УДК 004.056.5 (045)

ЗАГОРОДНЮК Сергій Петрович

НЕЛЕГАЛЬНИЙ КОНТЕНТ: БАГАТОГРАННІСТЬ ПРОБЛЕМИ

Побудова і розвиток в Україні цивілізованого інформаційного суспільства є безперервним і невпинним процесом, що зумовлюється світовою глобалізацією і розвитком інформаційних технологій. Держава може і повинна правильно спрямовувати цей процес. Зокрема, український телевізійний простір та вітчизняний сегмент мережі Інтернет щосекунди обмінюються з іншими країнами потужними інформаційними потоками. Заборонити або блокувати доступ до таких потоків неможливо. Стаття 9 Закону України "Про Інформацію" надає право кожному громадянину або підприємству на "вільне одержання, використання, поширення та зберігання" інформації, якщо реалізація цього права не порушує "інші права, свободи і законні інтереси". Слід лише забезпечити дотримання цього закону.

Серед усіх інформаційних ресурсів, до яких має доступ український користувач, слід виокремити так званий андеграунд (англ. *underground* – підземелля, підпілля). Це велика сукупність ресурсів, які частково або повністю містять незаконну інформацію або здійснюють незаконну діяльність [1], наприклад, надають користувачам незаконні послуги. Перелік і класифікацію всіх видів незаконної інформації та діяльності дослідив у своїй праці В.О.Голубєв [2]. Достатньо зазначити лише той факт, що саме завдяки існуванню андеграунду необмежений доступ до мережі Інтернет для дітей дошкільного і шкільного віку є небезпечним [3]. Коли середня школа звітує про обладнання класів сучасними комп'ютерами, приєднаними до інтернету, то відразу виникає питання: у який спосіб організовано контроль за використанням школярами інтернет-ресурсів? Зазвичай це питання залишається без відповіді.

Встановити особу адміністратора незаконного ресурсу і притягти його до відповідальності вдається далеко не завжди. Це залежить, як не дивно, від самого адміністратора і від його вміння користуватися наявним на цей час потужним арсеналом засобів маскування та приховування своєї нелегальної активності. Перед працівниками правоохоронних органів часто виникає практичне питання: чи можливо, принаймні, призупинити діяльність нелегального інтернет-ресурсу, що працює у режимі веб-сервера з доступом за мережевим протоколом HyperText Transfer Protocol (HTTP) [4], не порушуючи при цьому роботу законних ресурсів, що працюють поряд із незаконним? Виявляється, що це зовсім не просте питання. Більше того, коректно вирішити його неможливо, якщо не знати структуру веб-сервера і роботу протоколу HTTP. Отже, **метою статті** є класифікація режимів роботи інтернет-сайтів та опис ролі служби Domain Name System (DNS) [5] в організації доступу до них.

Визначимося із термінологією. Веб-сервер або просто сервер – це не обладнання, на якому працює служба HTTP, а комп'ютерна програма, що працює під управлінням однієї операційної системи (ОС). Головним призначенням ОС, як відомо [6], є виокремлення і розподіл ресурсів оперативної пам'яті, процесора та дискового простору між різними програмами. Для багатьох користувачів і навіть фахівців була традиційно сформована аксіома, що на одному комп'ютері у певний момент часу працює лише одна ОС. Ця аксіома втратила

чинність. Сучасні технології віртуалізації [7] дають змогу одночасно працювати на одному потужному комп'ютері практично необмеженій кількості різнорідних ОС, що повністю еквівалентно роботі відповідної кількості окремих комп'ютерів. Кожна віртуальна ОС налаштовується незалежно від інших, має власного адміністратора, власний набір IP-адрес [8]. Наприклад, на одному фізичному комп'ютері з однією фізичною мережевою платою може працювати п'ять ОС, кожна із трьома віртуальними мережевими платами, з окремою IP-адресою на кожну плату. При цьому інтернет-користувачі завжди сприйматимуть такий комп'ютер як п'ятнадцять окремих незалежних серверів з окремими IP-адресами. Проте, що насправді працює один комп'ютер із п'ятьма ОС, користувачі ніколи не дізнаються. Очевидно, що вимкнення такого комп'ютера призведе до припинення роботи всіх п'яти ОС, всіх п'ятнадцяти IP-адрес та до відповідних наслідків.

Розглянемо одну ОС та визначимо кількість веб-серверів, які можуть працювати під її управлінням. Веб-сервер приймає від веб-клієнтів команди протокола HTTP, який за стандартною конфігурацією [4] налаштований на використання порта транспортного протоколу Transmission Control Protocol (TCP) [8], що дорівнює значенню 80. Це дозволяє веб-клієнту за відомою IP-адресою веб-сервера, наприклад 212.109.32.5, відкрити його головну сторінку за такою URL-адресою [4]:

http://212.109.32.5

Якщо адміністратор веб-сервера змінює стандартне значення TCP-порту на інше значення, наприклад 81, то в такому разі URL-адреса ускладнюється:

http://212.109.32.5:81

Досвід свідчить, що саме через ускладнення URL-адреси, яку повинен зберігати і щоразу вводити під час відвідування сайту користувач, веб-сервери використовують лише TCP-порт 80. Особливо це стосується веб-серверів, що обслуговують комерційні проекти. Отже, якщо для звернення до веб-сервера використовувати його IP-адресу і не використовувати TCP-порт, то максимальна кількість веб-серверів у межах однієї ОС дорівнює кількості IP-адрес цієї ОС. Наприклад, якщо ОС має три IP-адреси, то кожна із них може бути прив'язана до окремого веб-сервера або навпаки, до одного спільного веб-сервера.

Використання IP-адрес для адресації веб-серверів є доволі незручним через цілу низку причин [5] і на практиці використовується рідко. Замість цього в URL-адресах використовуються доменні імена [5], наприклад, http://rada.gov.ua.

Для того, щоб веб-клієнт міг завжди використовувати доменні імена замість IP-адрес, він зобов'язаний бути також клієнтом служби DNS [5]. Винятком є випадок, коли веб-клієнт використовує для інтернет-доступу службу веб-проксі [9]. У цьому разі роль DNS-клієнта перекладається на цю службу. Служба DNS є спільною загальносвітовою розподіленою базою даних і має складну структуру, щоб розглядати її у цій статті. Отже, наведемо лише основні функції служби DNS, що притаманні веб-серверам.

Служба DNS ототожнює доменні імена та IP-адреси веб-серверів. Це дає змогу зіставляти довільну кількість доменних імен із однією IP-адресою і навпаки, одне доменне ім'я із довільною кількістю IP-адрес. Прикладом першого випадку є таке порівняння, що реально існує на сайті Верховної Ради України:

rada.gov.ua --> 193.19.152.74
www.rada.gov.ua --> 193.19.152.74
portal.rada.gov.ua--> 193.19.152.74
wrt.rada.gov.ua --> 193.19.152.74

Допитливі користувачі можуть легко перевірити справедливість, наприклад, другого рядка за допомогою команди:

NSLOOKUP www.rada.gov.ua

Зазначена вище властивість служби DNS дозволяє розгорнути в одній ОС практично необмежену кількість веб-серверів і у такий спосіб обійти наведене вище обмеження за кількістю IP-адрес цієї ОС. При цьому, за-

лежно від налаштувань ОС, в одному граничному випадку кожне доменне ім'я або IP-адреса можуть ідентифікувати окремий незалежний від інших веб-сервер. В іншому граничному випадку всі доменні імена та IP-адреси можуть бути псевдонімами [5] одного єдиного веб-сервера, як це справедливо, зокрема для сайту Верховної Ради України. Існують також змішані довільні комбінації доменних імен і веб-серверів. Головною умовою при зверненні до кожного веб-сервера є використання в URL-посиланні саме доменного ім'я, а не IP-адреси, що є вимогою протоколу HTTP, на рівні якого і відбувається ідентифікація веб-серверів у межах однієї ОС. Очевидно, що серед кількох веб-серверів однієї ОС лише деякі із них можуть бути нелегальними і заслуговувати на силове втручання, а отже, завершення роботи усієї ОС є далеко не найкращим способом вирішення проблеми.

Розглянемо один веб-сервер. Як незалежна серверна програма він має доволі складну деревоподібну структуру, що складається з кореневого веб-каталогу та ієрархії віртуальних каталогів. Кожен із них пов'язаний із конкретним фізичним каталогом цієї ОС, зі спільним каталогом іншого комп'ютера локальної мережі або віртуальним каталогом іншого веб-сервера у межах усієї мережі Інтернет. Кожен віртуальний каталог має цілу низку власних налаштувань, зокрема анонімний або авторизований доступ, можливість або неможливість для веб-клієнта перегляду змісту каталогу, файл, що відкривається за замовчуванням. Звернення до віртуального каталогу, що має, наприклад, ім'я "documents" і розташований в іншому віртуальному каталозі "download", здійснюється за таким URL-посиланням:

http://rada.gov.ua/download/documents.

Сукупність віртуальних каталогів веб-сервера та пов'язаних із ним веб-серверів дає змогу увести поняття "інтернет-сайту". Сайт – це логічно завершений, самодостатній проект, що складається із довільної кількості статичних або динамічних веб-сторінок, які відкриває веб-клієнт у результаті своєї активної роботи із сайтом, зокрема при використанні гіперпосилань сайту.

Статичні веб-сторінки не містять програмного коду і становлять собою текстові файли із HTML-розміткою [4], що зберігаються у віртуальних каталогах веб-сервера і мають розширення .htm або .html. Для того щоб завантажити статичну сторінку з ім'ям, наприклад, "start-page.html", у наведеному вище каталозі, потрібно відкрити URL-посилання http://rada.gov.ua/download/documents/start-page.html.

Статичні веб-сторінки, про що говорить їх назва, виглядають для всіх веб-клієнтів однаково, незалежно від того, яким чином клієнти відкривають ці сторінки. Веб-сервер зі статичними сторінками фактично становить собою файловий сервер протоколу HTTP і за функціональністю майже не відрізняється від сервера мережевого протоколу File Transfer Protocol (FTP) [10].

Протилежним випадком до статичних веб-сторінок є динамічні веб-сторінки, які також називають веб-програмами [11]. Переважна більшість усіх інтернет-сайтів використовує саме динамічні сторінки. При кожному HTTP-запиті клієнта такі сторінки своєчасно формуються постійно діючою на веб-сервері програмою, яка може працювати у різний спосіб залежно від багатьох факторів, навіть від версії браузера клієнта. Таким чином, динамічно сформована веб-сторінка з HTML-розміткою фактично становить собою інтерфейс взаємодії користувача з серверною програмою. Сторінки формуються персонально для кожного індивідуального користувача і можуть виглядати зовсім порізному. Програма працює як чорна скринька, і логіка її роботи є повністю прихованою не лише від користувачів веб-програми, але і від інших адміністраторів і програмістів веб-сервера. Змінювати програму може тільки її розробник-програміст.

Код веб-програми та HTML-розмітка можуть розміщуватись на сервері у вигляді одного файлу, але внаслідок поширеного зараз принципу роздільного коду веб-програми організовують у вигляді мінімум

двох файлів – файлу, що містить тільки HTML-розмітку і називається веб-формою, і файлу, що є самим "тілом" веб-програми. Останній, у свою чергу, має або текст із вихідним кодом програми (який може прочитати фахівець) або відкомпільований бінарний масив (який не може бути прочитаний людиною).

Розглянемо, наприклад, два найбільш популярні веб-сервери – Appach [12], що працює на ОС сімейства UNIX [6], і Microsoft Internet Information Server (Microsoft IIS) [13], який працює на ОС Microsoft Windows Server [6]. На веб-сервері Appach обидва файли зазвичай мають розширення .php, програма, як правило, має вигляд вихідного коду, який лише під час клієнтського запиту компілюється і виконується в оперативній пам'яті сервера. Після формування сторінки і направлення її до клієнта відкомпільовані дані відразу вилучаються. Однак програміст-порушник може навмисно відкомпілювати програму "вручну", а вихідний код на сервері вилучити. Внаслідок цього логіка роботи його програми залишиться невідомою. Прикладом веб-сервера, що працює на програмі Appach, є сайт документації мовою програмування PHP: http://php.net/manual/ru/index.php.

На веб-сервері Microsoft IIS файл веб-форми має розширення .aspx, а програма завжди зберігається у вигляді бінарного масиву з розширенням .dll, що створюється програмістом у результаті компіляції його програми. Прикладом веб-сервера, що працює на програмі Microsoft IIS, є сайт Посольства Канади в Україні: http://canadainternational.gc.ca/ukraine/visas/index.aspx.

Характерною властивістю усіх веб-програм є можливість приймати від веб-клієнта довільну кількість додаткових параметрів, які користувач може явно передати в URL-посиланні до веб-сторінки, наприклад:

http://canadainternational.gc.ca/ukraine/visas/index.aspx?lang=ukr&menu_id=42&view=.

У цьому випадку звернення до веб-програми

http://canadainternational.gc.ca/ukraine/visas/index.aspx

супроводжується трьома явно переданими до неї додатковими параметрами:

lang=ukr

menu_id=42

view=d.

Ці параметри є початковими значеннями змінних або констант веб-програми, залежно від яких програма може працювати по-іншому. У наведеному вище прикладі від першого параметра, зокрема, залежить мова сайту Посольства. Якщо деякі параметри користувач не задає, веб-програма використовує для цих змінних значення, закладені розробником. Очевидно, що залежність роботи веб-програми від додаткових параметрів є для зловмисника дуже зручним способом приховати справжню логіку роботи нелегального інтернет-сайта і замаскувати такий сайт, наприклад, під соціальну мережу, сайт новин або прогнозу погоди. Сайт може тривалий час надавати користувачам законну інформацію, аж поки до нього не направити HTTP-запит із конкретним значенням потрібного параметра.

Крім явно вказаних додаткових параметрів існують також і неявні, які не передаються в URL-посиланні, але входять до структури HTTP-запита веб-програми. Прикладом такого параметра є попередня веб-сторінка-референт (англ. *URL Referrer* [4]), на якій здійснено перенаправлення клієнта на цю веб-програму. Якщо користувач працював із веб-сторінкою А і у результаті його дій відбувся перехід на веб-сторінку Б, то сторінка А є референтом для сторінки Б. Якщо користувач відкрив сторінку Б відразу, а не перейшов до неї зі сторінки А, то у цьому випадку сторінка Б не має референта. Можна дійти висновку: якщо перший користувач перейшов на сторінку Б зі сторінки А, другий зі сторінки В, а третій відкрив сторінку Б відразу, набравши в браузері її точну URL-адресу, то для трьох користувачів сторінка Б може працювати абсолютно по-різному.

Найбільш серйозну проблему для компетентних служб становить широке викори-

стання веб-адміністраторами згаданої вище служби DNS. Користувачі інтернет-сайтів майже завжди ідентифікують і запам'ятовують сайти саме за їх доменними іменами, а не за IP-адресами. По-перше, це означає, що веб-адміністратор має змогу змінювати IP-адресу, а отже, фізичне місцезнаходження веб-сервера, на свій власний розсуд. По-друге, з міркувань розподілу навантаження або забезпечення відмовостійкості, зокрема від втручання сторонніх осіб, веб-адміністратор може ввести до експлуатації довільну кількість веб-серверів із різними IP-адресами, причому в службі DNS може бути зареєстрована лише частина цих веб-серверів.

Веб-адміністратор може обрати будь-яку всесвітньо відому інтернет-компанію на зразок американської "Go!Daddy" для реєстрації власного DNS-домена другого рівня [5], наприклад, PINOKKIO.COM у домені першого рівня COM [5]. Потім адміністратор реєструє доменне ім'я інтернет-сайту WWW.PINOKKIO.COM , розгортає три веб-сервери, що розташовані у різних підприємствах або домашніх мережах України або іншої держави. IP-адреси першого і другого веб-серверів адміністратор прив'язує до доменного ім'я WWW.PINOKKIO.COM, IP-адреса третього сервера не прив'язується, а залишається "на потім", якщо за певної причини припинить працювати перший або другий сервер. За такої конфігурації одна половина користувачів інтернет-сайту з'єднається з першим сервером, друга половина із другим сервером, а третій сервер використовуватись не буде і ніхто з допитливих користувачів ніколи не дізнається про його існування. Відповідальний адміністратор, зацікавлений в безперервній роботі інтернет-сайту, обов'язково налаштує спеціальний програмний монітор, який у випадку припинення нормальної роботи одного із веб-серверів відразу його сповістить про це за допомогою sms-повідомлення. Коли один із серверів припиняє роботу, адміністратор відразу вносить відповідні зміни у конфігурацію доменного ім'я WWW.PINOKKIO.COM, у результаті чого до цього доменного ім'я залишаються прив'язаними лише IP-адреси працюючих серверів. Адміністратор може також налаштувати автоматичне виконання цієї операції.

При використанні певної кількості веб-серверів адміністратор інтернет-сайту повинен врахувати те, що майже 90% користувачів не знають, що таке IP-адреса і не бажають це знати; їм не цікаво, яка кількість веб-серверів забезпечує роботу сайту, але для користувача сайт повинен працювати постійно, надійно і в єдиний спосіб, незалежно від того, з яким саме сервером з'єднається користувач. Групу однаково налаштованих серверів умовно називають фермою серверів. Інакше кажучи, адміністратор повинен забезпечити синхронізацію даних між усіма веб-серверами ферми. Виявляється, що за допомогою сучасних інформаційних технологій це завдання вирішити абсолютно не складно.

Головний принцип ферми серверів полягає у територіальному розподілі програми і даних, з якими ця програма працює. Розроблену і відлагоджену веб-програму розміщують на кількох веб-серверах, на яких, крім самої веб-програми, ніяких даних не зберігається. Отже, якщо один із таких веб-серверів потрапить до рук правоохоронців, то не зможе бути використаний як речовий доказ. Для даних, які отримує і зберігає кожна копія веб-програми, виділяють окремий сервер, який спільно використовується усіма веб-серверами – так зване спільне джерело даних. На ньому розгортають систему управління базами даних (СУБД) на основі такого програмного забезпечення, як FoxPro, SQL, LDAP або Oracle. Кожен веб-сервер має авторизований (захищений) мережевий доступ до серверів СУБД. Інформація, яку записує до бази даних один веб-сервер, є доступною для всіх інших веб-серверів, а отже, незалежно від того, з яким саме сервером з'єднався веб-користувач, інтернет-сайт працюватиме для нього абсолютно однаково і проблеми синхронізації даних між веб-серверами ферми не виникне.

Альтернативою сервера СУБД може бути так звана веб-служба [14]. Це постійно діюча спеціалізована веб-програма, яка не має інтерфейсу користувача, через що користувачі працювати безпосередньо з цією веб-програмою не можуть. Замість цього веб-служба має певний набір функцій спеціального формату і синтаксису, які можуть бути викликані іншими веб-програмами, зокрема тими, що працюють на веб-серверах ферми. Коли веб-серверу, з яким працює користувач, потрібно отримати або зберегти дані, він з'єднується з веб-службою і викликає відповідну функцію. Веб-служба може використовувати для накопичення даних сервер СУБД, файловий сервер, іншу веб-службу або будь-яке інше джерело даних. Уся внутрішня інфраструктура інтернет-сайту повністю прихована від користувача. Про факт з'єднання веб-серверів із спільними джерелами даних можна дізнатися лише аналізуючи мережевий трафік на тих підприємствах, де встановлені і налаштовані веб-сервери.

Нарешті, ферму можуть формувати взагалі не веб-сервери, а так звані проксі-сервери (англ. *proxy* – представник). Проксі-сервер не містить ні даних, ні програмного коду. Він є лише низькорівневим мережевим ретранслятором, що приймає мережеві запити від клієнта і передає їх на інший сервер, IP-адреса та місцезнаходження якого залишаються для клієнта невідомими. Цей інший сервер, у свою чергу, може бути або веб-сервером, або іншим проксі-сервером, що утворює з першим проксі ланцюжок мережевих з'єднань. Служба проксі має два типи – SOCKS-проксі і веб-проксі [9], які ретранслюють мережеві запити клієнтів за інформацією протоколу транспортного рівня TCP та програмного рівня HTTP відповідно. Для уточнення цього факту службу SOCKS-проксі також називають TCP-проксі, а веб-проксі – HTTP-проксі.

З огляду на зазначене доходимо висновку, що мережа Інтернет має логічну (глобальну) та фізичну (регіональну) інфраструктури, взаємно незалежні одна від одної. Інтернет-сайт є елементом логічної інфраструктури, тісно пов'язаної з реєстрацією доменного ім'я в службі DNS. Натомість веб-сервер є елементом регіональної інфраструктури, який по суті є лише одним екземпляром інтернет-сайту, що працює у конкретному регіоні. Що буде з інтернет-сайтом, якщо вимкнути один із його веб- або проксі-серверів? Може виявитись, що така дія не завадить, а навіть допоможе функціонуванню усього інтернет-сайту в цілому, завчасно даючи зрозуміти адміністратору, що вимкнений сервер був розташований у "ненадійному" місці і вдруге там його налаштовувати не потрібно. Однак доволі часто компетентні служби зводять питання зупинки роботи інтернет-сайту саме до технічної задачі вимкнення веб-сервера, додатково звинувачуючи при цьому також підприємство хостінг-провайдера, на якому встановлений і налаштований цей сервер.

Серйозним нокаутуючим ударом по роботі інтернет-сайту є припинення реєстрації його доменного ім'я в службі DNS, але тут правоохоронці стикаються з проблемами іншого роду. Для реєстрації DNS-доменів адміністратори-порушники користуються послугами переважно закордонних підприємств, причому в цьому зацікавлені обидві сторони. Веб-адміністратор зацікавлений, щоб за помірну плату DNS-домен був зареєстрований у недосяжному місці. З боку підприємства-реєстратора існує комерційна зацікавленість, яка полягає у тому, що підприємство, не використовуючи практично ніяких ресурсів, заробляє десятки або сотні доларів на рік лише за реєстрацію кожного DNS-домена другого рівня. Частину цих грошей у вигляді податків отримує держава, на території якої працює підприємство-реєстратор. Якщо діяльність інтернет-сайту, написаного, наприклад, лише українською мовою, для цієї держави шкоди не несе, то факт шкідливості того ж сайту для держави Україна її зовсім не хвилює. Безумовно, це не означає, що кожна індивідуальна країна вирішує власні проблеми самотужки. Тисячі міжнародних договорів і законів примушу-

ють цивілізовані країни колективно вирішувати спільні проблеми, зокрема кримінального характеру. Отже, підприємство-реєстратора можуть змусити припинити реєстрацію DNS-домена або місцеві силові структури, або представники іншої дружньої країни, приєднаної до відповідної чинної угоди або асоціації.

Держава Україна, безперечно, також має авторитет і повагу на міжнародному рівні, але, коли справа доходить до комерційних інтересів іншої країни, цього, на жаль, недостатньо. Не дивлячись на серйозний прогрес у напрямі інтеграції України до міжнародного соціуму цивілізованих країн, перспективи її повноцінного членства поки що є туманними і невизначеними. Як наслідок, на звернення з боку українських представників закордонне підприємство-реєстратор зазвичай дає лицемірну відповідь, що на території цього підприємства незаконних ресурсів не розміщено, а отже, підстав для припинення реєстрації DNS-домена немає. Як свідчить практика, взаємодія силових структур України із західними підприємствами-реєстраторами є неефективною, не в останню чергу через бюрократичні перешкоди самої України.

Висновок. Мережа Інтернет є кібернетичним віддзеркаленням світу людських відносин із усіма його особливостями. Проте, забезпечення в мережі повного виконання законів і правил, створених для регулювання реального життя людей, є складним технічним завданням, яке повністю ніколи не буде вирішеним. Основною причиною цього є відсутність кордонів між сегментами мережі Інтернет різних країн, необмежена свобода користувачів і веб-адміністраторів, виникнення нових інформаційних технологій, що дає змогу правопорушнику легко уникати відповідальності, і, нарешті, недостатньо ефективна взаємодія силових структур різних країн із хостінг-провайдерами та DNS-реєстраторами. Інтернет-сайти з нелегальним контентом є лише одним із різновидів порушень у мережі Інтернет. Зупинка роботи інтернет-сайту, діяльність якого є небажаною для цивілізованого суспільства, може бути як легким, так і складним завданням. Це безпосередньо залежить від комерційної зацікавленості його власника. У цій статті розглянуто основні та найбільш вживані методи організації інтернет-сайтів. Зауважено, що важливу роль при зверненні клієнтів до інтернет-сайтів відіграє служба DNS, а отже, при аналізі функціонування інтернет-сайту вкрай важливо проаналізувати HTTP-запит клієнта, з якого видно чи користуються клієнти доменним ім'ям сайту або його IP-адресою, скільки при цьому передають додаткових параметрів, з якого сайту переадресовані тощо; що до успішної зупинки інтернет-сайту варто максимально вивчити логіку його роботи і тільки після цього переходити до конкретних дій. Зокрема, руйнування регіональної інфраструктури інтернет-сайту та адміністративно-кримінальне переслідування українських підприємств-провайдерів, у мережах яких розміщені веб-сервери цього сайту, практично не має нічого спільного з ефективними заходами, спрямованими на повне припинення діяльності інтернет-сайту як логічно структурованого і глобально розподіленого проекту.

Список використаних джерел

1. Вехов В.Б. Расследования компьютерных преступлений в странах СНГ : моногр. / В.Б.Вехов, В.А.Голубев. – Волгоград : Волгоградская академия МВД России, 2004. – 304 с.

2. Голубєв В.О. Розслідування комп'ютерних злочинів : моногр. / В.О.Голубєв. – Запоріжжя : Гуманітарний університет "ЗІДМУ", 2003. – 296 с.

3. Сайтарлы Т. Детская порнография в Интернете: проблемы и решения / Т.Сайтарлы // Компьютерная преступность и кибертерроризм : сб. науч. раб. – Запорожье : Центр исследования компьютерной преступности, 2005. – Вып. 3. – С. 80-87.

4. Полубояров В.В. Введение в технологии создания Интернет-узлов [Электронный ресурс] / В.В.Полубояров // Открытые системы. – Режим доступа : http://www.intuit.ru/department/internet/inwwwtech/1/.

5. Основные понятия о службе DNS [Электронный ресурс] // Microsoft Technet. – Режим доступа : http://technet.microsoft.com/ru-ru/library/cc779489(v=ws.10).

6. Назаров С.В. Современные операционные системы [Электронный ресурс] / С.В.Назаров, А.И.Широков // Открытые системы. – Режим доступа : http://www.intuit.ru/department/os/modernos/1/1.html.

7. Виртуализация серверов [Электронный ресурс] // Trinity Group. – Режим доступа : http://www.trinitygroup.ru/solution/infrastucture/virtualization/server/.

8. Стек протоколов TCP/IP [Электронный ресурс] // CIT-Forum. – Режим доступа : http://citforum.ru/nets/ip/glava_2.shtml.

9. Веб-прокси и SOCKS-прокси [Электронный ресурс] // Floss Manuals. – Режим доступа : http://booki.flossmanuals.net/bypassing-ru/_draft/_v/1.0/ВЕБ ПРОКСИ/.

10. Получение файлов через FTP [Электронный ресурс] // CIT-Forum. – Режим доступа : http://citforum.ru/internet/ftp/ftpusage.shtml.

11. Яковлев С. Веб-программирование (Обзорная статья) [Электронный ресурс] / С.Яковлев // IBM. – Режим доступа : http://wseweb.ru/diz/obzor3.htm.

12. Яковлев С. У истоков Apache: История и обзор архитектуры [Электронный ресурс] / С.Яковлев // IBM. – Режим доступа : http://www.ibm.com/developerworks/ru/library/os-apache_3/.

13. Обзор доступных возможностей IIS 7 [Электронный ресурс] // Microsoft Technet. – Режим доступа : http://technet.microsoft.com/ru-ru/library/cc753198(v=ws.10).aspx.

14. Ньюкомер Э. Веб-сервисы: XML, WSDL, SOAP и UDDI / Э.Ньюкомер. – СПб. : Питер, 2003. – 256 с.

Аннотация. Проанализировано типичный сценарий развертывания и функционирования интернет-сайта, который содержит незаконную информацию.

Ключевые слова: интернет-ресурс с незаконной информацией, ферма веб-серверов, веб-служба, регистрация интернет-сайта в службе DNS.

Abstract: The article analyzes the typical scenario of developing and functioning the website, containing illicit information.

Key words: web resourse containing illicit information, web-server farm, web-service, registration of web-site in DNS service.

УДК 32.1:303.4:711.122

КАЧИНСЬКИЙ Анатолій Броніславович

МАТЕМАТИЧНІ МЕТОДИ ВИЗНАЧЕННЯ ГРАНИЧНИХ ЗНАЧЕНЬ СТРУКТУРНО СКЛАДНИХ СИСТЕМ БЕЗПЕКИ

Постановка проблеми. Важливим кроком оцінки стану захищеності та діяльності суб'єктів забезпечення безпеки структурно складних систем є правильний вибір критеріїв безпеки. Ця оцінка не мусить бути дуже глибокою, оскільки самі критерії безпеки потребують вибору певних показників (індикаторів) безпеки. Для оцінки стану безпеки таких систем, зокрема національної безпеки, важливе значення мають не самі показники, а їхні граничні значення.

Аналіз останніх досліджень і публікацій. Сучасне суспільство із його системним баченням проблем безпеки, озброєне знаннями синергетики й нелінійної динаміки, намагається розробити такі критерії безпеки, що базуються на граничних значеннях, основу яких становлять уявлення про збере-