Державний університет інформаційно-комунікаційних технологій

СУЧАСНИЙ ЗАХИСТ ІНФОРМАЦІЇ

№4 , 2011

Україна, 03110, Київ,
(44) 248-86-01
вул. Солом'янська, 7

тел.: 380 (44) 248-86-07, 380

e-mail: duikt_szi@ukr.net

ЗМІСТ

Список литературы

1. Хорошко В.О. Методи керування і інформаційною безпекою / В.О. Хорошко., Я.В. Невойт., М.М. Дівізінюк., І.П. Шумейко., Ю.Ю. Гончаренко. Севастополь: Вип. СНУЯЄтаП. 2010. – 328с.
2. Андреев В.И. Проектирование систем технической защиты информации / В.И. Андреев., Ю.Ю. Гончаренко., М.М. Дивизинюк., И.НПавлов., В.А. Хорошко. Севастополь: Изд. СНУЯЭиП, 2011. – 235с.
3. Дидковский В.С. Акустическая экспертиза каналов речевой коммуникации /В.С. Дидковский., М.В. Дидковская., А.Н. Продеус. Киев, 2008. – 420с.

Рецензент: Ерохин В.Ф.
Поступила 14.09.2011

УДК 35.075.5+355.405.1+355.40 (477) **БУРЯЧОК В.Л.**

ВАРІАНТ МЕХАНІЗМУ ЗЛОМУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА ЇХ ЗАХИСТУ ВІД СТОРОННЬОГО КІБЕРНЕТИЧНОГО ВПЛИВУ

Постановка завдання у загальному вигляді

Сучасний етап у розвитку теорії і практики обміну інформацією характеризується головним чином інтенсивним впровадженням нових інформаційно-комунікаційних технологій (далі, ІКТ) та інформаційно-телекомунікаційних систем (далі, ІТ систем або ІТС). Поєднання їх функціональних можливостей забезпечує нині суттєве підвищення якості сучасного інформаційного обміну. Це проявляється, як правило, практично на усіх рівнях ієрархії, починаючи з архітектурного рівня *Internet* та *Intranet* у цілому, включаючи мережні технології (мережне програмне забезпечення тощо) й закінчуючи рівнем загальносистемних засобів і додатків (ОС, СУБД тощо).

Зважаючи на те, що масштаби застосування сучасних ІКТ останнім часом розширились до практично неосяжних меж такий стан справ, поряд із проблемами забезпечення продуктивності, надійності й стійкості функціонування ІТС, які у цей час обумовлюються зростанням кількості деструктивних впливів на такі системи та високою технологічністю їх виконання, підвищенням професіоналізму потенціальних порушників (неавторизованих користувачів, хакерів, крекерів тощо) та прийняттям ними на озброєння нових засобів і методів інформаційних впливів (зокрема "хакерських" методів) тощо, визначило також й проблему захисту від несанкціонованого доступу (далі, НСД) циркулюючих у цих системах інформаційних ресурсів (далі, ІР). З одного боку ця проблема обумовлюється, як відомо, посиленою увагою до безпеки ІТС, а з іншого – неухильно зростаючими збитками, які порушники завдають власникам ІР. Вирішити її, як показує статистика, можна нині такими основними способами:

використанням тільки убудованих в операційні системи (далі, ОС) і додатки засобів захисту;

застосуванням, поряд з убудованими, додаткових захисних програмно-апаратних механізмів.

Тим не менш, як стверджують висококваліфіковані фахівці у галузі розробки нових та впровадження існуючих ІКТ, адміністратори безпеки сучасних ІТС та співробітники відповідних експлуатаційних служб, ідеального й одночасно універсального способу захисту власних та/або корпоративних інформаційних ресурсів на цей час практично не існує. У цьому питанні все надзвичайно індивідуальне, й варіант захисту, найбільш близький до раціонального, весь час потребує оновлювання (доопрацювання). Тобто, за таких обставин виправдовується відома аксіома буття: те, що намагаються скрити одні – намагатимуться розкрити й кінець-кінцем обов'язково розкриють інші.

Аналіз останніх досліджень і публікацій

Окреслені вище проблемні питання висвітлено у багатьох публікаціях зарубіжних і вітчизняних авторів. Найвідомішими серед них є роботи К. Касперски, Дж. Куртца, М. Левіна, С. Мак-Клара, Дж. Скембрея, Д. Фері, Б.Ю. Аніна, С.В. Ленкова, Д.В. Склярова, В.О. Хорошка та інших фахівців [1-7]. Тим не менш аналіз публікацій у предметній області, що розглядається, свідчить про те, що комплексне дослідження проблеми організації та проведення можливих механізмів злому ІТС, а також методів, які при цьому застосовуються на цей час практично відсутнє. Тому, враховуючи реалії сьогодення, вона потребує додаткового і більш глибокого вивчення.

Актуальність та мета статті

Отже, актуальність статті обумовлена насамперед обсягом інформації, що останнім часом надходить до користувачів із зовнішнього середовища та безперервно зростає, а також підвищенням 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 злому спеціальних ІТС (далі, СІТС) потенціальної протиборчої сторони (жертви), його призначення та етапів.

Виклад основного матеріалу

Науково-технічна революція наприкінці XX початку XXI сторіччя викликала у світі глибокі системні перетворення. Вони, як результат, дали можливість завдяки синтезу перспективних ІКТ і бурхливого розвитку ІТС сформуватись та розвинутись принципово новим глобальним субстанціям – **інформаційному суспільству**, а також **інформаційному** і **кіберпросторам**, які мають нині практично необмежений потенціал і відіграють суттєву роль в економічному та соціальному розвитку будь-якої країни світу. Про важливість кіберпростору, як такого, свідчить:

по-перше, поява концепцій ведення **кіберборотьби** у ньому – комплексу заходів, спрямованих на здійснення управлінського та/або деструктивного впливу на ІТС противника й використовувані ним ІКТ й захисту від такого впливу власних систем і технологій, а також створення у збройних силах ряду країн світу спеціальних структур, призначених для ведення такої боротьби;

по-друге, необхідність забезпечення внутрішньої **кібербезпеки** – стану захищеності їх кіберпростору від ризику стороннього кібернетичного впливу, за якого забезпечується сталий розвиток цих країн, а також своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз їх особистим, корпоративним та/або національним інтересам.

Найбільш розповсюдженими формами протиправних діянь у кіберпросторі нині визнані **кіберзлочини** (фактично неприховані кримінальні дії, що здійснюються з використанням засобів електронно-обчислювальної техніки й за які передбачається юридична відповідальність) та **кіберзагрози** (прояви дестабілізуючого негативного впливу на певний об'єкт, що реалізуються за рахунок використання технологічних можливостей кіберпростору й створює небезпеку як для нього самого, так й для свідомості людини в у цілому). Вони здійснюються, як правило, внутрішніми поодинокими інсайдерами або зовнішніми організованими злочинними співтовариствами – кіберугрупованнями хакерів, крекерів та/або розвідувальних організацій, які мають за мету порушення штатного режиму функціонування (зламуванню) ІТ систем один одного (табл. 1) і реалізуються ними за рахунок використання комп'ютерної й іншої спеціальної техніки та програмного забезпечення (далі, ПЗ) шляхом проведення кібернетичних атак (далі, **кібератак**) і терактів. В цьому випадку у західній літературі під **хакерами** (*haker*) розуміють комп'ютерних професіоналів високого рівня, які в ході проникнення до ІТС жертви не

здійснюють протиправних дій, а під **крекером** (*cracker*) – хакерів, які застосовують свої знання для злому комп'ютерних систем явно з корисною метою.

Таблиця 1.

Об'єкти, що підлягають захисту, методи і засоби впливу на них та методи можливої протидії

Об'єкти	**Засоби впливу, Загроза**	**Можливі методи впливу**	**Методи протидії**
Системи зв'язку: цифрові комутаційні системи; системи утворення каналів	Блокування роботи системи (вузла) управління, втручання в роботу системи (вузла) управління	Віддалене програмування системи (вузла) управління, занесення вірусів до програмного забезпечення системи	Використання прог-рамного забезпечення систем, що має експертний висновок ДССЗЗІ, використання антивірусного програм-ного забезпечення
Канали зв'язку, канали передачі даних	Блокування каналів зв'язку та каналів передачі даних на транзитних вузлах	Втручання в роботу системи управління Центру управ-ління телекомунікаційними мережами ВАТ "Укртелеком"	Резервування каналів
Захищена система супутникового зв'язку	Блокування серверного обладнання та каналів супутникового зв'язку	Занесення вірусів до програмного забезпечення системи	Використання антиві-русного програмного забезпечення, блокування зовнішнього підключення до системи
Канали супутникового зв'язку	Блокування каналів супутникового зв'язку на транзитних вузлах	Втручання в роботу системи управління супутниковим зв'язком, занесення вірусів до ПЗ системи, використання передавачів завад	Резервування каналів, використання міжна-родних каналів супутни-кового зв'язку
КХ радіоканали спеці-ального радіозв'язку	Завади роботі радіозв'язку	Використання передавачів завад	Резервування каналів
Сервери АС класу "3"	Блокування роботи сервера, спотворення інформації	Подолання системи захисту сервера та втручання в його роботу	Створення комплексної системи захисту інфор-мації з підтвердженим атестатом
Сервери АС класу "2": ЛОМ	Блокування роботи сервера	Впровадження вірусних програм, програм шпигунів	

Об'єкти	**Засоби впливу, Загроза**	**Можливі методи впливу**	**Методи протидії**
АРМ АС класу "3"	Блокування роботи АРМ, спотворення інформації, її перехоплення та підміна	Впровадження вірусних програм, програм шпигунів	
АРМ АС класу "2": ЛОМ, що обробляють ІзОД	Блокування роботи АРМ, несанкціонований доступ до інформації, витік інформації технічними каналами, спотворення інформації	Впровадження вірусних програм, програм шпигунів, порушення порядку роботи користувачами	
АРМ АС класу "1", що обробляють ІзОД	Несанкціонований доступ до інформації, витік інформації технічними каналами, спотворення інформації		

З урахуванням пропозицій [8-10] здійсненню кібератак на ресурси ІТС, як відомо, притаманні чотири головні фази (рис. 1) – фаза пошуку потенціальних жертв (об'єктів розвідки), фаза проникнення через уразливі системи, фаза поширення атаки та фаза координованого керування засобами організації атаки, у ході реалізації яких дії потенціального порушника розгортаються за таким алгоритмом.

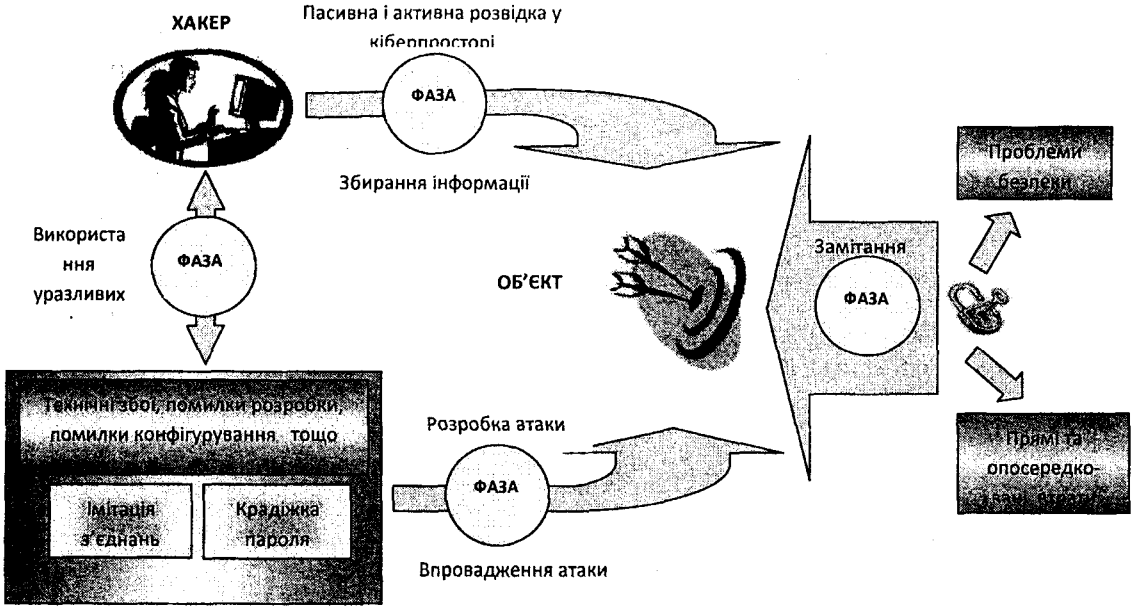

Рис. 1. Механізм злому СІТС

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*, *Net Cat* 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.

Формування дерева атак є однією із найбільш відповідальних процедур у діях порушників, оцінити рівень складності якої можна з виразу [13]:

$$F_{atak}(H_V) \le \begin{cases} K_{yrazl} \sum_{i=1}^{H_V-1} A_{\max}^{(i-1)} \dfrac{H_V!}{(H_V-i)!} & при \quad H_V = H \\ K_{yrazl}\left[H \cdot \sum_{i=0}^{H_V-1} A_{\max}^{(i)} \dfrac{H_V!}{(H_V-i)!} + \sum_{i=1}^{H_V-1} A_{\max}^{(i-1)} \dfrac{H_V!}{(H_V-i)!} \right] & при \quad H_V \neq H \end{cases},$$

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).

З метою ефективної реалізації процедури формування дерева атак кожна його вершина може бути представлена порушниками як трійка одиниць виду: "*NetworkState*, *Attack*, *Target*", де *NetworkState* – стан СІТС на момент реалізації атакуючої дії *Attack*, спрямованої на хост *Target* (рис. 2).

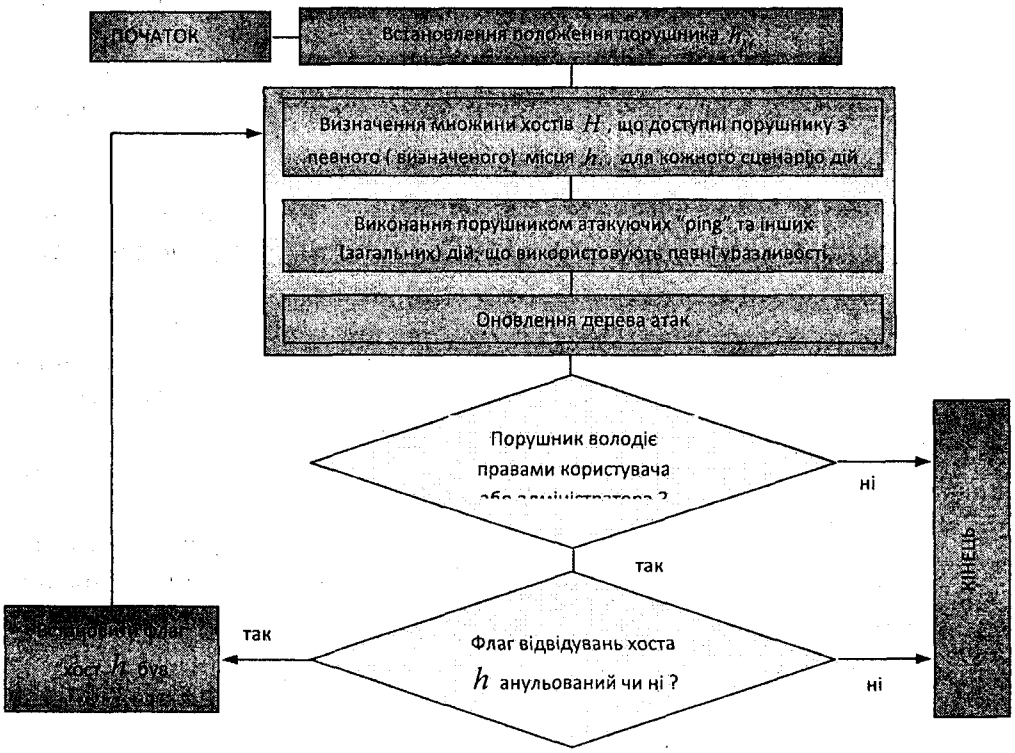

Рис. 2. Алгоритм формування дерева атак

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

реєстратори натискань клавіш - *Invisible Key Logger Stealth* (*IKS*);

аналізатори мережних 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 тунелірування (*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.

Зважаючи на те, що у загальному випадку ПЗ будь-якої СІТС складається з трьох основних компонент – ОС, системи управління базами даних (далі, СУБД) та мережного ПЗ (далі, МПЗ), всі спроби злому її системи захисту можна умовно розділити на три основні групи [2, 9, 10]: кібератаки на рівні СУБД, ОС та МПЗ. При цьому з метою розпаралелювання процесів оновлення загальнодоступних баз даних уразливостей та створення БД звичайних дій легітимних користувачів атаки на рівні ОС, МПЗ та СУБД доцільно поділяти на звичайні дії легітимних користувачів системи, а також дії, що використовують уразливості ПЗ і технічних засобів. Захист СУБД серед інших, наведених вище груп, вважається одним з найпростіших завдань [9, 10]. Це пов'язане з тим, що СУБД мають певну внутрішню структуру й визначену сукупність основних дій над елементами БД, що пов'язані з їх пошуком, вставкою, видаленням і заміною. Інші операції є допоміжними й застосовуються не так часто. Тим не менш існує два специфічних сценарію атак на СУБД, для захисту від яких доцільно застосовувати спеціалізовані методи. Їх головна ідея полягає у формуванні такого запиту до БД, щоб його результат складався з одного запису.

Враховуючи, що внутрішня структура сучасних ОС є надзвичайно складною – дотримання адекватної політики безпеки для них порівняно з захистом СУБД є завданням значно важчим. У цьому випадку мистецтво порушника полягає перш за все у його здатності знайти слабке місце в конкретній системі захисту певного об'єкту й, знаючи його архітектуру та конфігурацію, застосувати проти нього одну з відомих кібератак на кшталт:

сканування жорстких дисків комп'ютера (може бути організоване, наприклад, під ім'ям користувача, пароль якого хакеру відомий);

відновлення "сміття", вилученого з комп'ютера іншими користувачами;

крадіжки або підбору пароля доступу в ОС;

перевищення повноважень, які надані легальному користувачу відповідно до діючої політики безпеки;

запуску програми від імені користувача, що має на це необхідні повноваження;

модифікації коду або даних підсистем захисту самої ОС;

захоплення всіх наявних в ОС ресурсів та входження за рахунок цього у нескінченний цикл;

бомбардування ОС запитами, реакція на які вимагає залучення значних ресурсів;

відмови в обслуговуванні тощо.

Якщо адміністратор СІТС буде суворо дотримуватися політики безпеки, рекомендованої розробником ОС, а у ПЗ системи відсутні помилки, то усі перелічені вище атаки є мало ефективними.

Мережне ПЗ згідно з даними [9, 10] є найбільш уразливим для атак порушників. Це пояснюється тим, що канали зв'язку якими передаються повідомлення, частіш за все незахищені і тому практично кожний бажаючий може отримати до них доступ й, відповідно, може перехоплювати чужі повідомлення та відправляти по цих каналах власні. Враховуючи таке на рівні МПЗ можливе проведення хакерських атак типу: прослуховування сегмента локальної мережі; перехоплення повідомлень на маршрутизаторі; створення хибного маршрутизатора; нав'язування повідомлень; відмови в обслуговуванні тощо. Для їх відбиття необхідно захистити канали зв'язку шляхом: максимального обмеження розміру комп'ютерної мережі СІТС; ізолювання мережі від зовнішнього світу; шифрування мережних повідомлень та/або використання брандмауерів й електронного цифрового підпису тощо.

Типова архітектура системи виявлення цих та інших кібератак може бути представлена схемою, поданою на рис. 3. Вона поєднує в собі такі компоненти [11]: засоби збору інформації; засоби аналізу інформації; засоби реагування та засоби управління. Їх надійне і ефективне функціонування забезпечуються за рахунок впровадження автоматизованих робочих місць (далі, АРМ) або робочих станцій (далі, РСт), що створюються на базі персональних комп'ютерів (ПК), типового або спеціалізованого периферійного обладнання, а також відповідного програмного забезпечення й надають можливість здійснювати:

накопичення, систематизацію і опрацювання особистої інформації;

спільну роботу над загальними документами в складі структурного підрозділу;

доступ до власних та зовнішніх інформаційних ресурсів;

передачу та отримання кореспонденції по електронній почті тощо.

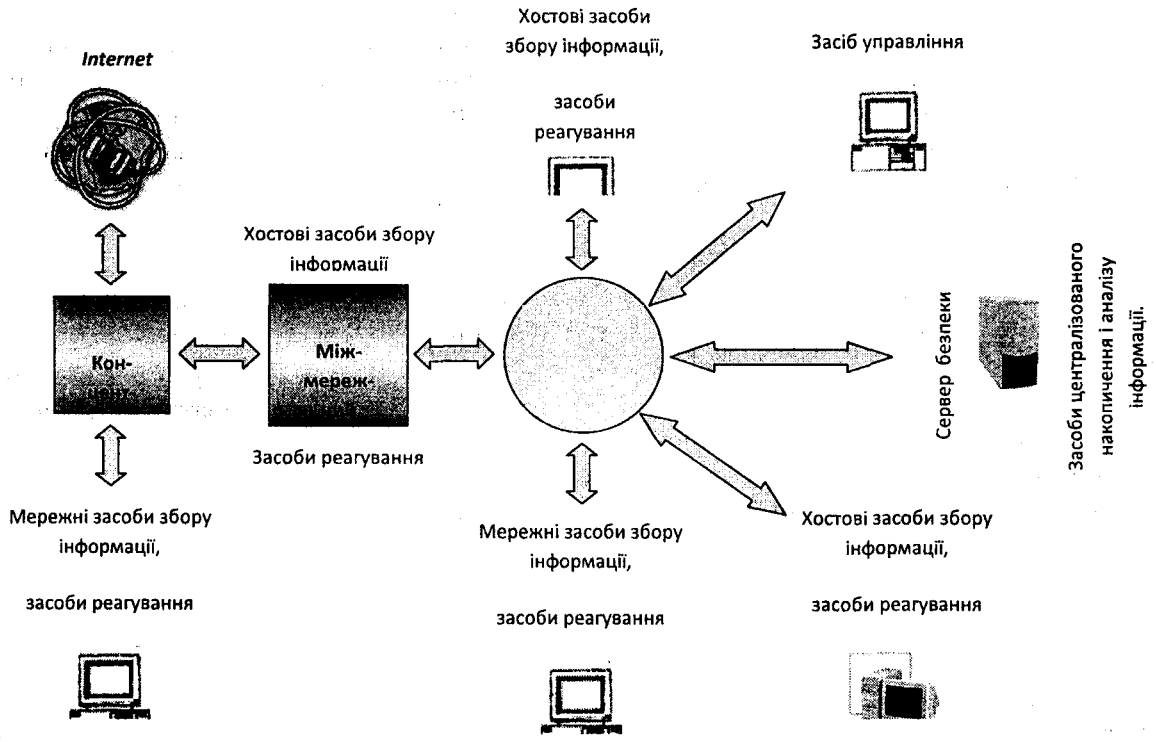

Рис. 3. Типова схема системи виявлення атак

При цьому мережні сенсори, згідно наведеної вище схеми, здійснюють перехоплення мережного трафіку. Хостові сервери у якості джерел інформації використовують журнали реєстрації подій ОС, МПЗ, СУБД та інших додатків. Інформація про події може бути отриманою хостовим сервером також безпосередньо від ядра ОС та/або мережного екрану.

Аналізатор, розміщений на сервері безпеки, здійснює централізоване збирання та аналіз інформації, отриманої від сенсорів. Засоби реагування можуть бути розташованими на станціях моніторингу мережі, мережному екрані, серверах та робочих станціях ЛОМ. При цьому типовий набір дій з реагування на атаки включає в себе:

оповіщення адміністратора безпеки (засобами електронної пошти, виведення повідомлень на консоль тощо);

блокування мережних сесій та користувальницьких реєстраційних записів з метою негайного припинення атак;

заповнення протоколу дій атакуючої сторони.

Засоби управління призначені для адміністрування усіх компонент системи виявлення атак, розробки алгоритмів виявлення і реагування на порушення безпеки, а також для огляду інформації про порушення та генерації звітів.

Формальна модель атак в межах описаних вище процесів з урахуванням пропозицій [12] може бути представлена в такий спосіб:

$$M_{KA} = F\left(M_{RF}^{РП}, M_{KA}^{РС}, M_{KA}^{АД}\right),$$

де $M_{RF}^{РП}$ - компонент, що описує рівень параметризації процесу аналізу захищеності (далі, АЗ) й слугує для завдання множини аналізованих об'єктів, цілей виконання атакуючих дій і параметрів, що характеризують порушника. Як правило він являє собою пару: об'єкт атаки - мета атаки, наприклад, (хост *Workstation* – "сканування портів");

$M_{KA}^{РС}$ - компонент, що описує сценарний рівень й слугує для формування множини різних сценаріїв (послідовності атакуючих дій) з урахуванням мети, сформованої на рівні параметризації процесу АЗ, що повинна бути досягнута порушником. При цьому формування сценаріїв здійснюється методом повного перебору всіх підцілей атакуючих дій цілі t, наприклад, ціль t – "розвідка", підцілі – "сканування портів", "визначення типу ОС" і т.д.);

$M_{KA}^{АД}$ - компонент, що описує всі можливі варіанти виконання атакуючих дій порушником з урахуванням його характеристик, включає також алгоритм формування дерева атак F_{atak}. Він у свою чергу може бути представлений у такий спосіб:

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

де $A = \{a_i\}_{i=1}^{N_A}$ - множина всіх атакуючих дій;

$E = \{e_i\}_{i=1}^{N_e}$ - множина всіх експлойтів;

$F^{АД}$ - множина функцій даного компонента.

При цьому наповнення множин A і E здійснюється на основі відкритих баз даних уразливостей, наприклад, *Open Source Vulnerability Database* або *National Vulnerability Database* (*NVD*) (атакуючі дії етапів впровадження, підвищення привілеїв і реалізації загрози), а також експертних знань (атакуючі дії етапів розвідки, приховування слідів, створення потайних ходів).

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. Денис Фери. Секреты супер-хакера.- СПб.: Издательский Дом "Невский прспект,1977.

2. Анин Б.Ю. Защита компьютерной информации. – СПб.:БХВ-Петербург, 2000. – 384 с. : ил.

3. Стюарт Мак-Клар, Джоел Скембрей, Джордж Куртц. Секреты хакеров. Безопасность сетей - готовые решения, 3-е издание. : Пер.с англ. - М. : Издательский дом "Вильямс", 2002. - 736 с. : ил.

4. Левин М. Библия хакера 2. Книга 1 (Книга 2). - М.: Майор, 2003. - 640 с. (- 688 с.)

5. Alex WebKnacKer. Быстро и легко. Хакинг и антихакинг: защита и нападение. Учебное пособие. - М.: Лучшие книги, 2004. - 400 с.: ил.

6. Скляров Д. В. Искусство защиты и взлома информации. – СПб.: БХВ-Петербург, 2004. – 288 с: ил.

7. Крис Касперски. Техника и философия хакерских атак – записки мыщ'а. – М.: СОЛОН-Пресс, 2004. – 272 с. : ил

8. Семёнов Ю.А. Обзор некоторых видов сетевых атак. [Електронний ресурс]. – Режим доступу: http://citforum.ru/nets/semenov/6/intrusion.shtml

9. Алексей Койнаш. Взлом и защита компьютерной сети: этапы и инструменты. [Електронний ресурс]. – Режим доступу: http://www.vlasnasprava.info/ru/business_az/how to_grow/protect.html?_m=publications&_t=rec&id=748

10. Методы взлома компьютерных систем. Електронний ресурс]. – Режим доступу:

11. Биячуев Т.А. / под ред. Л.Г.Осовецкого Безопасность корпоративных сетей. – СПб: СПб ГУ ИТМО, 2004. – 161 с.

12. Степашкин М.В. Оценка уровня защищенности компьютерных сетей на основе построения графа атак /И.В.Котенко, М.В. Степашкин // Труды международной научной школы "Моделирование и анализ безопасности и риска в сложных системах". – Спб., 2006. – С.150-154

Рецензент: РибальськийО.В.

Надійшла 22.09.2011

Мельник Н. Д., Кльок О.В., Паршуков С.С.

(Інститут спец. зв'язку та зах. інф.)

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ WMI ДЛЯ СТВОРЕННЯ АВТОМАТИЗОВАНОГО ОБЛІКУ НОСІЇВ ЕЛЕКТРОННОЇ ІНФОРМАЦІЇ

Технологія Windows Management Instrumentation (WMI) дозволяє за допомогою об'єктної моделі операційної системи та відповідних сценаріїв створити систему обліку використання зовнішніх носіїв, а структура таких сценаріїв буде повністю прозора.

Для виконання задачі обліку зовнішніх носіїв треба виконати наступні кроки: створити за допомогою технології WMI постійний споживач подій, який дозволить