних засобів, додавати економічні. Негативні наслідки від спаму можна подолати лише тоді, коли сама спам-діяльність перестане бути ефективним засобом заробітку, тому необхідно шукати шляхи щодо зниження її прибутковості, в ідеалі – до повного зникнення.

**Дослідження спам-активності на лабораторній системі.** Спираючись на дані джерел [7-9], автори досліджували загрози від спама на діючій досить великій поштовій системі mail.lanservice.net, яка працює на базі підприємства «DC LANSERVICE». Ця поштова система обслуговує кілька досить великих корпоративних клієнтів. Сервери системи розташовані у найкрупнішому датацентрі міста Варшава (Польща). Поштова система обслуговує 12 поштових доменів, деякі з яких функціонують більш ніж 20 років. Поштовий трафік був проаналізований на підставі даних серверних log-файлів, де збиралася детальна статистика загальних запитів до системи за різними поштовими протоколами, статистика запитів, які були відхилені та кваліфіковані як спам тощо. Таку статистику було проаналізовано за різні періоди та роки з 2016 по 2020 та порівняно з аналогічною статистикою [9] з деталізацією за годину, добу, тиждень, місяць, рік.

На рисунку 1 наведені зразки з витягів статистики роботи поштового серверу mail.lanserver.net за поточний місяць.

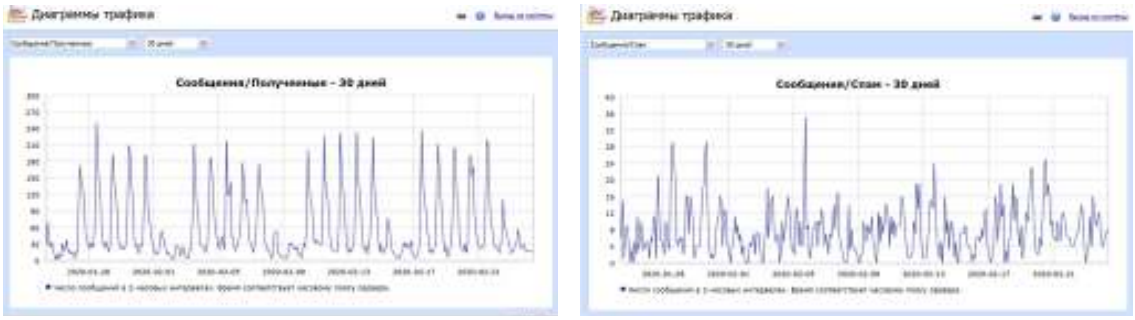


Рисунок 1 – Витяг з журналу роботи поштової системи mail.lanservice.net за 30 днів

Ми бачимо, що загальний трафік досить рівномірно розподілений за днями тижня. Він має піки, які приходяться на денні (робочі) часи та спадає увечері та вночі. Також можна помітити загальне зменшення трафіка у вихідні дні. На графіку праворуч маємо аналогічний розподіл спам-трафіка за цей самий період. Спам також розподіляється в цілому досить рівномірно упродовж місяця, але неважко побачити, що в нічні години та у вихідні дні він не тільки не спадає до нуля, а, навпаки, складає головну частку поштового трафіка. Подальше вивчення log-файлів сервера, які ми не наводимо тут зараз лише через їх громіздкість, дозволяє провести детальний аналіз різноманітних небезпек, що загрожують поштовій системі та її користувачам, коли вона знаходиться під постійними спам-атаками. Звернемо увагу на те, що загальна кількість запитів до сервера досить значна і становить від кількох одиниць до кількох десятків запитів на секунду. У той самий час, у середньому лише раз на кілька хвилин ми маємо повідомлення, яке проходить усі види серверного спам-контролю та опиняється у поштовій скриньці користувача. Таким чином, бачимо, що більша частка серверного часу та апаратних ресурсів вимушено витрачається не на корисну працю з доставки необхідної кореспонденції, а на відбивання різноманітних спам-атак, які сьогодні дуже поширені.

Підтвердимо свої висновки даними з відомого Інтернет-порталу [13]. Отримані нами графіки роботи лабораторної системи mail.lanservice.net (див. рис. 1) дуже схожі за своєю структурою, якісними та кількісними характеристиками, наведеними у [13].



ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

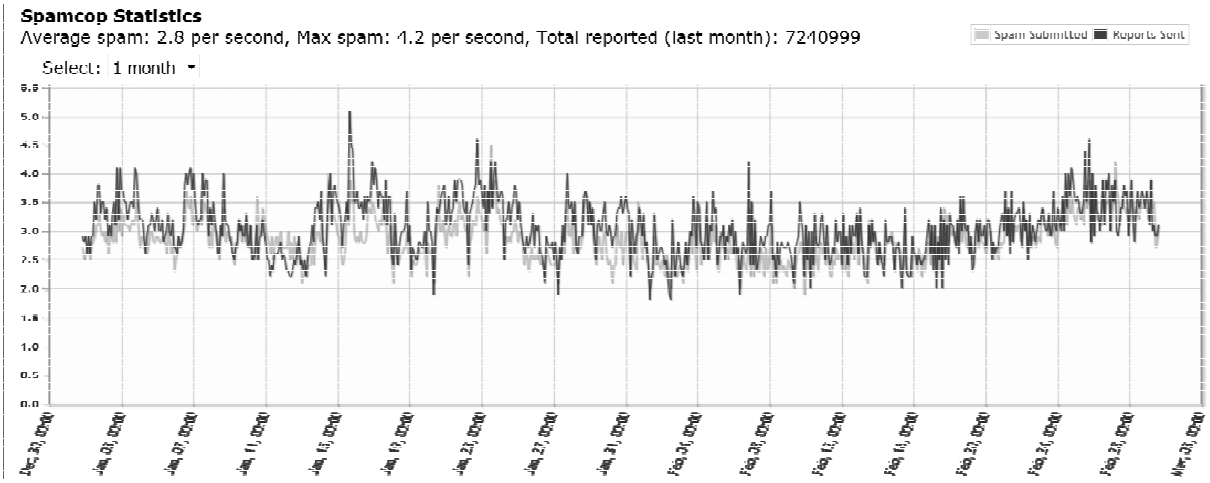


Рисунок 2 –Зразок статистичних спостережень за поштовим трафіком за допомогою системи SpamCop [13]

Схожість результатів наших спостережень з результатами, що фіксуються у глобальній мережі, дають змогу констатувати, що наша лабораторна система відповідає всім умовам релевантності для подальшого пошуку шляхів блокування кібернебезпечного спам-трафіка, розробки нових алгоритмів та методів фільтрації сучасного спама, які будуть розглянуті в наступних роботах авторів.

**Висновки.** Автори статті виконали системне дослідження ризиків та небезпек, які супроводжують роботу поштової системи в умовах наявності активного спам-трафіка. Детально проаналізовані види кіберзагроз та можливі шляхи їх усунення. На підставі виконаних досліджень підготована лабораторна система, яка може бути використана для пошуку нових методів фільтрації, математичного моделювання та розробки алгоритмів лінгвістичного розпізнавання поштового спама. Авторами доведена релевантність цієї системи для подібних досліджень. Завдяки наявності такої лабораторної системи авторам удалося провести всі необхідні експерименти та виміри на базі власного поштового трафіка, який містив у собі найсучасніший та різноманітний спам. Результати, отримані авторами, добре корелюють з даними інших відомих аналітичних досліджень, які проводилися раніше, та мають значні перспективи для подальшого творчого розвитку.

**ЛІТЕРАТУРА / ЛИТЕРАТУРА**

1. Спам: общественная опасность и способы борьбы. По материалам информационного бюллетеня Microsoft // Информационное общество. 2004. Вып. 1. С. 33-48. URL:
http://emag.iis.ru/arc/infosoc/emag.nsf/
BPA/89e60fc6af485149c32571460048f30c (дата звернення: 10.02.2020).
2. Александр Прохоров. Спам — проблема века // КомпьютерПресс. 2004. №10.
3. Иван Игнатьев. Проблема спама // Academia. 2006. №12. С. 31-35. URL: https://www.academia.edu/735859/%D0%9F%D1%80%D0%BE%D0%B1%D0%BB%D0%B5%D0%BC%D0%B0_%D1%81%D0%BF%D0%B0%D0%BC%D0%B0 (дата звернення: 10.02.2020).
4. Григорий Акопов. Проблемы несанкционированных электронных рассылок // Релга. 21.07.2004. №6 [96])
5. О.М.Певзнер. Економіко-математичне моделювання та управління зниженням спам-ризиків віртуальних підприємств. Математичне моделювання та системний аналіз соціально-економічних процесів: //Наук.-практ. конф.: тези доповідей (м. Запоріжжя: ЗІДМУ, 30-31 жовтня 2003 р.). Запоріжжя: ЗІДМУ, 2003. Т. 2, ч.7.
6. О.М.Певзнер. Аналіз економічної ефективності спама та перспектив його застосування як дешевої Інтернет-реклами // Митна політика України в контексті європейського вибору: проблеми та шляхи їх вирішення : матеріали наук.-практ. конф. (м. Дніпропетровськ: АМСУ, 20-21 листоп. 2003 р.). Дніпропетровськ, 2003.
7. Річний звіт Cisco з кібербезпеки за 2018 рік // Cisco Systems, Inc. URL: https://www.cisco.com/c/uk_ua/products/security/security-reports.html (дата звернення: 10.02.2020).
8. Мария Вергелис, Татьяна Сидорина, Татьяна Щербакова. Спам и фишинг в третьем квартале 2019 года // Лаборатория Касперского. URL: https://securelist.ru/spam-report-q3-2019/95097/ (дата звернення: 10.02.2020).
9. Email & Spam Data. Total Global Email & Spam Volume for January 2020 // Cisco Talos.
URL: https://talosintelligence.com/reputation_center/email_rep (дата звернення: 10.02.2020).



ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

9. Alex Johnson. 12 Massive Phishing Attack Targets Gmail Users // NBC News. URL: https://nbcnews.com/tech/security/massive-phishing-attack-targets-millions-gmail-users-754501 (дата звернення: 10.02.2020).
11. Lizzie Deardon. Hackers target Irish energy networks amid fears of further cyber attacks on UK's crucial infrastructure // The Independent. URL: https://independent.co.uk/news/world/europe/cyber-attacks-uk-hackers-target-irish-energy-network-russia-putin-electricity-supply-board-nuclear-a7843086.html (дата звернення: 10.02.2020).
12. Nick Biasini, Edmund Brumaghin, Warren Mercer. Jaff Ransomware: Player 2 Has Entered the Game // Блог Cisco Talos. URL: blog.talosintelligence.com/2017/05/jaff-ransomware.html (дата звернення: 10.02.2020).
13. Spamcop Statistics // Cisco Systems. 2020. URL: https://www.spamcop.net/spamgraph.shtml?spamstats (дата звернення: 10.02.2020).

**REFERENCE**

1. Spam: obschestvennaya opasnost i sposobyi borbyi. Po materialam informatsionnogo byulletenya Microsoft // Informatsionnoe obschestvo. 2004. Vyp. 1. S. 33-48. URL: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/89e60fc6af485149c32571460048f30c (the date of application: 10.02.2020).
2. Aleksandr Prohorov. Spam — problema veka // KompyuterPress. 2004. №10.
3. Ivan Ignatev. Problema spama// Academia. 2006. №12. C. 31-35. URL: https://www.academia.edu/735859/%D0%9F%D1%80%D0%BE%D0%B1%D0%BB%D0%B5%D0%BC%D0%B0_%D1%81%D0%BF%D0%B0%D0%BC%D0%B0 (the date of application: 10.02.2020).
4. Grigoriy Akopov. Problemyi nesanktsionirovannyih elektronnyih rassyilok // Релга. 21.07.2004. №6 [96]).
5. O.M.Pevzner. Ekonomiko-matematychne modeliuvannia ta upravlinnia znyzhenniam spam-ryzykiv virtualnykh pidpryiemstv. Matematychne modeliuvannia ta systemnyi analiz sotsialno-ekonomichnykh protsesiv: //Nauk.-prakt. konf.: tezy dopovidei (m. Zaporizhzhia: ZIDMU, 30 – 31 zhovtnia 2003 r.). Zaporizhzhia: ZIDMU, 2003. T. 2, ch.7.
6. O.M. Pevzner. Analiz ekonomichnoi efektyvnosti spama ta perspektyv yoho zastosuvannia yak deshevoi Internet-reklamy // Mytna polityka Ukrainy v konteksti yevropeiskoho vyboru: problemy ta shliakhy yikh vyrishennia :

materialy nauk.-prakt. konf. (m. Dnipropetrovsk: AMSU, 20-21 lystop. 2003 r.). Dnipropetrovsk, 2003.
7. Richnyi zvit Cisco z kiberbezpeky za 2018 rik // Cisco Systems, Inc. URL: https://www.cisco.com/c/uk_ua/products/security/security-reports.html (the date of application: 10.02.2020).
8. Maryia Verhelys, Tatiana Sydoryna, Tatiana Shcherbakova. Spam y fyshynh v tretem kvartale 2019 hoda // Laboratoryia Kasperskoho. URL: https://securelist.ru/spam-report-q3-2019/95097/ (the date of application: 10.02.2020).
9. Email & Spam Data. Total Global Email & Spam Volume for January 2020 // Cisco Talos. URL: https://talosintelligence.com/reputation_center/email_rep (the date of application: 10.02.2020).
10. Alex Johnson. 12 Massive Phishing Attack Targets Gmail Users // NBC News. URL: https://nbcnews.com/tech/security/massive-phishing-attack-targets-millions-gmail-users-754501 (the date of application: 10.02.2020).
11. Lizzie Deardon. Hackers target Irish energy networks amid fears of further cyber attacks on UK's crucial infrastructure // The Independent. URL: https://independent.co.uk/news/world/europe/cyber-attacks-uk-hackers-target-irish-energy-network-russia-putin-electricity-supply-board-nuclear-a7843086.html (the date of application: 10.02.2020).
12. Nick Biasini, Edmund Brumaghin, Warren Mercer. Jaff Ransomware: Player 2 Has Entered the Game // Блог Cisco Talos. URL: blog.talosintelligence.com/2017/05/jaff-ransomware.html (the date of application: 10.02.2020).
13. Spamcop Statistics // Cisco Systems. 2020. URL: https://www.spamcop.net/spamgraph.shtml?spamstats (the date of application: 10.02.2020).

Received 03.03.2020.
Accepted 06.03.2020.

***Анализ проблем кибербезопасности почтовых систем, функционирующих в условиях присутствия современного спам-трафика***

*На основе данных авторитетных международных источников выполнен детальный системный анализ современного почтового спам-трафика и связанных с ним киберугроз. Рассмотрены различные аспекты возможного противодействия такому трафику: технические, экономические, юридические и т.д. Создана собственная лабораторная система для дальнейших исследований, доказана ее релевантность в отношении общей структуры и содержания глобального международного спам-трафика.*


ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

***The analysis of the cybersecurity problems of mail systems operating in the presence of modern spam traffic***

*The last researches and publications analysis. The world globalization and comprehensive digitalization of society create conditions for further increase of interest in the electronic communications problems. Cyber threats from spam traffic, which is reaching a truly huge scale today, are one of such problems. It has been considered by various scientists for more than 20 years and still remains relevant due to the rapid evolutionary spam changes in the global information space and the significant criminalization of spam sending technologies. The problems of spam threats have different aspects: technical, economic, legal, etc. so they should be investigated in a comprehensive way. Equally comprehensive should be measures to reduce the negative impact of spam on human activity.*

*The aim of the research. The purpose of the authors' research is to provide the detailed system analysis of cyber security issues that threaten the modern mail system operating under continuous spam attacks.*

*The main research material. Based on the authoritative data of the world analytical centers, the authors analyzed the general structure and features of modern spam traffic. Various aspects of spam counteracting are considered and the ways of prospective research are targeted. The own laboratory mail system has been created and its relevance to the global spam traffic has been proven. Using this system, the proper experiments with spam on our own mail traffic were performed and the necessary measurements were made. The obtained results correlate well with other known research centers data. The proposed system is planned to be used for further research in the field of mathematical modeling and development of algorithms for spam linguistic recognition and its blocking according to these algorithms.*

*Conclusions. By this article the authors start the work series aimed at comprehensive research into modern spam and cyber threats that accompanies its sending. The authors are actively seeking further effective methods and algorithms for spam risk reducing.*

**Гнатушенко Виктория Владимировна** – д.т.н., доцент, профессор кафедры информационных технологий и систем Национальной металлургической академии Украины.

**Певзнер Олег Менделевич** – главный системный администратор датацентра «DC LANSERVICE»; специалист учебно-методического отдела национального Центра аэрокосмического образования молодежи им. А. М. Макарова.

**Блат Ольга Леонидовна** – преподаватель Колледжа ракетно-космического машиностроения Днепровского национального университета имени Олеся Гончара, студентка Национальной металлургической академии Украины.

**Гнатушенко Вікторія Володимирівна** – д.т.н., доцент, професор кафедри інформаційних технологій і систем Національної металургійної академії України

**Певзнер Олег Мендельович** – головний системний адміністратор дата-центру «DC LANSERVICE»; фахівець навчально-методичного відділу національного Центру аерокосмічної освіти молоді ім. О. М. Макарова

**Блат Ольга Леонідівна** – викладач Коледжу ракетно-космічного машинобудування Дніпровського національного університету імені Олеся Гончара, студентка Національної металургійної академії України.

**Hnatushenko Viktoriia** – Doctor of engineering's sciences, professor, Department of Information Technologies and Systems, National Metallurgical Academy of Ukraine.

**Pevzner Oleg** – the Chief System Administrator of datacenter «DC LANSERVICE»; the educational-methodical department specialist of the O. M. Makarov National Aerospace Educational Center of Youth.

**Blat Olga** – the teacher of Rocket-and-Space Engineering College of Oles' Gonchar Dnipro National University; the student of National Metallurgical Academy of Ukraine.



ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)