УДК 681.3

В. Ю. Зубок
Інформаційний центр «Електронні вісті»

Виявлення та протидія інформаційним атакам з мережі Інтернет

Досліджено методи вивчення ресурсів інформаційно-комутативних технологій (ІКТ) і використання їхніх вразливостей з метою нейтралізації інформаційного впливу супротивника в ході інформаційних атак, які частіше називають інформаційними операціями. Наведено схеми аналізу відкритих джерел і реальні приклади. Алгоритм дій з дослідження ІКТ-інфраструктури супротивника однаково придатний і для застосування тієї ж методики з метою аналізу власних вразливостей. Надано рекомендації щодо запобіжних заходів для ускладнення та уповільнення розвідки власної ІКТ-інфраструктури з боку супротивника.

Ключові слова: *інформаційні операції, Інтернет, мережна розвідка, мережні вразливості, відкриті джерела, сканування мереж.*

Вступ

Сьогодні інформація стає найважливішим стратегічним ресурсом, недостача якого призводить до істотних утрат у всіх областях життя. Раніше вважалося, що інформація всього лише забезпечує поінформованість людей про події й факти в навколишньому світі, тобто вона сприймалась як корисний ресурс, призначений для розширення людських можливостей. Наразі ж будь-який суспільний процес потребує обробки надзвичайної кількості інформації, і ця обробка вже давно є неможливою без інформаційно-комунікаційних технологій (ІКТ).

Щодня ми стаємо свідками того, що політичні, суспільні та бізнес-конфлікти переходять в площину інформаційних протиборств, які без перебільшення мають характер інформаційних війн. У класичному розумінні інформаційна війна — це одна з форм інформаційного протиборства, а точніше — комплекс заходів щодо інформаційного впливу на масову свідомість для зміни поведінки людей і нав'язування їм цілей, які не відповідають їхнім інтересам, а також захист від подібних впливів.

ІКТ-ресурси суперника стають одними з перших цілей, і часто — першими жертвами інформаційної війни. Глибоке проникнення всесвітньої комп'ютерної мережі Інтернет в життя суспільства неймовірно збільшує як можливості супротивників, так і їхні вразливості. Метою статті є показати шляхи для аналізу вразли-

востей власних ІКТ-ресурсів, способи запобігання та протидії використанню вразливостей ІКТ-ресурсів у ході «інформаційних операцій».

Поняття «інформаційні операції»

Термін «інформаційні операції» поширився завдяки численним документам і публікаціям Міністерства оборони США. Інформаційні операції визначаються як «*акції, спрямовані на вплив на інформацію та інформаційні системи супротивника, також захист власної інформації та інформаційних систем*» [1].

Інформація є відображенням вкладеного в неї змісту, а інформаційні системи обробляють інформацію, критичну для прийняття рішень. Тому сьогодні інформація перетворилася з абстрактного терміна в об'єкт, мету та засіб інформаційних операцій. Відповідно до польового уставу військового відомства США «Інформаційні операції» (FM 100-6), «*Орієнтація в ситуації означає комбінацію ясного представлення про диспозиції своїх і ворожих сил з оцінкою ситуації та намірів з боку командування»*. Рівень готовності до проведення інформаційних операцій сьогодні вважається ключовим фактором успіху проведення будь-якої соціальної процедури, кампанії.

Особливою метою при проведенні інформаційних операцій є інформаційно-аналітичні системи суб'єкта впливу. Здійснюючи вплив на такі системи, можна домогтися того, що особи з табору супротивника, що приймають рішення, робитимуть неадекватні висновки.

У цьому випадку до безпосередніх інформаційних впливів може бути віднесене розміщення в інформаційному просторі документів, що компрометують протилежну сторону, рекламу (у тому числі приховану) своїх переваг, перекручені дані про зовнішнє середовище, перекручену інформацію про наміри тощо.

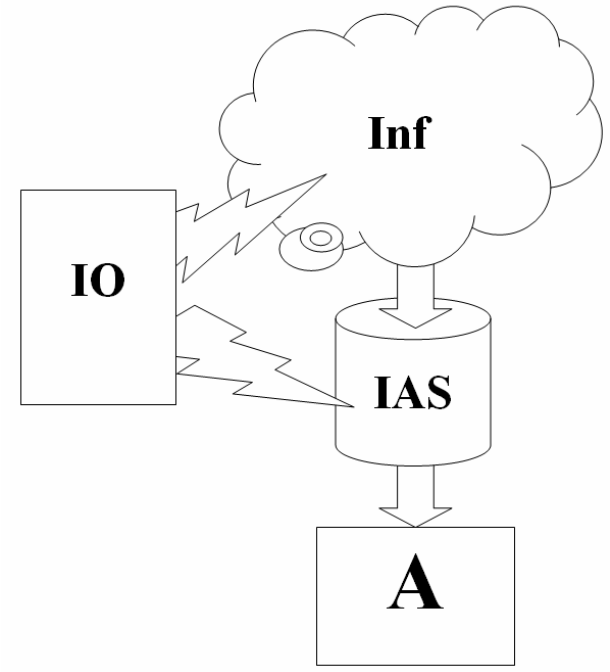


Рис. 1. Вплив на інформаційно-аналітичну систему супротивника:
Inf — інформаційний простір;
IAS — інформаційно-аналітична система;
A — абонент системи (особа, що приймає рішення);
IO — інформаційні впливи

Інформаційний вплив

Одним із основних методів ведення інформаційних операцій є інформаційний вплив, що надається з метою інформаційного керування — непрямого інформаційного впливу, коли об'єкту керування дається певна інформаційна картина, під впливом якої він формує лінію своєї поведінки.

Процес інформаційного впливу може бути розділений на такі етапи [2]:

— генерацію джерелом впливу даних, інформаційних елементів та інформаційних сукупностей;

— передачу інформації джерелом впливу;

— прийом інформації реципієнтом;

— генерацію сукупності даних, інформаційних елементів і нових сукупностей об 'єкта впливу;

— відповідні активні дії об'єкта впливу.

Інформаційні впливи на елементи систем можна класифікувати за такими ознаками, як джерела виникнення, тривалість впливу, природа виникнення тощо.

Для вибору конкретних способів реалізації інформаційного керування необхідно конкретизувати завдання, розв'язувані за допомогою інформаційного впливу, провести аналіз процесу формування інформаційних операцій і виробити критерії їхньої оцінки. Інформаційне керування розглядають як процес, що охоплює такі три взаємозалежні напрямки:

1) керування обміном даними між реальним світом і віртуальним світом суб'єкта впливу;

2) керування віртуальним світом суб'єктів впливу, механізмами прийняття рішень;

3) керування процесом перетворення рішень у дії суб'єкта впливу в реальному світі.

Інформаційний вплив може бути двох основних видів:

1) зміна в необхідний бік даних, які використовує інформаційно-аналітична система об'єкта впливу при прийнятті рішень;

2) безпосередній вплив на процес ухвалення рішення об'єкта впливу, наприклад, на процедури ухвалення рішення або окремих осіб, що приймають рішення.

Нейтралізація інформаційного впливу супротивника за допомогою атаки на ІКТ-ресурси

У XXI столітті вплив на ІКТ-ресурси супротивника в ході інформаційної операції може стати найпродуктивнішим знаряддям інформаційних війн. Втручання в технології передачі, обробки та зберігання інформації в автоматизованих системах може бути з метою:

— несвоєчасного потрапляння інформації до інформаційно-аналітичної системи (ІАС), а як наслідок — несвоєчасного аналізу інформації та реагування з боку абонента ІАС;

— затримки в обробці та розповсюдженні інформації, а як наслідок — несвоєчасного поширення інформації, яка породжена згідно рішень абонента ІАС; це може суттєво знизити ефективність соціального та суспільного впливу інформації, що мала бути поширена;

— постачання в ІАС хибної інформації шляхом несанкціонованого втручання в довірені канали постачання інформації, в тому числі підробки мережних атрибутів, електронних підписів і т.ін., що може вплинути на аналіз справжньої інформації та примусити абонента прийняти помилкові рішення;

— здобуття конфіденційної інформації стосовно супротивника шляхом несанкціонованого втручання в його автоматизовані системи чи шляхом впливу на певних користувачів автоматизованих систем супротивника, що мають доступ до конфіденційної інформації;

— розповсюдження хибної інформації від імені супротивника шляхом втручання в його канали розповсюдження та (або) підробки атрибутів джерела інформації.

З точки зору етапів реалізації інформаційної операції, її напрямків та видів, є цілком очевидним, що атака на ІКТ-ресурси, яка досягла мети, заважатиме реалізації одного, декількох чи всіх етапів інформаційного впливу супротивника за будь-яким з напрямків, які перелічені раніше. Крім того, успішна атака на ІКТ-ресурси водночас є дійовим засобом реалізації власного інформаційного впливу.

Пошук вразливостей ІКТ-ресурсів підчас інформаційних операцій

Процес інформаційної атаки через втручання в ІКТ може бути умовно розділено на три основні етапи: дослідження ІКТ-структури супротивника, аналіз вразливостей, використання вразливостей [3]. Дослідження ІКТ-структури організації починається ззовні, з використанням лише відкритої інформації. Наведемо декілька зразків на прикладі власного приватного домена автора.

Досліджуються пошукові системи WWW стосовно їхніх знань про відомі домени та IP-адреси об’єкта дослідження, участь користувачів з такими доменними та IP-адресами у різноманітних форумах (рис. 2). Також за допомогою пошукових систем можна знайти приховані сторінки сайтів, які колись були з’єднані з основними, але на момент дослідження не існує посилань на них з інших ресурсів.

Результати можуть бути приголомшливими. Так, на сайті однієї поважної організації було виявлено публічно доступні звіти proxy-сервера стосовно внутрішніх користувачів і перелік ресурсів, які вони відвідували.

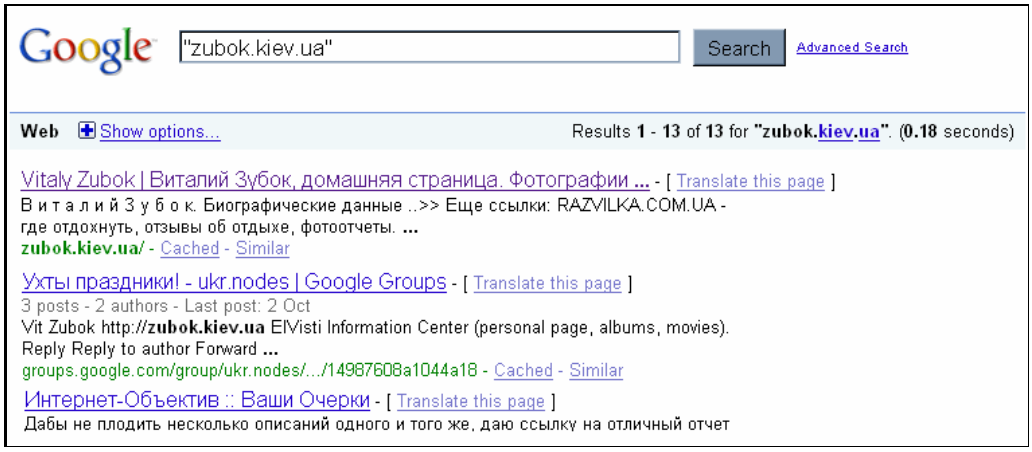
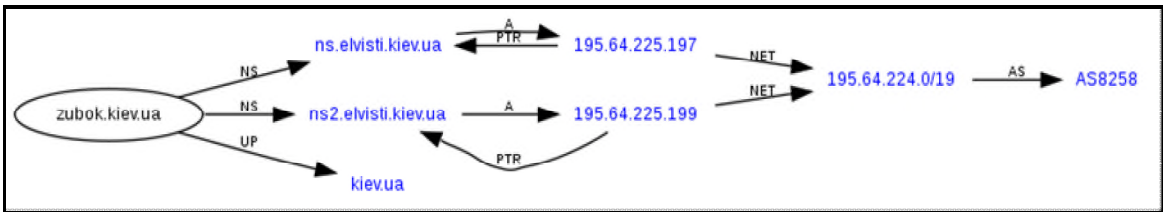


Рис. 2. Дослідження посилань за допомогою пошукових систем

Досліджуються публічні бази даних WHOIS, які належать адміністраторам публічних доменів, щоб з ’ясувати, де підключені авторитетні DNS та хто їх адмініструє. На рис. 3 наведено результат аналізу домена, який пропонує сайт www.robtex.com, у вигляді графа і таблиці.



а)

delegation information (beta) for zubok.org.ua

```
                                          +-cd1.ns.ua (194.0.1.9)
                                          |  +-he1.ns.ua (216.218.215.27)
                                          |  |  +-ho1.ns.ua (195.47.253.1)
                                          |  |  |  +-ns-ua.ripe.net (193.0.12.232)
                                          |  |  |  |  +-ns.uu.net (137.39.1.3)
                                          |  |  |  |  |  +-pch.ns.ua (204.61.216.12)
                                          |  |  |  |  |  |  +-sunic.sunet.se (192.36.125.2)
                                          |  |  |  |  |  |  |  +-ya1.ns.ua (77.88.210.88)
                                          |  |  |  |  |  |  |  |  +-ba1.ns.net.ua (72.20.97.27)
                                          |  |  |  |  |  |  |  |  |  +-ho1.ns.org.ua (195.47.253.10)
                                          |  |  |  |  |  |  |  |  |  |  +-ns.dn.ua (194.44.61.65)
                                          |  |  |  |  |  |  |  |  |  |  |  +-ns.net.ua (62.149.2.12)
                                          |  |  |  |  |  |  |  |  |  |  |  |  +-q.ns.org.ua (195.24.154.110)
                                          |  |  |  |  |  |  |  |  |  |  |  |  |  +-sns-pb.isc.org sns-pb.isc.org (192.5.4.1)
serial 2008070301                         |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  +-ns.elvisti.kiev.ua (195.64.225.197)
serial 2008070301                         |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  +-ns.secondary.net.ua (195.149.112.1)
                                          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
ns.secondary.net.ua   a   195.149.112.1   |  |  |  |  |  |  |  |  g  |  |  |  |  |  |  g  |
ns.dn.ua              a   194.44.61.65    |  g  g  g  g  g  g  g  |  |  |  |  |  |  |  |  |
ns.net.ua             a   62.149.2.12     |  g  g  g  g  g  g  g  |  |  |  |  |  |  |  |  |
ns.elvisti.kiev.ua    a   195.64.225.197  |  |  |  |  |  |  |  |  |  |  |  |  |  |  g  |
ba1.ns.net.ua         a   72.20.97.27     |  g  g  g  g  g  g  g  |  |  |  |  |  |  |  |  |
q.ns.org.ua           a   195.24.154.110  |  g  g  g  g  g  g  g  |  |  |  |  |  |  |  |  |
ho1.ns.org.ua         a   195.47.253.10   |  g  g  g  g  g  g  g  |  |  |  |  |  |  |  |  |
org.ua                ns  sns-pb.isc.org |  d  d  d  d  d  d  d  |  |  |  |  |  |  |  |  |
org.ua                ns  q.ns.org.ua    |  d  d  d  d  d  d  d  |  |  |  |  |  |  |  |  |
org.ua                ns  ns.dn.ua       |  d  d  d  d  d  d  d  |  |  |  |  |  |  |  |  |
org.ua                ns  ba1.ns.net.ua  |  d  d  d  d  d  d  d  |  |  |  |  |  |  |  |  |
org.ua                ns  ho1.ns.org.ua  |  d  d  d  d  d  d  d  |  |  |  |  |  |  |  |  |
org.ua                ns  ns.net.ua      |  d  d  d  d  d  d  d  |  |  |  |  |  |  |  |  |
zubok.org.ua          a   195.64.225.202  |  |  |  |  |  |  |  |  |  |  |  |  |  |  X  |  X
zubok.org.ua          ns  ns.secondary.net.ua  d  |  |  |  |  |  |  d  d  d  d  d  d  X  |  X
zubok.org.ua          ns  ns.elvisti.kiev.ua   d  |  |  |  |  |  |  d  d  d  d  d  d  X  |  X
LEGEND:
X - Provided in answer section
g - Glue record provided
d - Delegation
```

б)

Рис. 3. Аналіз DNS у вигляді графа (а) та таблиці ієрархії DNS (б) з сайту www.robtex.com

Досліджуються публічні бази даних регіонального Інтернет-реєстру (RIR), які керують наданням IP-адрес у певному регіоні, щоб з’ясувати які блоки IP-адрес пов’язані з мережею досліджуваного об’єкта, як вони взаємодіють з іншими провайдерами та хто їх адмініструє.

Аналізуються глобальні таблиці маршрутизації Інтернету, які є публічно доступними в багатьох центрах координації мережі. Інформація з серверів маршрутів і так званих «looking glass» дозволить виявити, до яких операторів підключена досліджувана мережа шляхом вивчення взаємодії автономних систем (AS), та навіть дізнатись, якими були ці зв’язки протягом останнього часу (рис. 4).

Наведений аналіз тим складніше, чим менше такої інформації дозволяє побачити організація. Нажаль, повністю приховати структуру неможливо, бо в багатьох випадках посилення захисту призводить до суттєвого або навіть неприйнтного ускладнення взаємодії ІКТ із зовнішнім світом — мережею Інтернет. Насамперед, неможливо приховати точки входу (IP-адреси) для повідомлень e-mail, DNS, адресу публічного веб-сайту. За необхідності та при наполегливості можна вирахувати доволі точне географічне розташування того чи іншого сервера.

AS number: 8258
IXP location: ALL
Time interval: 3 months
Output type: HTML Text
Search

The RIS database contains data until **2009-10-14 13:00:00 UTC**.

5 neighbors were found for AS8258

This AS was last seen by RIS on **2009-10-14 10:17:42 UTC**.

Number of Unique ASpaths found: 2277
Average Path Length: 7
Number of Unique Origin ASes: 4

Type	Neighbor AS	# ASpaths	Av. Path Length	# Origins	Last seen	First Seen	Last Seen ASpath
Left	21219	791	6	4	2009-10-14 10:17:42 UTC	2009-03-20 07:59:59 UTC	9002 21219 **8258** 13027
Right	13027	599	7	1	2009-10-14 10:17:42 UTC	2009-04-02 08:11:43 UTC	9002 21219 **8258** 13027
Right	43662	234	11	1	2009-09-27 05:27:37 UTC	2009-08-09 03:14:04 UTC	34695 3549 21219 **8258** 43662 43662 43662 43662 43662 43662
Left	21011	1486	8	4	2009-10-14 10:04:11 UTC	2009-06-23 07:59:56 UTC	29222 3303 21011 **8258** 13027
Right	39446	594	8	1	2009-09-16 09:59:21 UTC	2009-08-08 10:58:05 UTC	27664 16735 3549 174 21011 **8258** 39446

Рис. 4. Дослідження «провайдерських» зв'язків стосовно досліджуваних IP-адрес за останній час (з сайту www.ripe.net)

Після вивчення відкритої інформації атакуючою стороною, можливе застосування суто «хакерських» методів щодо випробування мережної інфраструктури та мережних служб на наявність відомих вразливостей, які можуть допомогти в реалізації інформаційної операції. Під «хакерськими» методами маються на увазі сканування адрес і мереж, спроби «брутального» підбору пароля, різноманітних атак, пов'язаних з проблемами реалізації комунікаційних протоколів в певному програмному забезпеченні атакованої мережі. Кінцевою метою атаки на ІКТ може бути отримання конфіденційної інформації, виведення з ладу (тобто недосяжність для легальних користувачів) певного сервісу, зміна інформації на офіційному сайті супротивника (deface). Все це має допомогти в реалізації мети всієї інформаційної операції, яка була наведена раніше і загалом визначається як атака на інформаційний вплив.

Якщо виконується тестування мережі великої організації, коли організація дозволяє побачити мінімум інформації, оцінювання безпеки великих мереж може стати досить довгим циклічним процесом. Крок за кроком, дані, отримані через витоки інформації, стосовно довірених доменних імен, IP-адрес, деталей обліко-

вих записів користувачів можуть бути передані до інших процесів для подальшого тестування. Блок-схема на рис. 5 окреслює цю процедуру і дані, що передаються між процесами [4].

Ця блок-схема включає складання «реєстру» (enumeration) мережі, масове сканування мережі, і, наприкінці, тестування специфічних сервісів. У процесі тестування аналітик може натрапити на неконтрольований сервіс DNS, що дозволить ідентифікувати попередньо невідомі блоки IP-адресс, які можуть бути знов «згодовані» процесу enumeration щоб ідентифікувати подальші компоненти мережі. Таким самим чином у публічно доступних директоріях аналітик може натрапити на декілька облікових записів, до яких може бути застосований метод підбору пароля.

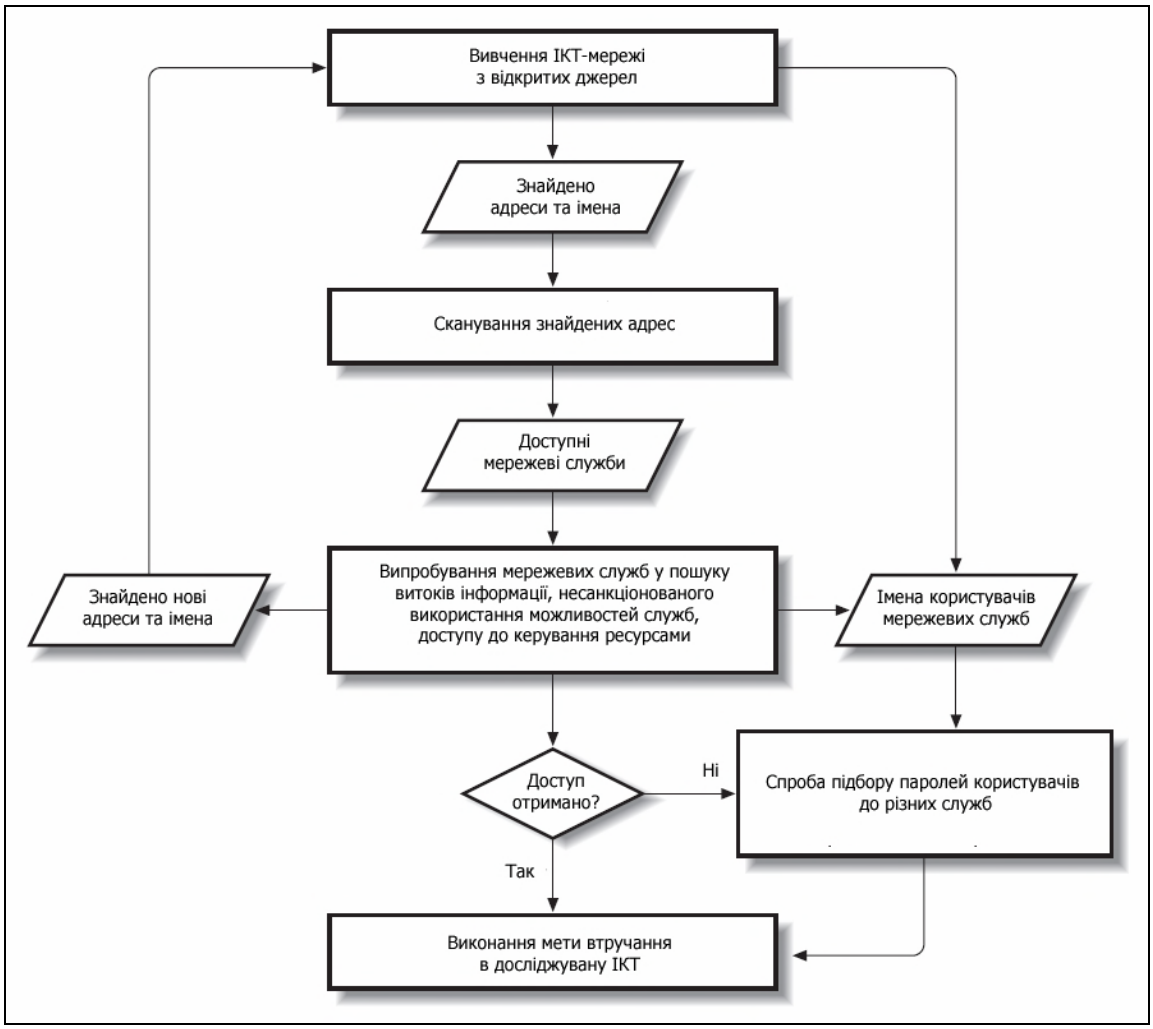


Рис. 5. Блок-схема алгоритму дослідження і втручання в інформаційно-комунікаційну мережу

Контрзаходи проти дослідження ІКТ-ресурсів

Очевидним є те, що при захисті власних ІКТ-ресурсів під час проведення інформаційних операцій першим завданням постає ускладнення роботи супротив-

ника щодо дослідження ІКТ-інфраструктури. Найбільш дієвим контрзаходом такому вивченню є доведення обсягу публічно доступної інформації до такого мінімуму, щоб стороннє оцінювання безпеки стало буквально нескінченним циклічним процесом. Щоб досягти цього, можна скористатися такими рекомендаціями:

1) публічно доступні веб-сервери не повинні містити чи видавати зайвого контенту:

— ніяких веб-документів, крім тих, до яких необхідний доступ зовнішніх користувачів;

— заборонити лістинг директорій (directory index);

2) поштові системи мають не деталізувати структуру поштової системи в заголовках e-mail;

3) у DNS не деталізувати, і тим більше не конкретизувати інформацію зворотнього резолвінгу стосовно будь-яких адрес, крім тих, що належать відкритим сервісам;

4) опубліковані контакти з адміністративних і технічних питань у БД адміністраторів доменів та IP-ресурсів повинні бути не персональні, а узагальнені (так звані «рольові»), для запобігання атакуванню окремої особи засобами соціальної інженерії.

Використовуючи схему, наведену на рис. 5, та спеціалізоване програмне забезпечення, можна самостійно перевіряти ступінь відкристості ІКТ-ресурсів організації до такого дослідження.

Висновки

Втручання в ІКТ-ресурси сьогодні є одним із дієвих засобів проведення інформаційних операцій і йому властива така ж етапність і схема проведення, що й більш традиційним операціям, які проходять за межами ІКТ.

Як і традиційна інформаційна операція, атака на ІКТ-ресурси може виявитись або вдалою, або невдалою. Для своєчасного виявлення атаки необхідно приділити увагу вивченню мережної активності, спроб сканування, відносного обсягу електронних листів із шкідливим контентом тощо. Для цього доречно використовувати і ретроспективний аналіз, тобто знаходження аналогів — операцій, що вже відбулися, вдалих або невдалих. Вжиття профілактичних запобіжних заходів, що направлені на ускладнення та уповільнення вивчення ІКТ-інфраструктури об'єкта атаки, суттєво знизить ефективність останньої.

1. *Information* Operations Roadmap — DoD US. — 30 October 2003. — 78 p.

2. *Фурашев В.М.* Інформаційні операції крізь призму системи моніторингу та інтеграції Інтернет-ресурсів / В.М. Фурашев, Д.В. Ланде // Правова інформатика. — 2009. — № 2(22). — С. 49–57.

3. *Klevinsky T.J.* Hack I.T. — Security Through Penetration Testing / T.J. Klevinsky, S. Laliberte, A. Gupta. — Addison -Wesley Professional, 2002.

4. *Chris McNab.* Network Security Assessment. — [2-nd ed.] / McNab. Chris. — O'Reilly, 2008.

Надійшла до редакції 04.11.2009