УДК 004.056

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 2, pp. 123-131

МОДЕЛЬ ФОРМУВАННЯ ДЕРЕВА АТАК ДЛЯ ОДЕРЖАННЯ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ І МЕРЕЖАХ ПРИ ВИЛУЧЕНОМУ ДОСТУПІ

В.Л. Бурячок

Військова частина А1906,
Україна; e-mail: bur@ukr.net

У статті, зважаючи на низку проблем, пов'язаних із забезпеченням продуктивності, надійності та стійкості функціонування інформаційно-телекомунікаційних систем, а також можливості несанкціонованого доступу до циркулюючих у таких системах інформаційних ресурсів, розглянуто один із можливих методів одержання інформації за рахунок формування дерева атак при вилученому доступі.

Ключові слова: інформація, дерево атак, інформаційно-телекомунікаційна система, інформаційно-комунікаційні технології, об'єкти інформаційної діяльності, несанкціонований доступ

Вступ

Наприкінці XX – початку XXI сторіччя завдяки глибоким системним перетворенням, викликаним синтезом перспективних інформаційно-комунікаційних технологій (ІКТ) та бурхливим розвитком інформаційно-телекомунікаційних (ІТ) систем і мереж у світі та Україні зокрема суттєво активізувалась робота за напрямами:

- виявлення інформаційних потреб та добору джерел інформації;
- пошуку та збору інформації у відкритих і відносно-відкритих, а також її добування із закритих електронних джерел;
- опрацювання інформації, оцінювання її повноти і значущості;
- подання інформації у зручному для користувачів вигляді та організації зворотного зв'язку з нею;
- використання інформації для оцінювання тенденцій, розробки прогнозів, оцінювання альтернатив рішень і дій, вироблення стратегій тощо.

Цьому сприяло створення спеціальних ІТ систем (СІТС), що мали високі споживчі якості та були здатні реалізовувати певні обчислювальні, відслідковувальні, запам'ятовувальні, комунікаційні, інформаційні, регулювальні, оптимізаційні, прогнозні, аналітичні та документувальні функції, зростання кількості та висока технологічність нових засобів і методів деструктивного впливу протиборчими сторонами на об'єкти інформаційної діяльності (ОІД) один одного, підвищення професіоналізму потенціальних порушників тощо.

Зважаючи на те, що масштаби застосування сучасних ІКТ останнім часом розширились до практично неосяжних меж поряд із проблемами забезпечення продуктивності, надійності та стійкості функціонування ІТС (СІТС) це визначило також й проблему несанкціонованого доступу (НСД) до циркулюючих у таких системах інформаційних ресурсів (ІР). З одного боку ця проблема нині обумовлюється, як відомо, посиленою увагою до безпеки ІТС (СІТС), а з іншого – неухильно

зростаючими збитками, які порушники завдають власникам ІР. Вирішити її, як показує статистика, можна за рахунок використання існуючих та розроблення нових методів і засобів несанкціонованого отримання інформації з таких систем.

Аналіз останніх досліджень і публікацій

Зазначене завдання у певних аспектах висвітлено в публікаціях як зарубіжних, так і вітчизняних авторів. Найвідомішими серед них є роботи А.В. Возженікова, В.І. Ярочкіна, Г. Почепцова, М. Лібіцкі, К.А. Мініхена, О. Шермана, Ф. Фукуями та інших фахівців. Проте аналіз цих та багатьох інших джерел свідчить, що комплексного оцінювання палітри методів і засобів несанкціонованого одержання інформації із СІТС до цього часу, нажаль, не проводилось. Зважаючи на те, що вирішення цього завдання достатньо суттєво залежить від використовуваної операційної системи (ОС), систем управління базами даних (СУБД) та мережевого програмного забезпечення (МПЗ), параметрів безпеки, а також інших факторів, воно потребує додаткового і більш глибокого вивчення.

Отже, актуальність статті зумовлено передусім обсягом інформації, що останнім часом надходить до користувачів із зовнішнього середовища та безперервно зростає, а також потребою підвищення вимог до захисту такої інформації від НСД. Важливою умовою розв'язання сформульованих вище проблем стає оперування єдиним понятійним апаратом у цій царині та знання специфіки процесів злому ІТ систем потенційними порушниками. Тому *мета* статті та її основний зміст саме й полягають у викладенні можливого варіанту (алгоритму) дій хакерів (крекерів тощо) щодо формування дерева атак для отримання доступу до спеціальних ІТС протиборчої сторони, тобто їх злому.

Виклад основного матеріалу

Враховуючи, що загальне програмне забезпечення будь-якої ІТС або СІТС складається з трьох основних компонент – ОС, СУБД та МПЗ [1], варіант несанкціонованого одержання інформації шляхом злому систем захисту цих компонент при вилученому доступі може бути поданий структурно-логічною схемою, наведеною на рисунку 1 [2].

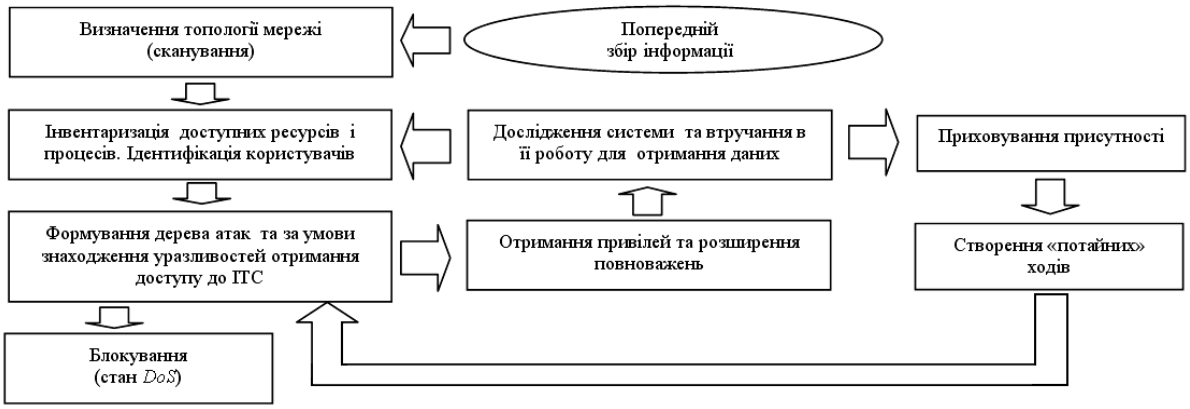

Рис. 1. Структурно-логічна схема методу несанкціонованого одержання інформації з ІТС (СІТС)

Головними дійовими особами цього процесу виступають внутрішні поодинокі інсайдери, або зовнішні організовані злочинні співтовариства – кіберугруповання хакерів (комп'ютерних професіоналів високого рівня, які в ході проникнення до СІТС жертви не здійснюють протиправних дій) і крекерів (хакерів, які застосовують свої знання для злому КМ явно з корисною метою), а також терористичні і розвідувальні організації, дії яких розгортаються як правило за таким типовим алгоритмом. *На першому кроці* порушниками проводиться так звана пасивна розвідка шляхом:

1) пошуку інформації про об'єкт розвідки та збору інформації про нього. Для цього порушники використовують відомі пошукові системи та/або спеціалізовані пошукові машини й працюють з відкритими джерелами в Internet, а саме: адресами й місцями розташування офісів на web-вузлах; інформацією про ділових партнерах; номерами телефонів та електронною поштою тощо. При цьому вони, як правило, ставлять собі за мету одержати відповіді на такі питання:

- ім'я домену або доменів об'єкта розвідки;
- адреси підмереж, якими він володіє;
- точні адреси вузлів, що знаходяться на периметрі мережі об'єкта розвідки та їх ролі;
- механізми мережної безпеки, використовувані об'єктом розвідки (міжмережні екрани, фільтруючі маршрутизатори, системи виявлення атак);
- сервіси та ОС, запущені на визначених вище вузлах, тощо.

Окрім цього порушники можуть збирати щодо об'єкта розвідки відомості про SNMP, таблиці маршрутизації та інші інформаційні і розвідувальні матеріали (відомості, дані);

2) зондування ІТС, тобто визначення комп'ютерів (ПЕОМ), підключених у цей момент до мережі Internet та прослуховування мережного трафіку. Ці операції порушники здійснюють з використанням *Traseroute*, *VisualRoute*, *NeoTrace* та інших ним подібних програм.

Запобігти діям порушників у проведенні пасивної розвідки допоможуть правильно налаштовані програмно-апаратні засоби виявлення вторгнень, а саме: маршрутизатори і брандмауери, а також програмні файєрволи.

Другим кроком дій порушників є активна розвідка, що передбачає:

- сканування мережі, тобто визначення її топології, з використанням *ping*-подібних утиліт. Кращими з них вважаються *Nmap*, *Ping Sweep* виробництва компанії *Solar Winds* та інші ним подібні програмні додатки;
- визначення відкритих портів у системі – тобто, точок входу в систему, установлених різними додатками й процесами, що очікують підключення. Для цих цілей порушниками використовуються, як правило, утиліти типу *Nmap*, *Super Scan*, *IP Eye*, *NetCat*, тощо;
- інвентаризацію користувальницьких ресурсів і облікових записів. Ці операції порушники можуть робити скориставшись *Win2K Resource Kit*, а також убудованими командами системи, такими як *net view*, *nbtstat* та ним подібними.

Запобігти діям порушників у проведенні активної розвідки допоможуть правильно й жорстко налаштовані списки на брандмауерах, обмеження доступу до відкритих портів, а також внесення змін у визначенні значення в реєстрі ОС.

Далі, *на третьому кроці*, якщо знайдені уразливості в СІТС жертви й таким чином отриманий доступ до неї, порушниками здійснюється сукупність заходів, що мають за мету саме зламування системи. Вони реалізуються шляхом:

- формування дерева атак (F_{atak});
- зламування та/або неправильного налаштування наявного ПЗ;
- використання сценаріїв автоматизації;
- розширення повноважень, тощо.

З метою ефективної реалізації процедури формування дерева атак її формалізована модель, з урахуванням пропозицій [3–6], може бути представлена кортежем (рис. 2):

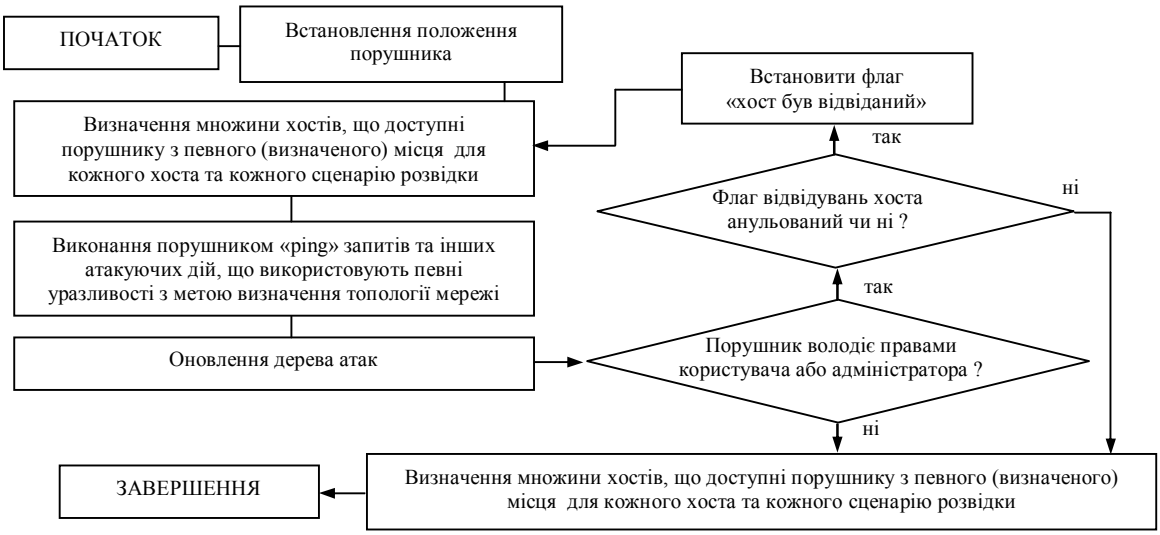

Рис. 2. Алгоритм формування дерева атак для визначеного положення порушника

$$F_{АД} = \left\langle M_{АД}^{об'єкт}, M_{АД}^{сценарій}, M_{АД}^{варіант} \right\rangle, \qquad (1)$$

де

$M_{АД}^{об'єкт}$ — компонент, що описує параметри процесу аналізу захищеності (АЗ), а саме рівень атакуючих дій і програмний код за рахунок якого ці дії можуть бути реалізованими та який визначає множину аналізованих об'єктів, мету виконання атакуючих дій, що може являти собою, наприклад, пару «об'єкт атаки – мета атаки» (наприклад, хост Workstation, «сканування портів») та параметри, що характеризують порушника $M_{П} = F\left(K_{пристр}^{мер}, K_{ОС+серв}^{відомі}, p_{поруш}^{положж}\right)$, де $K_{пристр}^{мер}$ — множина пристроїв у мережі; $K_{ОС+серв}^{відомі}$ — множина відомих порушнику ОС і сервісів; $p_{поруш}^{положж}$ — початкове положення порушника у мережі ($p_{поруш}^{положж} \in K_{пристр}^{мер}$);

$M_{АД}^{сценарій}$ — компонент, що описує сценарний рівень (рис. 3) й слугує для формування множини послідовності атакуючих дій з урахуванням мети, сформованої на рівні параметризації процесу АЗ, що повинна бути досягнута порушником. Формування сценаріїв атак здійснюється шляхом визначення та повного перебору всіх підцілей атакуючих дій цілі T (наприклад, ціль T – «розвідка», підцілі – «сканування портів», «визначення типу ОС», тощо);

$M_{АД}^{варіант}$ — компонент, що описує всі можливі варіанти виконання атакуючих дій порушником з урахуванням їх характеристик.

При цьому кожна з підцілей може бути коренем (вершиною) власного дерева атак і мати власний атрибут, наприклад, тривалість життя (визначає тривалість подій для цілей і підцілей), степінь конфіденційності (визначає імовірність досягнення цілі, якщо мета підцілі досягнута) тощо. За таких умов, наприклад, коренем (вершиною) дерева атак «Bypassing 802.1x» (рис. 4) може бути ціль T , що має за мету «Обхід 802.1x» [5].

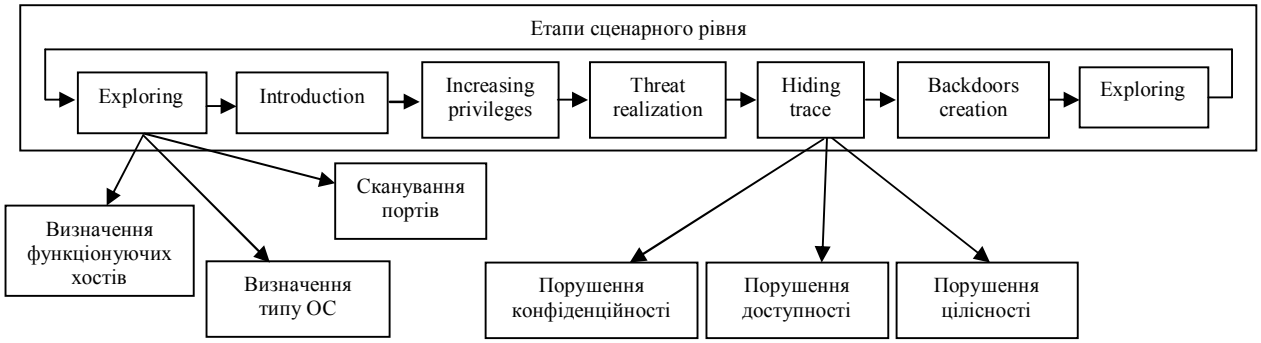

Рис 3. Фрагмент сценарного рівня з узагальненої моделі атак

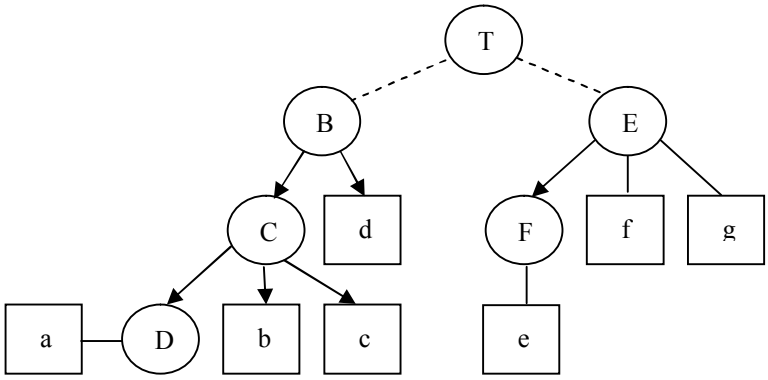

Рис. 4. Дерево атаки «Bypassing 802.1x»

Для її реалізації необхідно «Перехопити сеанс автентифікації 802.1x» (підціль B) або провести атаку «Людина посередині у сеансі 802.1x» (підціль E). Підціль B у свою чергу може бути досягнута за рахунок досягнення або підцілі C – «Відключення клієнта» (реалізувати яку, наприклад, для мережі WLAN можна виконавши атаки типу «Підміна АР» (підціль D), «Підслуховування MAC-адреси точки доступу» (підціль b), або «Відправлення повідомлення про відключення MAC-адреси» (підціль c)), або підцілі d – «Підміна автентифікованого клієнта 802.1x», тощо.

Підціль E у свою чергу може бути досягнута за рахунок підбору пароля або ж шляхом використання злоякісного (шпигунського) ПЗ і методів соціальної інженерії. Атрибути, що притаманні підцілям наведені у табл. 1.

Тобто, дане дерево має два можливі шляхи атаки, що означає два сценарії атаки для досягнення поставленої мети:

$$T\left(B\left(C\left(D\left(a\right),b,c\right),d\right)\right) \text{ та } T\left(E\left(F\left(e\right),f,g\right)\right).$$

З урахуванням пропозицій [4–6] компонент $M_{АД}^{варіант}$ може бути представлений таким кортежем:

$$M_{АД}^{варіант} = F\left(A, E, F^{АД}\right),$$

де

$A = \left\{U_i^{зовн}, U_i^{внутр}\right\}_{i=1}^{N_A}$ — множина всіх атакуючих дій N_A (являє собою сукупність внутрішніх $U^{внутр} = \left\langle S_m^{вн}, K, З^{безп}, П, O^k\left(C_m^k\right)\right\rangle$ і зовнішніх $U^{зовн} = \left\langle S_m^{зв}, K, З^{безп}, П, O^k\left(C_m^k\right)\right\rangle$

атак на СІТС, що використовують уразливості як програмних, так і технічних засобів системи);

$S^{зв}$ — зовнішнє джерело загрози;

$S^{вн}$ — внутрішнє джерело загрози;

K — комунікаційне обладнання у каналі зв'язку;

$З^{безп}$ — мережеві, хостові, параметричні сервіси безпеки на шляху розповсюдження атаки;

$П$ — протоколи; пакети;

O^k — об'єкт доступу;

C_m^k — сегмент СІТС, у якому обробляється інформація й найвищий рівень критичності якої дорівнює k;

m — номер сегменту;

$E = \{e_i\}_{i=1}^{N_e}$ — множина всіх вірусів (програмних кодів, виконання яких дасть можливість порушнику реалізувати атакуючу дію);

$F^{АД}$ — множина функцій даного компонента (складається з функції, яка дає можливість порушнику повернутися до виконання атакових дій, якщо поставлена ним мета не досягнута та функції, яка веде облік знань і умінь порушника, тобто, здатна з множини усіх атакових дій видалити ті, що в умовах свого виконання містять невідомі йому ОС та сервіси).

Таблиця 1.

Архітектура мережі та призначення її складових елементів

Підцілі	Сценарії атак	Атрибути тривалості життя
B	$T(B(C(D(a),b,c),d))$	4/4=1
C	$T(B(C(D(a),b,c),d))$	3/4=0.75
D	$T(B(C(D(a),b,c),d))$	1/4=0.25
E	$T(E(F(e),f,g))$	3/3=1
F	$T(E(F(e),f,g))$	1/3=0.33

Наповнення множин A та E, згідно [4] має здійснюватися на основі відкритих БД уразливостей, наприклад, Open Source Vulnerability Database або National Vulnerability Database (NVD), а також експертних знань (атакуючі дії етапів впровадження, підвищення привілеїв і реалізації загрози, пасивної і активної розвідки, приховування слідів, створення потайних ходів тощо). За таких обставин кожна атакуюча дія складатиметься з: високорівневого ідентифікатора; мети, що досягається виконанням даних дій; множини умов виконуваності; подання впливу на об'єкт, що атакується (послідовність мережевих пакетів, команд ОС, вірусів або експлойтів); множини результатів атакуючих дій; множини рекомендацій з усунення уразливостей.

Таким чином, наявність моделі формування дерева атак при реалізації власних процедур віддаленого доступу до ІТ і криптосистем протиборчої сторони дасть можливість: підвищити ймовірність подолання неавторизованим користувачем засобів захисту СІТС від вірусних атак та несанкціонованого одержання інформації з їх основних компонент таких, як ОС, СУБД та МПЗ; описати всі можливі варіанти виконання порушником атакуючих дій з урахуванням їх характеристик, представивши при цьому корінь дерева атак трійкою одиниць виду: «Стан СІТС на момент реалізації

АД, Атакуюча дія, Об'єкт АД». Оцінити рівень її складності можна з такого відомого виразу [4]:

$$F_{atak}(H_V) \le \begin{cases} K_{yrazl} \sum_{i=1}^{H_V-1} A_{\max}^{(i-1)} \frac{H_V!}{(H_V-i)!} \text{ при } H_V = H \\ K_{yrazl}\left[H \sum_{i=0}^{H_V-1} A_{\max}^{(i)} \frac{H_V!}{(H_V-i)!} + \sum_{i=1}^{H_V-1} A_{\max}^{(i-1)} \frac{H_V!}{(H_V-i)!} \right] \text{ при } H_V \ne H \end{cases} \quad (2)$$

де

H — множина аналізованих хостів у СІТС ($H = |K_H|$ — число хостів);

K_{yrazl} — число уразливостей у внутрішній базі даних;

$H_V \subset H$ — множина хостів у СІТС, що мають уразливості та дають можливість порушникові отримати права користувача або адміністратора ($H_V = |K_{H_V}|$ — число даних хостів);

A_{h_V} — кількість уразливостей на хості $h \in H_V$, що дають можливість порушникові отримати права користувача або адміністратора й перейти на даний хост ($A_{\max} = \max_{h \in H_V} A_{h_V}$ — максимальне число даних уразливостей по усім хостам аналізованої СІТС).

У подальшому з метою закріплення і розширення своїх привілей (повноважень) порушники можуть використати такі утиліти:

- реєстратори натискань клавіш – *Invisible Key Logger Stealth* (IKS);
- аналізатори мережевих пакетів – сніфери типу *BUTTSniffer*, *NetXRay*;
- утиліти перенацілювання портів *fpipe*, тощо.

Захистом від розширення повноважень на третьому кроці злому СІТС є застосування регулярно оновлюваних антивірусних пакетів, а також використання програм підраховування контрольних сум файлів.

На четвертому кроці завантажується шкідливе програмне забезпечення, результатом роботи якого має бути несанкціоноване отримання даних. При цьому з метою приховування своєї присутності порушники залишають так звані «потайні ходи», застосовуючи для цього, наприклад, такі команди ОС, як *attrib +h*, утиліти *Win2K Resource Kit*, набори «відмичок» – *rootkit* і програму *eLiTeWrap*.

На наступному, *п'ятому кроці* відбувається збереження результатів доступу. З цією метою порушниками застосовуються так звані «люки» (механізми усередині ОС або іншого ПЗ, що дають можливість їх програмам одержати привілейовану функцію або режим роботи, які не були їм дозволені) та програмне забезпечення типу «троянський кінь».

При цьому для вилученого адміністрування та об'єднання можливостей декількох програм з метою асинхронного й прихованого виконання певних деструктивних дій порушниками можуть бути використані так звані троянські коні типу *Net Bus*, *Sub Seven* та *Back Orifice*, а також методи тунелювання (DNS, HTTP, SNMP).

Захистом від дій порушників по несанкціонованому отриманню даних та подальшого збереження ними результатів доступу на четвертому і п'ятому кроках алгоритму може бути застосування програм, що підраховують контрольні суми файлів, відслідковують ведення журналів реєстрації подій та періодичність оновлювання антивірусних баз і системи у цілому.

Останнім кроком зловмисних дій порушників є замітання або інакше знищення ознак їх перебування в системі. Для цього порушники перезавантажують систему шляхом її «бомбардування» пакетами ICMP (*Smarf*-атака) або UDP (*Fraggle*-атака) з використанням посилюючої мережі й переводять її у стан DoS (*Denial of Service*).

Захистом від таких дій може бути встановлення фільтрів у програмно-апаратних файєрволах.

Висновок

Об’єктивною реальністю сьогодення є широке впровадження у сфери життєдіяльності особи, суспільства та держави у цілому сучасних ІКТ, розгортання на їх основі локальних і глобальних ІТС та мереж, об’єднання яких уже сьогодні складає основу нової інфраструктури планети – інфосфери. В Україні, нажаль, має місце низка проблем законодавчого і технічного характеру, які не дозволяють отримати всі переваги від розвитку ІКТ та впровадження ІТС, а інколи і перешкоджають таким процесам або призводять до неефективного використання засобів на їх розробку, впровадження і захист. До найбільш значущих серед них слід віднести:

- фактичну самоізоляцію України від міжнародного інформаційного співтовариства зважаючи на невідповідність законодавства і стандартів нашої держави світовим вимогам;
- відсутність сумісності між ІТС різних відомств і організацій України, що призводить до надмірності у зборі первинної інформації, подорожчання розробок і експлуатації таких систем;
- відсутність централізованої державної структури, що регламентує інформаційні процеси у нашому суспільстві тощо.

Дані проблеми суттєво впливають на створення комплексної системи захисту інформаційного і кіберпросторів України від внутрішніх і зовнішніх злочин і загроз, а також на можливість інтеграції нашої держави у світову інформаційну спільноту.

Список літератури

1. Анин, Б.Ю. Защита компьютерной информации [Текст] / Б.Ю. Анин. — Санкт-Петербург : БХВ, 2000. — 384 с.
2. Бурячок, В.Л. Варіант механізму злому інформаційно-телекомунікаційних систем та їх захисту від стороннього кібернетичного впливу / В.Л. Бурячок // Сучасний захист інформації. — 2011. — № 4. — С. 77–86.
3. Бурячок, В.Л. Основи формування державної системи кібернетичної безпеки [Текст] : монографія / В.Л. Бурячок. — К. : НАУ, 2013. — 432 с.
4. Котенко, И.В. Анализ защищенности компьютерных сетей на основе моделирования действий злоумышленников и построения графа атак [Текст] / И.В. Котенко, М.В. Степашкин // Труды Института системного анализа Российской академии наук. — 2008. — Т. 31. — С. 126–207.
5. Машкина, И.В. Управление и принятие решений в системах защиты информации [Текст] : учеб. пособие / И.В. Машкина. — Уфа : УГАТУ, 2007. — 160 с.
6. Степашкин, М.В. Оценка уровня защищенности компьютерных сетей на основе построения графа атак / И.В. Котенко, М.В. Степашкин, В.С. Богданов // Труды международной научной школы «Моделирование и анализ безопасности и риска в сложных системах (МАБР–2006)». — СПб., 2006. — С. 150–154.

МОДЕЛЬ ФОРМИРОВАНИЯ ДЕРЕВА АТАК ДЛЯ ПОЛУЧЕНИЯ ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ ПРИ УДАЛЕННОМ ДОСТУПЕ

В.Л. Бурячок

Военная часть А1906,
Украина; e-mail: bur@ukr.net

В статье, учитывая ряд проблем, связанных с обеспечением производительности, надежности и устойчивости функционирования информационно-телекоммуникационных систем, а также возможности несанкционированного доступа к циркулирующим в таких системах информационным ресурсам, рассмотрен один из возможных методов получения информации за счет формирования древа атак при удаленном доступе.
Ключевые слова: информация, дерево атак, информационно-телекоммуникационная система, информационно-коммуникационные технологии, объекты информационной деятельности, несанкционированный доступ

TREE ATTACKS FORMATION MODEL FOR REMOTELY ACCESS TO DATA IN INFORMATION AND COMMUNICATION SYSTEMS AND NETWORKS

Volodymyr L. Buryachok

A1906 Military Unit,
Ukraine; e-mail: bur@ukr.net

This article focuses on one of possible method for remotely access based on formation of tree attacks. Number of problems associated with the performance, reliability and sustainability of information and telecommunication systems, as well as the possibility of unauthorized access to such systems and circulating information resources are described.
Keywords: information, attack tree, information and telecommunication systems, information and communication technologies, information activity, unauthorized access