НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

УДК 004.932:004.032.26

ПОГОДЖЕНО	**ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ**
Декан факультету	Завідувач кафедри
Інформаційних технологій	комп'ютерних систем, мереж та кібербезпеки
_____ / Болбот І.В., д.т.н, проф. /	_____ / Касаткін Д.Ю., к.пед.н., доцент. /
підпис ПІБ, вч. звання і ступінь	підпис ПІБ, вчене звання і ступінь
«___»_____2024 р.	«___»_____2024 р.

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему: **«Розробка рекомендацій та побудова комплексу оптимізації засобів захисту домашніх інформаційно-комунікаційних мереж»**

Спеціальність: 123 «Комп'ютерна інженерія»

Освітня програма: "Комп'ютерні системи захисту інформації"

Гарант освітньої програми
д.пед.н., професор _____ / Мамченко С.М./
науковий ступінь, вчене звання підпис ПІБ

Керівник магістерської кваліфікаційної роботи
д.пед.н., професор _____ / Мамченко С.М./
наук.ступінь, вч.звання підпис ПІБ

Виконав: _____ / Гуртовий В.О. /
підпис ПІБ

КИЇВ-2024

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ
І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

«ЗАТВЕРДЖУЮ»
завідувач кафедри
комп'ютерних систем, мереж та кібербезпеки
_____/ Касаткін Д.Ю., к.пед.н., доцент./
підпис ПІБ, вч. звання і н.ступінь
«__» _____ 2024 р.

ЗАВДАННЯ
ДО ВИКОНАННЯ
МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ СТУДЕНТУ

Гуртовий Володимир Олександрович
(прізвище, ім'я, по батькові)

Спеціальність (напрям підготовки): 123 «Комп'ютерна інженерія»
Освітня програма: " Комп'ютерні системи захисту інформації "

Тема магістерської роботи: «Розробка рекомендацій та побудова комплексу оптимізації засобів захисту домашніх інформаційно-комунікаційних мереж»
затверджена наказом ректора НУБІП України від " 1 " листопада 2023 № 1999 "С"
Термін подання завершеної роботи на кафедру _____
Вихідні дані до магістерської роботи: оптимізація засобів захисту домашніх інформаційно-комунікаційних мереж.
Перелік питань, що підлягають дослідженню:
1.Вирішення проблеми принципу захисту комп'ютерних ДІКС.
2.Класифікація комп'ютерних атак і систем їх виявлення.
3. Вибір розподіленої системи виявлення вторгнень.
4. Вирішення проактивної системи захисту інформації в ДІКС
Дата видачі завдання " 11 " листопада 2023 р.
Керівник кваліфікаційної роботи _____ / Мамченко С.М., д.пед.н., професор. /
(підпис) (ПІБ, вчене звання і ступінь)
Завдання прийняв до виконання _____ / Гуртовий В.О. /
(підпис) (ПІБ)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Постановка задачі магістерської роботи	15.11.2023	Виконано
2	Аналіз предметної області	13.04.2024	Виконано
3	Проектування системи	20.05.2024	Виконано
4	Реалізація системи	27.06.2024	Виконано
5	Тестування розробленої системи	11.09.2024	Виконано
6	Оформлення пояснювальної записки	18.10.2024	Виконано
7	Оформлення графічного матеріалу	26.10.2024	Виконано
8	Постерний передзахист	07.11.2024	Виконано

Студент _____ / Гуртовий В.О. /
підпис ПІБ

Керівник магістерської кваліфікаційної роботи _____ / Мамченко С.М./
підпис ПІБ

РЕФЕРАТ

Пояснювальна записка: 72 сторінок, 17 рисунків, 12 діаграм, 37 використаних джерел літератури та додаток.

Ключові слова: СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ДОМАШНЯ КОМП'ЮТЕРНА МЕРЕЖА, ЗАХИСТ МЕРЕЖЕВОГО ПЕРИМЕТРА, СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ.

Магістерська кваліфікаційна робота складається з вступу, трьох розділів, висновків та додатків.

Актуальність теми. Задачі підвищення ефективності забезпечення системи захисту інформації в домашній інформаційно-комунікаційній системі (ІКС), компонентів комп'ютерної мережі, інформаційна безпека, є актуальними.

Об'єкт та предмет дослідження. Домашня комп'ютерна мережа. Стан проблеми захисту інформації домашньої ІКС (ДІКС). Захист мережевого периметра комп'ютерної мережі. Захист комп'ютерної мережі від розподілених атак.

Мета дипломної роботи. Вирішення проблеми принципу захисту комп'ютерних ДІКС. Класифікація комп'ютерних атак і систем їх виявлення. Проактивна система захисту інформації в комп'ютерній мережі. Вибір розподіленої системи виявлення вторгнень. Вирішення проактивної системи захисту інформації в ДІКС.

Методи дослідження. Методи аналітичних оглядів і аналізів початкових даних для побудови вирішення проблеми принципу захисту комп'ютерних мереж та ДІКС. Основи побудови системи захисту мережевого периметру ДІКС. Технологія "медових пасток". *Honeypot* в системі безпеки промислового ДІКС. Розробка моделі конфлікту і аналіз стратегій атак та захисту. Динамічні характеристики процесу розвитку конфлікту з затягуванням у "медову пастку".

Матеріали дипломної роботи рекомендується використовувати при розробці системи захисту комп'ютерної мережі або ДІКС.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, ТЕРМІНІВ

СРЧ - Система реального часу

СМРЧ - Система м'якого реального часу

СЖРЧ - Система жорсткого реального часу

ЗМП - Захист мережевого периметра

МТ - Мережевий трафік

КА - Комп’ютерна атака

РСД - Рефлекторний список доступу

СВВ - Система виявлення вторгнень

ПСЗ - Практична система захисту

РА - Розподілена атака

ТМП - Технологія медових пасток

АСАЗ - Аналіз стратегій атаки та захисту

ВСТУП

Система захисту комп’ютерної мережі ДІКС має актуальне значення для ефективності функціонування мережі ДІКС.

Останнім часом в літературі з інформаційної безпеки відмічається тенденція до збільшення кількості порушень в області комп'ютерних злочинів. Спостерігається великий інтерес до методів аналізу та оптимізації систем захисту комп'ютерних та об'єднаних мереж від атак і несанкціонованих вторгнень. Наводиться велике число прикладів таких систем, розробок різних протоколів, технологій, проектів і пов'язаних з ними міркувань, висновків та прогнозів. З огляду на різноманітність загроз і складність сучасних мереж, реалізація рішення для захисту вимагає глибоких знань і досвіду в цілому ряді вузькоспеціалізованих дисциплін. У число поширених загроз входить умисне використання небезпечного програмного коду (вірусів, хробаків, троянських програм), а також атаки типу DoS (відмова в обслуговуванні) і DDoS (розподілена відмова в обслуговуванні).

Існує кілька ключових елементів забезпечення безпеки, які повинні знайти своє відображення в створюваній інфраструктурі захисту: управління доступом; управління погрозами; управління конфіденційністю; ведення контрольних журналів та моніторинг.

Дослідження в області виявлення атак на комп'ютерні мережі і системи ведуться вже давно. Досліджуються ознаки атак, розробляються і експлуатуються методи і засоби виявлення спроб несанкціонованого проникнення через системи захисту, як міжмережний, так і локальної - на логічному і навіть на фізичному рівнях. Насправді, сюди можна віднести також дослідження в області побічних електромагнітних випромінювань і наведень, оскільки електромагнітні атаки мають свої прямі аналоги в комп'ютерній мережному середовищі.

Не менш інтенсивно проводяться дослідження і в сфері захисту від комп'ютерних атак, розробки систем виявлення вторгнень і ін. На сьогодні системи виявлення

вторгнень і атак зазвичай являють собою програмні або апаратно-програмні рішення, які автоматизують процес контролю подій, що відбуваються в комп'ютерній системі або мережі, а також самостійно аналізують ці події в пошуках ознак проблем безпеки. Оскільки кількість різних типів і способів організації несанкціонованих проникнень в чужі комп'ютерні мережі за останні роки значно збільшилася, системи виявлення атак стали необхідним компонентом інфраструктури безпеки будь-яких установ, організацій і ДІКС.

Системи виявлення аномальної поведінки (anomaly detection) засновані на тому, що відомі деякі ознаки, що характеризують правильну або допустиму поведінку об'єкта спостереження. Під «нормальною» або «правильною» поведінкою розуміють дії, що виконуються об'єктом і не суперечать політиці безпеки. Системи виявлення злочинної поведінки (misuse detection) засновані на тому, що заздалегідь відомі деякі ознаки, що характеризують поведінку зловмисника. Найбільш поширеними методами виявлення злочинної поведінки є експертні та статистичні методи.

Системи виявлення атак, як і більшість сучасних програмних продуктів, повинні задовольняти ряду вимог. Це і сучасні технології розробки, і орієнтація на особливості сучасних інформаційних мереж, і сумісність з іншими програмами.

При побудові систем захисту комп'ютерних мереж треба враховувати наступні фактори:

- комп'ютерна мережа є територіально та функціонально розподіленою системою за визначенням;
- атаки на комп'ютерну мережу вельми різноманітні;
- більшість атак та несанкціонованих вторгнень, що здійснюється зловмисниками, також носять розподілений та узгоджений характер;
- найбільш небезпечними атаками на системи захисту інформації є такі, що мають чисто випадковий характер і є некорельованими у часі та просторі;

- силова протидія автономних термінальних вузлів мережі розподіленим атакам, як правило, не матиме успіху.

Наведені фактори впливу на належне функціонування комп'ютерних мереж загального призначення мають таке ж значення і для комп'ютерних мереж та ДІКС. Однак, комп'ютерні мережні системи захисту ДІКС мають свої принципові відмінності побудови, що випливають зі специфіки комп'ютерних мереж та систем, що забезпечують автоматизацію та роботизацію роботи ДІКС. Найбільш значуща відмінність – фактор часу. Комп'ютерні мережі та системи ДІКС завжди мають бути системами реального часу. Більш того, на ДІКСх критичного застосування використовуються виключно системи жорсткого реального часу.

Важливим фактором впливу на інформаційну безпеку ДІКС являється також наявність чи відсутність територіально віддалених філій та регіональних підрозділів. Якщо підприємство, як правило, має вельми довершену систему інформаційного захисту, то філії та канали обміну даними бувають захищені менше – за різними резонами, як об'єктивними, так і суб'єктивними.

З іншого боку, наявність територіально рознесених підрозділів ДІКС, які мають схожу архітектуру мережних сегментів, побудованих за однаковими стандартами та протоколами, дає можливість вдосконалювати усі вузли та елементи системи захисту. Тут велику роль грають організаційні заходи, на які треба звертати особливу увагу.

Виходячи з наведених міркувань, сформулюємо основні завдання дипломної роботи.

Провести докладний аналіз стану проблеми та невирішені задачі захисту комп'ютерної мережі ДІКС.

Намітити основні напрями розробки елементів системи захисту:

- мережний периметр вузлів та каналів передачі даних;

- брандмауери та маршрутизатори з фільтрацією пакетів;
- транслятори мережних адрес;
- транслятори адрес основних та альтернативних портів.

Розробити підсистему захисту від розподілених мережних атак:

- псевдосервіси з явними вразливостями ("медові пастки");
- мережні псевдосервіси з вразливостями (мережні "медові пастки").

Надати рекомендації з застосування різновидів систем силового, розподіленого захисту та псевдосервісів.

В результаті виконання дипломної роботи буде розроблено систему захисту комп'ютерної мережі з різними принципами протидії атакам та несанкціонованим вторгненням для промислового ДІКС критичного призначення.

РОЗДІЛ 1
СТАН ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ДІКС

Специфіка інформаційно-обчислювальних та управляючих мереж ДІКС суттєво відрізняється від специфіки інформаційних мереж загального призначення. Для того, щоб мати однозначне тлумачення цієї специфіки, основними характеристиками мереж підприємств, перш за все дамо перелік термінів та визначень, які застосовуються надалі. Джерелами являються закони України, постанови органів державного управління, розробки наукових закладів, монографії, дисертації тощо.

1.1. Терміни та визначення

ДІКС критичного призначення – це ДІКС, до яких висуваються наступні вимоги:

абсолютна надійність та безпека впродовж робочого дня або іншого терміну експлуатації (тиждень, місяць). Під абсолютним характеристиками розуміють характеристики, імовірність дотримання яких прагне до одиниці за обраний термін експлуатації;

живучість, тобто можливість працювати в агресивних середовищах, в умовах хімічного або бактеріологічного забруднення, за наявністю електромагнітного або радіаційного опромінення тощо;

спроможність виконувати свої функції у реальному часі, наприклад, у будь- яких умовах неперервно видавати продукцію без затримок та збоїв.

До таких підприємств відносяться ваіаційні та ракетно-космічні комплекси, ДІКС металургічної, хімічної, транспортної галузей, енергетичні (зокрема, атомні електростанції) та інші системи.

Система реального часу – апаратно-програмний комплекс, який реагує в передбачувані часи на непередбачуваний потік зовнішніх подій.

Система м'якого реального часу – затримка реакції не критична, хоча і може привести до збільшення вартості результатів і зниження продуктивності системи в цілому.

Приклад - робота мережі. Якщо система не встигла обробити черговий прийнятий пакет, це призведе до тайм-ауту на передавальній стороні і повторної посилці (в залежності від протоколу). Дані при цьому не втрачаються, але продуктивність мережі знижується.

Система жорсткого реального часу не допускають ніяких затримок реакції системи ні за яких умов, оскільки:

результати можуть виявитися марні в разі запізнення,

можуть бути катастрофічні наслідки у разі затримки реакції,

вартість запізнення може бути нескінченно велика.

Приклади систем жорсткого реального часу – бортові системи управління, системи аварійного захисту, реєстратори аварійних подій

Основна відмінність між системами жорсткого і м'якого реального часу можна виразити так: система жорсткого реального часу ніколи не запізниться з реакцією на подію, система м'якого реального часу – не має спізнюватися з реакцією на подію.

Інформаційно-обчислювальні та управляючі мережі ДІКС – це комп'ютерні та телекомунікаційні, проводові або бездротові мережі будь-яких різновидів. Їх об'єднує одна властивість – усі мережі повинні функціонувати у реальному часі. Для підприємств загального застосування це може бути м'який

реальний час, для підприємств критичного призначення – жорсткий реальний час.

1.2 Принципи захисту комп'ютерних мереж та ДІКС

Поняття інформації нерозривно пов'язане з комп'ютерними технологіями, системами і мережами зв'язку, то стає очевидною важливість питання захисту інформації в них. Добросовісна конкуренція передбачає суперництво, засноване на дотриманні законодавства та загальновизнаних норм моралі. Однак нерідко підприємці, конкуруючи між собою, прагнуть за допомогою протиправних дій отримати інформацію на шкоду інтересам іншої сторони і використовувати її для досягнення переваги на ринку. Криміналізація суспільства і недостатня ефективність державної системи охорони правопорядку змушує представників економіки, виробництва та бізнесу самим вживати заходів для адекватного протистояння негативним процесам, які сприяють витоку конфіденційної інформації.

Причин активізації комп'ютерних злочинів і пов'язаних з ними економічних, матеріальних та репутаційних втрат досить багато. Істотними з них є:

- перехід від традиційної "паперової" технології зберігання і передачі відомостей на електронну і недостатній при цьому розвиток технології захисту інформації в таких технологіях;

- об'єднання обчислювальних систем, створення глобальних мереж і розширення доступу до інформаційних ресурсів;

- збільшення складності програмних засобів.

Останнім часом в сучасних оглядах з інформаційної безпеки простежується тенденція до збільшення кількості порушень в області комп'ютерних злочинів. З огляду на різноманітність загроз і складність сучасних мереж, реалізація рішення для захисту вимагає глибоких знань і досвіду в цілому ряді вузькоспеціалізованих дисциплін. У число поширених загроз входить умисне

використання небезпечного програмного коду (вірусів, хробаків, троянських програм), а також атаки типу DoS (відмова в обслуговуванні) та DdoS (розподілена відмова в обслуговуванні).

Існує кілька ключових елементів забезпечення безпеки, які повинні знайти своє відображення в створюваній інфраструктурі захисту: управління доступом; управління погрозами; управління конфіденційністю; ведення контрольних журналів та моніторинг.

Вельми важливе значення для захисту інформації, яка циркулює в комп'ютерних мережах ДІКС, має визначення найбільш небезпечних комп'ютерних атак та розробка систем виявлення та протидії атакам. Розглянемо цу питання більш докладно.

1.3 Класифікація комп'ютерних атак і систем їх виявлення

Ефективний захист від потенційних сеті вих атак неможлива без їх детального класифікації, що полегшує їх виявлення і завдання протидії їм. В даний час відносно велика кількість різних типів класифікаційних ознак. Як та ких ознак може бути вибрано, напри заходів, поділ на пасивні і активні, зовнішні і внутрішні атаки, свідомі й несвідомі і т.д. На жаль, незважаючи на те, що деякі з існуючих класифікацій мало застосовні на практиці, їх активно використовують при виборі і експлуатації систем виявлення атак і вторгнень.

Розглянемо класифікацію комп'ютерних атак, яка досить широко застосовується у державних організаціях з захисту конфіденційної інформації:

віддалене проникнення (англ. *remote penetration*) – тип атак, які дозволяють реалізувати віддалене управління комп'ютером через мережу;

- локальне проникнення (англ. *local penetration*) – тип атак, які приводять до отримання несанкціонованого доступу до вузла, на який вони направлені;

- віддалена відмова в обслуговуванні (англ. *remote denial of service*) - тип атак, які дозволяють порушити функціонування системи в рамках глобальної мережі;

- локальна відмова в обслуговуванні (англ. *Local denial of service*) - тип атак, що дозволяють порушити функціонування системи в рамках локальної мережі. Як приклад такої атаки можна привести впровадження і запуск ворожої програми, яка завантажує центральний процесор нескінченним циклом безглуздих запитів, що призводить до неможливості обробки запитів інших додатків;

- атаки з використанням мережних сканерів (від англ. *Network scanners*) - це тип атак, заснованих на використанні мережних сканерів - програм, які аналізують топологію мережі і виявляють сервіси, доступні для атаки;

- атаки з використанням сканерів вразливостей (від англ. *Vulnerability scanners*) - тип атак, заснованих на використанні сканерів вразливостей - програм, які здійснюють пошук вразливостей на вузлах мережі, які в подальшому можуть бути застосовані для реалізації мережних атак;

- атаки з використанням зломщиків паролів (від англ. *Password crackers*) - це тип атак, які засновані на використанні зломщиків паролів - програм, що підбирають паролі користувачів;

- атаки з використанням аналізаторів протоколів (від англ. *Sniffers*) - це тип атак, заснованих на використанні аналізаторів протоколів - програмах, прослуховуючих мережний трафік. З їх допомогою можна автоматизувати пошук в мережному трафіку такої інформації, як ідентифікатори і паролі користувачів, інформацію про кредитні картки і т.д.

Наведена класифікація (рис. 1.1) є досить повною з практичної точки зору, оскільки вона охоплює майже всі можливі дії зловмисника. Однак для протидії мережним атакам цього недостатньо, тому що її використання в даному вигляді не дозволяє визначати елементи мережі, схильні до дії тієї чи іншої атаки, а

також наслідки, до яких може привести успішна реалізація атак. В такому випадку не включається в аналіз найважливіший компонент, а саме - модель загроз безпеки, з побудови якої повинні починатися всі заходи щодо забезпечення захисту інформації.

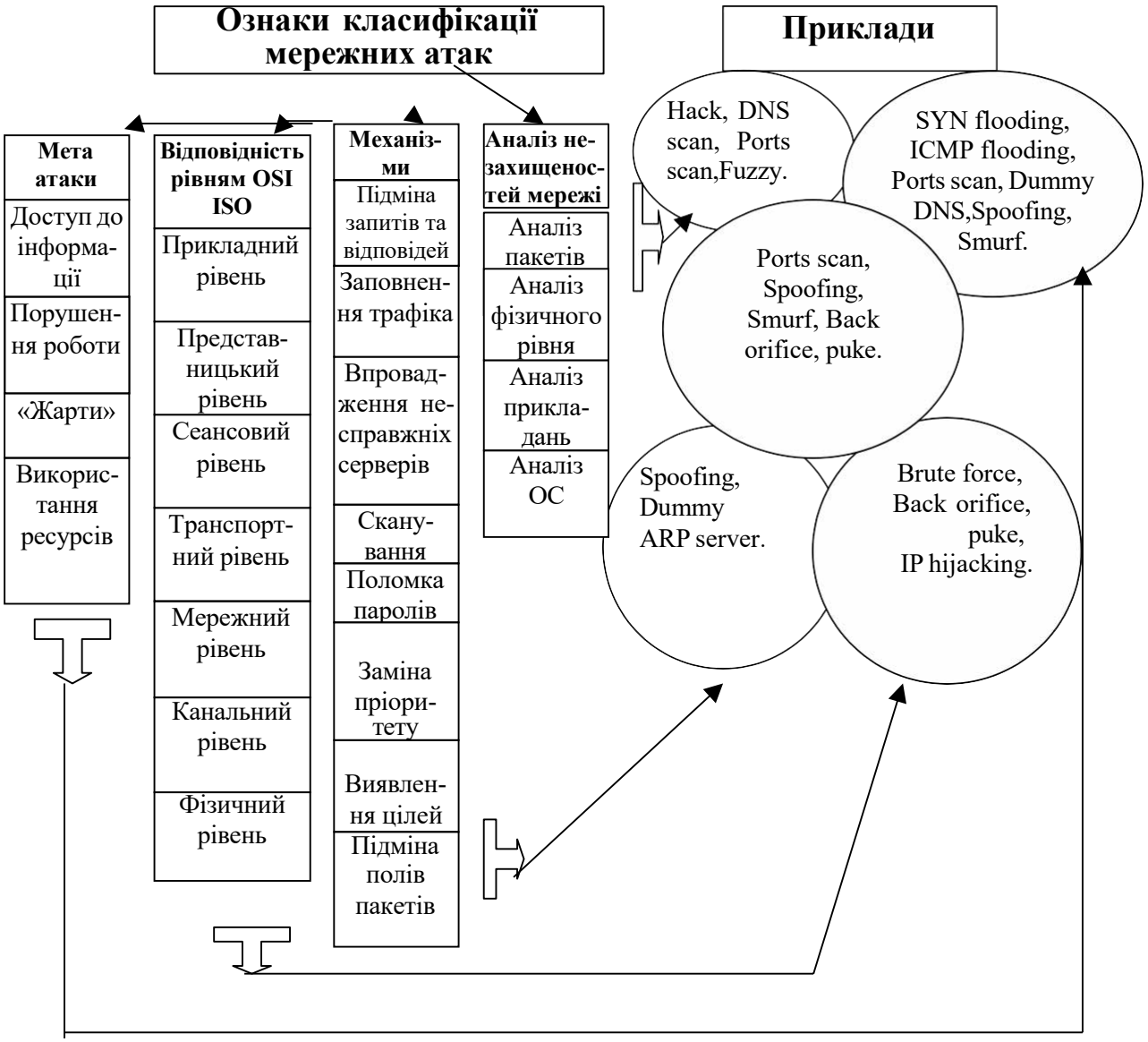

Рис. 1.1 Класифікація мережних атак різних рівнів

До можливих загроз мереж ДІКС треба віднести також наступні. Аналіз мережного трафіку

Аналіз трафіку є одним із способів отримання паролів і ідентифікаторів користувачів в мережі Internet. Аналіз здійснюється за допомогою спеціальної програмі - аналізатора пакетів (*sniffer*), перехоплює всі пакети, що передаються

по сегменту мережі, і виділяє серед них ті, в яких передаються ідентифікатор користувача і його пароль.

У багатьох протоколах дані передаються у відкритому, незашифрованому вигляді. Аналіз мережного трафіку дозволяє перехоплювати дані, передані по протоколах *FTP і TELNET* (паролі і ідентифікатори користувачів), *HTTP* (*Hypertext Transfer Protocol* - протокол передачі гіпертекстових файлів - передача гіпертексту між WEB-сервером і браузером, в тому числі і вводяться користувачем у форми на web -сторінках дані), *SMTP*, *POP3*, *IMAP*, *NNTP* (електронна пошта та конференції) і *IRC -Internet Relay Chat* (*online*-розмови, *chat*). Так можуть бути перехоплені паролі для доступу до поштових систем з web-інтерфейсом, номери кредитних карт при роботі з системами електронної комерції і різна інформація особистого характеру, розголошення якої небажано.

В даний час розроблені різні протоколи обміну, що дозволяють захистити мережне з'єднання і зашифрувати трафік. На жаль, вони ще не змінили старі протоколи і не стали стандартом для кожного користувача. Певною мірою їх поширенню завадили існуючі в ряді країн обмеження на експорт засобів сильної криптографії. Через це реалізації даних протоколів або не вбудовувалися в програмне забезпечення, або значно послаблялися (обмежувалася максимальна довжина ключа), що призводило до практичної марності їх, так як шифри могли бути розкриті за прийнятний час.

Аналіз мережного трафіку дозволяє:

1. По-перше, вивчити логіку роботи розподіленої обчислювальної системи, тобто одержати взаємно однозначне відповідність подій, що відбуваються в системі, і команд, що пересилаються один одному її об'єктами, в момент появи цих подій (якщо проводити подальшу аналогію з інструментарієм хакера, то аналіз трафіку в цьому випадку замінює і трассировщик). Це досягається шляхом перехоплення і аналізу пакетів обміну на канальному рівні. Знання логіки роботи розподіленої обчислювальної системи дозволяє на практиці моделювати і

здійснювати типові віддалені атаки, розглянуті в наступних пунктах на прикладі конкретних розподілених ВС.

2. По-друге, аналіз мережного трафіку дозволяє перехопити потік даних, якими обмінюються об'єкти розподіленої ВС. Таким чином, віддалена атака даного типу полягає в отриманні на віддаленому об'єкті несанкціонованого доступу до інформації, якою обмінюються два мережних абонента. Відзначимо, що при цьому відсутня можливість модифікації трафіку і сам аналіз можливий тільки всередині одного сегмента мережі. Прикладом перехопленої за допомогою даної типової віддаленої атаки інформації можуть служити ім'я і пароль користувача, що пересилаються в незашифрованому вигляді по мережі.

За характером впливу аналіз мережного трафіку є пасивним впливом Здійснення даної атаки без зворотного зв'язку веде до порушення конфіденційності інформації всередині одного сегмента мережі на канальному рівні *OSI* При цьому початок здійснення атаки безумовно по відношенню до мети атаки.

Підміна довіреного об'єкта або суб'єкта розподіленої обчислювальної мережі

Однією з проблем безпеки розподіленої обчислювальної мережі є недостатня ідентифікація і аутентифікація її віддалених один від одного об'єктів. Основна складність полягає в здійсненні однозначної ідентифікації повідомлень, переданих між суб'єктами і об'єктами взаємодії. Зазвичай в розподілених ЗС ця проблема вирішується таким чином: в процесі створення віртуального каналу об'єкти РВС обмінюються певною інформацією, унікально ідентифікує даний канал. Такий обмін зазвичай називається "рукостисканням" (*handshake*). Однак, відзначимо, що не завжди для зв'язку двох віддалених об'єктів в розподіленій обчислювальної мережі створюється віртуальний канал. Практика показує, що найчастіше, особливо для службових повідомлень (наприклад, від маршрутизаторів) використовується передача одиночних повідомлень, які не потребують підтвердження.

Як відомо, для адресації повідомлень в розподілених ЗС використовується мережну адресу, який є унікальним для кожного об'єкта системи (на канальному рівні моделі OSI - це апаратний адресу мережного адаптера, на мережному рівні - адреса визначається в залежності від використовуваного протоколу мережного рівня (наприклад, *IP*- адреса). Мережна адреса також може використовуватися для ідентифікації об'єктів розподіленої обчислювальної системи. Однак мережна адреса досить просто підробляється і тому використовувати його в якості єдиного засобу ідентифікації об'єктів неприпустимо.

На рис. 1.2 наведені основні підходи до побудови систем виявлення атак

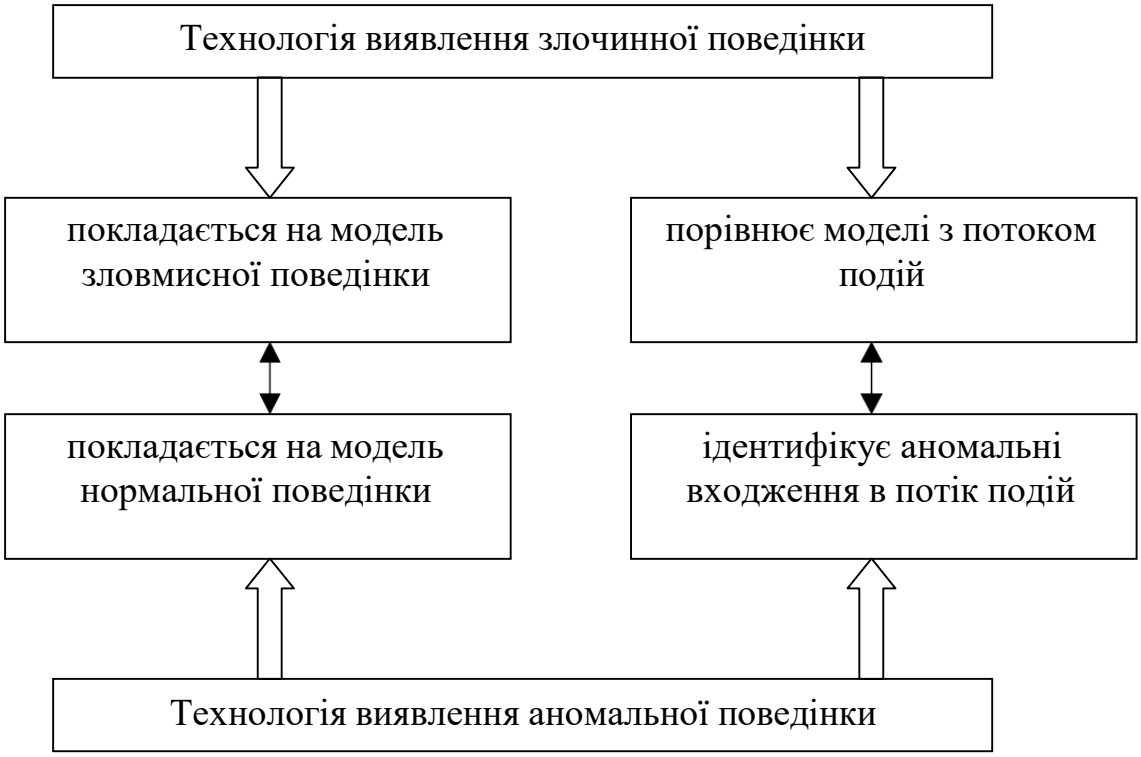

Рис. 1.2. Основні підходи до побудови систем виявлення атак

При побудові систем захисту комп'ютерних мереж треба враховувати наступні фактори:

комп'ютерна мережа є територіально та функціонально розподіленою системою за визначенням;

атаки на комп'ютерну мережу вельми різноманітні;

більшість атак та несанкціонованих вторгнень, що здійснюється зловмисниками, також носять розподілений та узгоджений характер;

найбільш небезпечними атаками на системи захисту інформації є такі, що мають чисто випадковий характер і є некорельованими у часі та просторі;

силова протидія автономних термінальних вузлів мережі розподіленим атакам, як правило, не матиме успіху.

Наведені фактори впливу на належне функціонування комп'ютерних мереж загального призначення мають таке ж значення і для комп'ютерних мереж та систем підприємств. Однак, комп'ютерні мережні системи захисту підприємств мають свої принципові відмінності побудови, що випливають зі специфіки комп'ютерних мереж та систем, що забезпечують автоматизацію та роботизацію роботи ДІКС. Найбільш значуща відмінність – фактор часу. Комп'ютерні мережі та системи ДІКС завжди мають бути системами реального часу. Більш того, на ДІКСх критичного застосування використовуються виключно системи жорсткого реального часу[1].

Важливим фактором впливу на інформаційну безпеку ДІКС являється також наявність чи відсутність територіально віддалених філій та регіональних підрозділів. Якщо головне підприємство, як правило, має вельми длвершену систему інформаційного захисту, то філії та канали обміну даними бувають захищені менше – за різними резонами, як об'єктивними, так і суб'єктивними.

З іншого боку, наявність територіально рознесених підрозділів ДІКС, які мають схожу архітектуру мережних сегментів, побудованих за однаковими стандартами та протоколами, дає можливість вдосконалювати усі вузли та елементи системи захисту. Тут велику роль грають організаційні заходи, на які треба звертати особливу увагу.

Статистичний аналіз комп'ютерних атак

[1] Терміни та визначення, що не є загально відомими та широко вживаними, наведені у відповідному підрозділі.

Системи виявлення вторгнень (*IDS*) дуже швидко стали ключовим компонентом будь-якої стратегії мережного захисту. За останні кілька років їх популярність значно зросла, оскільки продавці засобів захисту значно поліпшили якість і сумісність своїх програм. Основою систем виявлення вторгнення є аналіз. У процесі аналізу про-розглядати кожен пакет, визначається, чи є він шкідливим, і оголошується тривога в випадку необхідності, що є основними завданнями *IDS*. В даний час з'явилися два різних методу *IDS*. Обидва методи мають своїх шанувальників, використовують для свого просунення рясний маркетинговий матеріал з вигідними для себе прикладами. Але, незважаючи на це, кожен метод має і свої слабкі сторони. Розглянемота порівняємо їх, слідуючи роботі [1]

Детерміновані методи аналізу комп'ютерних атак

Аналіз сигнатур і аналіз протоколів

1. Основні поняття систем виявлення вторгнень (*IDS*). Ці пристрої, подібно міжмережним екранам (*firewall*), перевіряють весь вхідний і вихідний мережний трафік. Принциповою відмінністю від *firewall* є те, що вони не змінюють потік трафіку, скоріше, вони шукають зловмисний трафік, який може означати можливий напад або неправомірне використання, і оголошують тривогу для системного адміністратора.

Другий метод аналізу полягає в розгляді строго форматованих даних трафіку мережі, відомих як протоколи. Кожен пакет супроводжується різними протоколами. Автори IDS, знаючи це, впровадили інструменти, які розгортають і оглядають ці протоколи, згідно зі стандартами або *RFC*. Кожен протокол має кілька полів з очікуваними або нормальними значеннями. Якщо що-небудь порушує ці стандарти, то ймовірна зловмисність. *IDS* проглядає кожне поле всіх протоколів вхідних пакетів: *IP*, *TCP*, і *UDP*. Якщо є порушення протоколу, наприклад, якщо він містить несподіваного значення в одному з полів, оголошується тривога. Аналіз протоколу використовує детальне знання про

очікувані або нормальних значеннях в полях пакета, для того щоб виявити шкідливий трафік. Перші версії таких *IDS* були вкрай примітивні і обманювалися елементарно. Аналіз протоколу дуже відрізняється від аналізу підпису, який використовує відомі характеристики атак для оголошення тривоги.

Системи аналізу сигнатури мають кілька важливих сильних сторін. По-перше, вони дуже швидкі, тоді як повний аналіз пакету - досить важка задача. Правила легко написати, зрозуміти і налаштувати. Крім того, є постійна підтримка комп'ютерного співтовариства в швидкому виробництві сигнатур для нових небезпек. Ці системи перевершують всі інші при вилові хакерів на первинному етапі: прості атаки мають звичку використовувати якісь попередні дії, які легко розпізнати. Нарешті, аналіз, заснований на сигнатурі, точно і швидко повідомляє, що в системі все нормально (якщо це дійсно так), оскільки повинні відбутися якісь особливі події для оголошення тривоги.

З іншого боку *IDS*, яка грунтується тільки на аналізі сигнатур, має певні слабкості. Будучи спочатку дуже швидкою, з часом швидкість її роботи буде сповільнюватися, оскільки зростає число перевіряються сигнатур. Це - суттєва проблема, оскільки число перевіряються сигнатур може рости дуже швидко. Фактично, кожна нова атака або дія, придумане атакуючим, збільшує список перевіряються сигнатур. Не допоможуть навіть ефективні методи роботи з даними і пакетами: величезна кількість злегка змінених атак можуть прослизнути через таку систему.

У разі аналізу протоколів маємо аналогічну ситуацію: ця система теж має свої позитивні і негативні сторони, але зовсім інші. Через предпроцессов, що вимагають ретельної експертизи протоколів, аналіз протоколу може бути досить повільним. Крім того, правила перевірки для системи протоколу важко написати і зрозуміти. Можна навіть сказати, що в цьому випадку доводиться сподіватися на сумлінність виробника програми, так як правила щодо складні і важкі для самостійного налаштування. Більш того, правила стають все більш і більш

складними, часто ігнорують загальноприйняті стандарти, протоколи і *RFC*, що створює додаткову проблему розробникам *IDS* і дає шанс для зловмисника.

На перший погляд, *IDS* на основі аналізу протоколу працюють повільніше, ніж системи на основі сигнатури, вони більш «грунтовні» в сенсі масштабності і результатів. Крім того, ці системи шукають «генетичні порушення» і часто можуть відловлювати найсвіжіші "експлоїти нульового дня", що в принципі не можуть робити системи на основі аналізу сигнатур. На жаль, подібні системи можуть іноді пропускати, очевидно, ненормативні події, типу *root Telnet session*, які не порушують жодного протоколу. Системи на основі протоколу зводять помилкові тривоги до мінімуму, так як вони реєструють реальні порушення. На жаль, вони часто не забезпечують достатню кількість інформації. Замість цього, вони просто перекладають тягар відповідальності за виниклу аномалію на адміністратора [1]

На перший погляд два методи виявлення вторгнення - аналіз сигнатур і аналіз протоколу, здаються вельми різними, але ретельне вивчення проблеми показує їх деяку схожість. Зрештою, ці інструменти безпеки досліджують відформатовані дані про атаки і аномаліях.

Обидва розглянутих методи, по суті, є детермінованими. Їх слабкість, окрім уповільнення з ростом числа можливих загроз, заключається в неможливості виявлення вперше створених нових загроз, так званих експлоїтів сьогоднішнього дня.

Альтернативою детермінованим методам сигнатурного аналізу та аналізу протоколів є статистичні методи з використанням байєсівського, мінімаксного підходів та методу максимальної правдоподібності. Застосування методів статистичного аналізу є найбільш поширеним видом реалізації технології виявлення аномальної поведінки. Статистичні сенсори збирають різну інформацію про типову поведінку об'єкта і формують її у вигляді профілю.

Профіль в даному випадку - це набір параметрів що характеризують типову поведінку об'єкта. Існує період початкового формування профілю. Профіль формується на основі статистики об'єкта, і для цього можуть застосовуватися стандартні методи математичної статистики, наприклад метод ковзних вікон і метод зважених сум. У подальшому зупинимося на розгляді статистичних методів виявлення вторгнень, атак та протидії зловмисникам. [1-44].

1.4. Висновки до розділу

Розглянуто стан проблеми захисту інформації ДІКС.

Проаналізовано інформаційно-обчислювальні та управляючі мережі ДІКС – це комп'ютерні та телекомунікаційні, проводові або безпроводові мережі будь-яких різновидів. Їх об'єднує одна властивість – усі мережі повинні функціонувати у реальному часі. Для підприємств загального застосування це може бути м'який реальний час, для підприємств критичного призначення – жорсткий реальний час.

Розглянути принципи захисту комп'ютерних мереж підприємств.

Проаналізовано класифікація комп'ютерних атак і систем їх виявлення. Ефективний захист від потенційних сеті вих атак неможлива без їх детального класси фікації, що полегшує їх виявлення і завдання протидії їм. В даний час відо стно велика кількість різних типів класифікаційних ознак.

РОЗДІЛ 2

ЗАХИСТ МЕРЕЖЕВОГО ПЕРИМЕТРА КОМП'ЮТЕРНОЇ МЕРЕЖІ ДІКС

2.1. Основи побудови системи захисту мережного периметру

Мережний периметр – це укріплена границя мережі, що може включати:

- маршрутизатори;
- брандмауери;
- систему виявлення вторгнень (*IDS*);
- пристрої віртуальної приватної мережі (*VPN*);
- програмне забезпечення;
- демілітаризовану зону (*DMZ*) і екрановані підмережі [2].

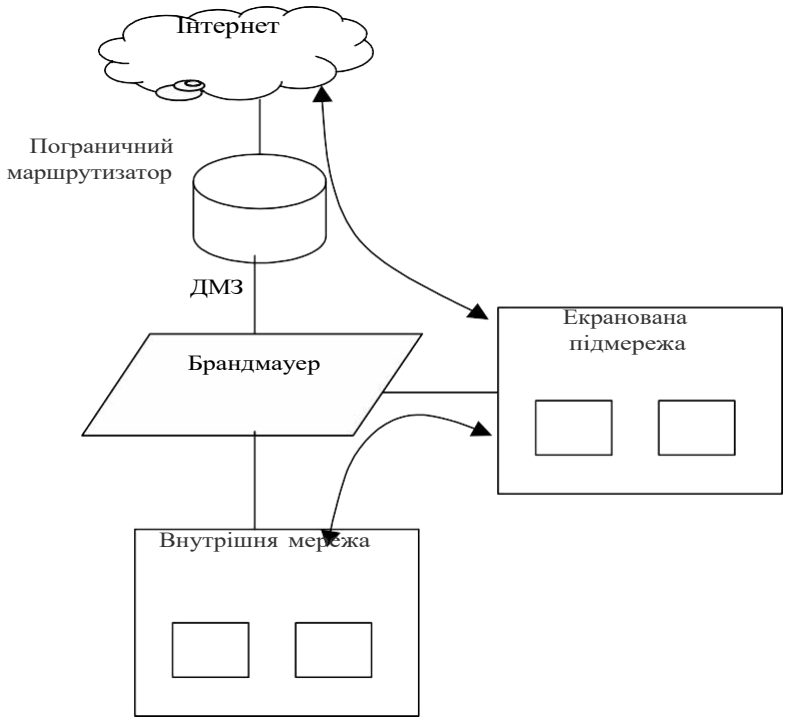

Рис. 2.1. Компоненти захисту мережного периметра

Демілітаризована зона розміщена перед брандмауером, екранована підмережа ізольована від внутрішньої мережі, однак для неї все-таки необхідний захист, що може надати брандмауер.

Маршрутизатори здійснюють розпізнавання та керування трафіком, що надходить у мережу або виходить з мережі, та внутрішнім трафіком, що циркулює усередині самої мережі. Маршрутизатор прикордонного шлюзу є останнім маршрутизатором, що контролюється безпосередньо перед виходом в Інтернет і часто функціонує в ролі першої й останньої лінії захисту мережі, забезпечуючи фільтрацію вхідного і вихідного трафіка.

Брандмауер (*firewall*, чи міжмережний екран) являє собою пристрій, який аналізує трафік з використанням набору правил, що дозволяють визначити, чи можна передавати цей трафік по мережі, чи не можна. Область дії брандмауера починається там, де закінчується область дії прикордонного маршрутизатора, і він виконує більш ретельну перевірку пакетів при фільтрації трафіка. Існує кілька різних типів брандмауерів, до яких відносяться статичні пакетні фільтри (для блокування доступу до підмережі можна використовувати, наприклад, вбудований статичний пакетний фільтр маршрутизатора *Nortel Accellar*), брандмауери експертного рівня (для контролю за дозволеними сервісами, наприклад *Cisco PIX*), а також проксі-брандмауери (для контролю за вмістом, наприклад *Secure Computing's Sidewinder*). Незважаючи на те, що брандмауери не є досконалими модулями, вони зможуть заблокувати або дозволити усе, що їм указати.

IDS (*Intrusion Detection System* – система виявлення вторгнень) — це охоронна сигналізація мережі, яка використовується для виявлення і повідомлення про всі вторгнення і потенційно небезпечні події. Система може містити безліч детекторів різного типу, розміщених у стратегічних точках мережі, які шукають заздалегідь задані сигнатури небажаних подій і можуть виконувати статистичний аналіз і аналіз аномальних подій. У випадку виявлення

небажаних подій детектори IDS оповіщають адміністратора різними способами: використовуючи електронну пошту, пейджинговий зв'язок чи розміщуючи запис у *log*-файлі.

VPN (*Virtual Private Network* – віртуальна приватна мережа) являє собою захищений сеанс, для організації якого використовуються незахищені канали, наприклад, Інтернет. Дуже часто під *VPN* мають на увазі апаратний компонент периметра, що підтримує шифрування сеансів. Доступ до корпоративної мережі через VPN можуть використовувати ділові партнери компанії, співробітники, які знаходяться у відрядженні або працюють вдома. При безпосередньому підключенні до внутрішньої мережі компанії *VPN* дозволяє вилученим користувачам працювати в ній так, ніби вони знаходяться в офісі.

DMZ (*DeMilitarized Zone* – демілітаризована зона) являє собою незахищену область між захищеними ділянками. *DMZ* розміщена перед брандмауером, у той час як екранована підмережа розміщується за брандмауером.

Екранована підмережа являє собою ізольовану мережу, з'єднану з визначеним інтерфейсом брандмауера чи іншого фільтруючого трафік пристрою. Екранована підмережа часто використовується для ізоляції серверів, до яких необхідно забезпечити доступ з Інтернету, що використовуються тільки внутрішніми користувачами даної організації. Екранована підмережа звичайно містить сервіси "загального використання", включаючи *DNS*, пошту і web.

Брандмауер являє собою бар'єр, що захищає від спроб зловмисників вторгнутися в мережу, для того щоб скопіювати, змінити чи стерти інформацію, або щоб скористатися смугою пропущення, пам'яттю чи обчислювальною потужністю працюючих у цій мережі комп'ютерів. Брандмауер установлюється на границі двох мереж - мережі Інтернет і ЛОМ, тому його ще називають і міжмережним екраном. Він фільтрує всі вхідні і вихідні дані, пропускаючи тільки авторизовані пакети. Скоріше, брандмауер - це підхід до безпеки; він

допомагає реалізувати політику безпеки, яка визначає дозволені служби і типи доступу до них. Він реалізує політику мережного доступу, змушуючи проходити всі з'єднання з мережею через брандмауер, де вони можуть бути проаналізовані, дозволені або відкинуті.

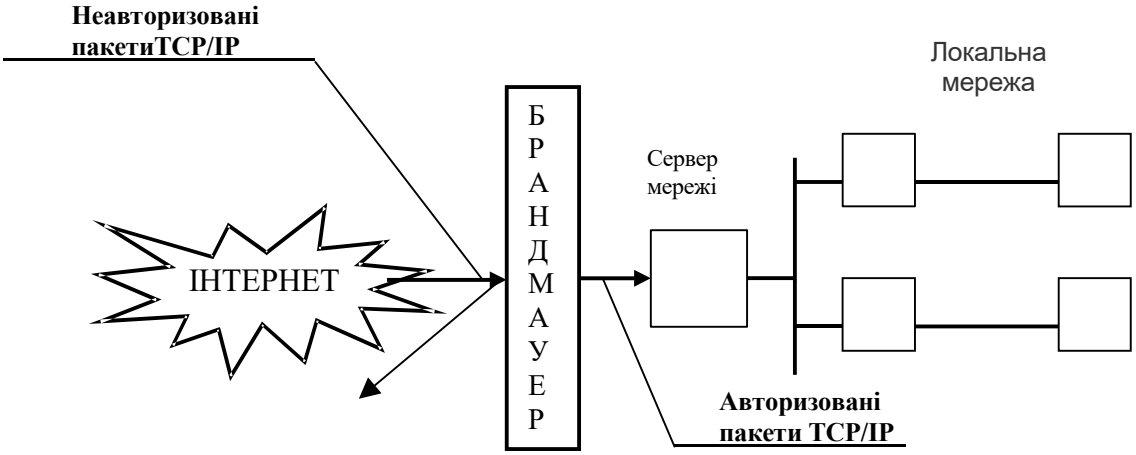

Рис. 2.2. Умовна схема розміщення та функціонування брандмауера

Функції брандмауера можуть виконувати маршрутизатор, спеціалізований комп'ютер, хост чи група хостів, створена спеціально для захисту мережі чи підмережі від неавторизованого використання протоколів і служб хостами, що знаходяться за межами цієї підмережі. Звичайно система брандмауера створюється на основі маршрутизаторів верхнього рівня, зазвичай на тих, які з'єднують мережу з Інтернетом, хоча може бути створена і на інших маршрутизаторах, для захисту тільки частини хостів чи підмереж.

Існуючі брандмауери сильно відрізняються один від одного як за рівнем захисту, так і за використовуваними у них способах захисту. Однак більшість брандмауерів, що поставляються як комерційні продукти, можна (утім, досить умовно) віднести до однієї з трьох категорій:

- Брандмауери з фільтрацією пакетів;
- Брандмауери експертного рівня;
- Проксі - брандмауери.

Брандмауер з фільтрацією пакетів являє собою маршрутизатор чи працюючу на сервері програму, сконфігуровані таким чином, щоб фільтрувати вхідні і вихідні пакети. Брандмауер пропускає чи відкидає пакети відповідно до інформації, що міститься в IP-заголовках пакетів: адреси відправника, адреси одержувача, інформації про додаток чи протокол, номера порту джерела, номера порту одержувача.

Пакетна фільтрація – одне із самих старих і найбільш розповсюджених засобів керування доступом до мережі. Ідея пакетної фільтрації – установити, чи дозволено даному пакету входити в мережу чи виходити з неї. Однак вона не вміє відрізняти один від одного різні типи трафіка. Оскільки пакетні фільтри не аналізують потоки трафіка так глибоко, як це роблять інші технології брандмауерів, вони працюють помітно швидше.

Брандмауер з фільтрацією пакетів перед відправленням пакета одержувачу порівнює його повну асоціацію з таблицею правил, у відповідності, з якою він повинний пропустити чи відкинути даний пакет. Брандмауер продовжує перевірку доти, поки не знайде правила, з яким погодиться повна асоціація пакета. Якщо брандмауер одержав пакет, який не відповідає жодному з табличних правил, він застосовує правило, задане за замовчуванням, яке також повинне бути чітко визначене в таблиці брандмауера. З розумінь безпеки це правило звичайно вказує на необхідність відкидання всіх пакетів, що не задовольняють жодному з інших правил.

Фільтрація, заснована на адресі джерела: стандартний список керування доступом

Одна з причин, по якій технологія фільтрації пакетів продовжує застосовуватися – блокування чи дозвіл трафіка на підставі *IP*- адреси системи джерела. Цей список не може здійснювати фільтрацію на підставі пункту призначення чи номеру порту. Тому стандартний список доступу працює

швидко, і йому варто віддавати перевагу, коли критерієм для фільтрації служить тільки адреса джерела.

Синтаксис для стандартного списку доступу наступний:

access-list <list number 1-99> <permit/deny> <source address> <mask> <log>

Номер списку не повинний виходити за межі діапазону 1-99. Опція *mask* є необхідною маскою групового символу, що говорить маршрутизатору про те, що це один хост, який необхідно відфільтрувати, чи цілий діапазон. Опція *log* може бути додана для того, щоб маршрутизатор спеціально реєстрував будь-які відповідності цьому фільтру.

Популярним використанням стандартного списку доступу є організація «чорного списку» у відношенні конкретних мереж хостів. Тобто можна заблокувати доступ до своєї мережі одному конкретному хосту чи цілій мережі. Теоретично можна використовувати стандартний список доступу також для дозволу трафіка з даної IP- адреси, але цього робити не варто, тому що це зробить мережу вразливою перед атаками і скануваннями, що використовують неправдиві адреси. Стандартні списки доступу використовуються також для дозволу вихідного трафіка: з мережі будуть випущені тільки ті пакети, у яких у полі адреси джерела зазначена адреса своєї мережі.

Фільтрація за адресою призначення і портам: розширений список керування доступом

Технологія пакетної фільтрації також добре себе зарекомендувала і при фільтрації на основі інформації заголовка пакета і номерів портів. Ці приклади можна застосовувати в ролі специфічних «каналів», що дозволяють одній системі мати доступ до іншої (екстрамережі), або дозволяючих доступ до визначеної системи відкритого доступу (web чи сервер *DNS*), або дозволяючих введення визначеного типу трафіка у свою мережу (занадто великий пакет *ICMP*).

Синтаксис для розширеного списку доступу наступний:

access-list <list number 100-199> <permit/deny> <protocol> <source> <source-mask> <source-port> <destination> <destination-mask> <destination-port> <log/log-input> <options>

Ключове слово *protocol* визначає протокол, який цікавить при фільтрації. Компоненти *source-port* чи *destination-port* визначають тип трафіка, який необхідно дозволити чи заборонити. Наприкінці списку доступу можна додати безліч опцій, наприклад *log* (як вказувалося в стандартному списку доступу чи *log-input*, що також показує вхідний інтерфейс і *MAC*- адреси джерела), чи ключове слово *established*, що виконує перевірку прапорів, установлених у вхідних пакетах.

Корисною функцією розширеного списку доступу є фільтрація деяких типів трафіка. Додатковим рівнем захисту може стати заборона трафіка у відповідності зі списком портів, використовуваних популярними троянськими програмами чи програмами, що конфліктують з політикою користування Інтернетом чи політикою безпеки. Цей тип фільтрації може також використовуватися і для дозволу чи заборони деяких інформаційних *ICMP*-повідомлень, що входять у мережу. Найкращим способом блокування *ICMP* є дозвіл тільки того типу трафіка, що необхідний, а на всі інші типи накладення заборони.

Проблеми, пов'язані з використанням пакетних фільтрів

Використання пакетних фільтрів, поряд з перевагами, пов'язані також і з рядом проблем. Зокрема, якщо захист не реалізований належним чином, спуфінговий і фрагментований трафік можуть обійти пакетний фільтр. Крім того, у зв'язку з тим, що «дозволяючий» статичний пакетний фільтр постійно відкритий, існує загроза виникнення «дір». І, нарешті, дозвіл зворотного трафіка може бути ускладний при використанні технології, нездатної відслідковувати поточний стан потоку трафіка.

Динамічна пакетна фільтрація і рефлексивний список доступу

Багато проблем, з якими зіштовхується статична пакетна фільтрація, можуть бути частково вирішені за допомогою технології динамічної пакетної фільтрації. Ідея цієї технології полягає в тім, що фільтри проектуються «на льоту» по мірі необхідності, і припиняють роботу після розриву з'єднань. Рефлексивні списки доступу є прикладами технології динамічної пакетної фільтрації. В зовнішньому інтерфейсі встановлюється критерій, на підставі якого проходить відстеження визначених типів з'єднань. У випадку повернення трафіка він порівнюється зі списком доступу, який був динамічно створений відразу після того, як трафік вийшов з мережі.

Рефлексивні списки контролю доступу підвищують функціональність розширених іменованих списків контролю доступу за рахунок включення двох додаткових ключових слів: *reflect* і *evaluate*. Слово *reflect* вживається для відновлення динамічного *ACL* за допомогою дзеркального образу пакета, що відповідає конкретному запису в ACL. Зворотний трафік згодом порівнюється з цим динамічним ACL за допомогою ключового слова *evaluate*.

На жаль, рефлексивні списки доступу не є досконалими, але пройти їх набагато складніше, ніж інші пакетні фільтри. Одного пакета "*reset*" досить, щоб цілком видалити рефлексивно створений список керування доступом. Інша проблема полягає в тім, що ці списки не зберігають ніяких записів про прапори TCP, тому початковий трафік може просочитися без сигналу тривоги.

Брандмауери експертного рівня

Найбільш розповсюдженим типом брандмауерів є брандмауери експертного рівня [9]. Крім статичної фільтрації пакетів, вони спостерігають за з'єднаннями в таблиці станів. Стан характеризує поточний статус даного сеансу з'єднання. Пристрої, що здійснюють відстеження стану, представляють дані у виді таблиці. Кожен запис містить довгий список інформації про *IP*-адресу джерела і призначення, прапори, порядковий номер і номер підтвердження і т.д. Кожен елемент у таблиці станів створюється з початком з'єднання, що проходить через

пристрій експертного контролю, який під час повернення трафіка порівнює інформацію пакета з інформацією в таблиці станів. Якщо пакет пов'язаний з поточним записом у таблиці, проходження пакета дозволяється.

Витяг з таблиці станів маршрутизатора *Cisco*, що використовує рефлексивні списки доступу:

Reflexive IP access list packets

Permit tcp host xx. yy. zz . 45 eq 36204 host 192. 168.1.1 eq smtp

(10 matches) (time left 295)

Permit tcp host xx. yy. zz . 99 eq www host 192. 168.1.1 eq 2151

(8 matches) (time left 294)

Permit tcp host xx. yy. zz . 247 eq www host 192. 168.1.1 eq 2149

(10 matches) (time left 294)

Permit udp host xx. yy. zz . 34 eq domain host 192. 168.1.1 eq 2150 log

(3matches) (time left 293)

Permit tcp host xx. yy. zz . 247 eq www host 192. 168.1.1 eq 2148

(16 matches) (time left 296)

Permit udp host xx. yy. zz . 34 eq domain host 192. 168.1.1 eq 2146 log

(3matches) (time left 292)

Можна побачити всі динамічно створені списки доступу, які формуються вихідними з'єднаннями, що передбачають таку ж функціональність, як і таблиця стану, в тім сенсі, що вони відслідковують інформацію про поточні сеанси зв'язку, щоб дозволити успішне проходження зворотного трафіка через маршрутизатор. Кожен запис починається з ключового слова *Permit*. За ним іде інформація про стан сеансу. Підтримується як *TCP*, так і *UDP*. За протоколом іде адреса і порт призначення. І нарешті, виводиться число відповідностей визначеному правилу, а далі – час, після закінчення якого відбувається автоматичне видалення динамічно розміщеного списку.

Подібне спостереження за з'єднаннями корисно при багаторівневому захисті, оскільки брандмауер експертного рівня блокує трафік, що не визначений у його таблиці встановлених з'єднань. База правил брандмауера визначає IP- адреси відправника й одержувача, а також номера портів, що дозволені для встановлення з'єднання. Аналізується будь-яке виявлене зондування, що служить чітким індикатором атаки, що насувається.

Брандмауери експертного рівня забезпечують один з найвищих на сьогоднішній день рівнів захисту корпоративних мереж, проте навіть ці надійні брандмауери не забезпечують 100%-ної безпеки.

Брандмауер експертного рівня можна класифікувати двома способами: експертна фільтрація та експертний контроль. Експертна фільтрація широко використовується для визначення фільтрації стану пакетних потоків на основі інформації IP-адреси джерела та призначення, номера порту, порядкового номеру та номеру підтверджень, флагів та іншої інформації транспортного рівня. Експертний контроль також спостерігає за інформацією четвертого рівня а також пропонує засоби захисту для обробки потоку нестандартного трафіку TCP/IP. Експертна перевірка пропонує більш захищену середу ніж пакетний фільтр. В порівнянні з проксі-брандмауером у брандмауера експертного рівня більш висока продуктивність. Проте ті ж самі особливості, які дають експертній перевірці перевагу в продуктивності в порівнянні з проксі-брандмауером, роблять її менш захищеною там, де необхідно аналізувати всі аспекти зв’язку на прикладному рівні.

Проксі – брандмауери

Альтернативою, а іноді комбінацією з брандмауером експертного рівня, є проксі-брандмауери, що являють собою більш довершений і менш розповсюджений тип брандмауерів. Проксі-брандмауери також виконують функції брандмауера експертного рівня; це виявляється в тім, що вони блокують невстановлені і недозволені з'єднання. База правил проксі-брандмауера порівнює

IP джерела й адресата, а також номера портів, дозволених для встановлення з'єднання. Проксі-брандмауери забезпечують високий рівень безпеки, оскільки внутрішні і зовнішні хости ніколи не з'єднуються безпосередньо. У такій ситуації брандмауер діє як посередник між хостами. Проксі-брандмауери виконують перевірку всього пакета, щоб переконатися у відповідності його протоколу, що зазначений у номері порту адресата. Гарантуючи, що буде пропущений тільки той трафік, який відповідає заявленому протоколу, брандмауер допомагає будувати багаторівневий захист, зменшуючи імовірність проходження злочинного вхідного чи вихідного трафіка.

Переваги проксі-брандмауерів

У порівнянні з іншими типами брандмауерів, проксі-брандмауери володіють рядом переваг:

Внутрішні *IP*-адреси захищені від зовнішнього світу завдяки тому, що проксі-служби не допускають прямих з'єднань між зовнішніми серверами і внутрішніми комп'ютерами.

Адміністратори мають можливість проводити моніторинг порушень політики безпеки брандмауера, використовуючи для цього записи аудита, що генеруються службами проксі.

Використання проксі-брандмауерів дозволяє організувати захист, заснований на користувачах. Служби проксі ефективні при захисті від неавторизованого використання на однокористувальницькій основі і здатні підтримувати строгу аутентифікацію.

Внаслідок того, що можливість організації з'єднань заснована на службах, а не на фізичних з'єднаннях, проксі-брандмауери виявляються невразливими перед *IP*-спуфиінгом (підміна *IP*-адреси).

IP-адреси хостів у межах внутрішньої захищеної мережі не вимагають з'єднання за допомогою проксі-брандмауера .

Проксі-брандмауери мають кращі можливості реєстрації, чим

брандмауери фільтрації і маршрутизації, і пропонують єдину точку для аудита і керування.

- Користувачі не можуть ввійти в проксі-сервери.

У бастіонних хостах не вимагаються ніякі облікові записи. Проксі-служби працюють по команді користувачів.

Проксі-сервер забезпечує централізовану точку для мережі, і спостереження за трафіком може виконуватися дуже ретельно. Але це може створити вузькі місця мережного трафіка.

Топологія внутрішньої захищеної мережі в проксі-брандмауерах є прихованою.

Деякі проксі пропонують поліпшені засоби виконання аудита, маючи інструменти для моніторингу трафіка.

Проксі-брандмауери пропонують строгу аутентифікацію і реєстрацію. Можливе виконання попередньої аутентифікації прикладного трафіка, перш ніж він досягне внутрішніх хостів, а також більш ефективна реєстрація в порівнянні зі стандартною реєстрацією хоста.

Проксі-брандмауери мають менш складні правила фільтрації, ніж брандмауери пакетних фільтрів.

Недоліки проксі-брандмауерів

Незважаючи на те, що проксі-брандмауери пропонують більш високий рівень безпеки в порівнянні з брандмауерами пакетної фільтрації, вони, проте, мають деякі недоліки:

Зниження продуктивності внаслідок додаткових запитів на обробку, необхідних для прикладних служб. Прикладні проксі працюють повільніше в порівнянні з пакетними фільтрами.

Для кожного нового додатка чи протоколу, які необхідно пропустити через брандмауер, необхідно розробляти новий проксі.

Доступним є лише обмежена кількість служб.

Невід'ємні проблеми в операційних системах і їхніх компонентах

можуть негативно вплинути на безпеку сервера брандмауера. Проксі-служби уразливі перед помилками в операційних системах і помилками на прикладному рівні.

Операційна система хоста, що містить проксі, залишається незахищеною перед зовнішніми погрозами і може бути піддана атакам.

Процес установки проксі-служби може виявитися досить складним для кожного додатка, що використовує шлюз.

Оскільки проксі-сервер може виявитися вузьким місцем у мережі, він може стати також і єдиною точкою збою.

Маршрутизатор також відіграє важливу роль в безпеці мережі. Він захищає проти атак, основаних на відмові в обслуговуванні, виконує фільтрацію вхідного та вихідного трафіка, може бути задіян в якості пограничного брандмауера, використовуючи такі технології як керування доступом на основі контексту, трансляція мережних адрес і списки контролю доступу.

В цьому розділі були розглянуті принципи роботи віртуальної приватної мережі і процесу тунелювання, а також основи систем виявлення вторгнень.

Отже, проаналізувавши основні компоненти захисту мережного периметру, можна зробити висновок, що не існує ніяких універсальних засобів, жоден окремий компонент не може в достатній мірі захистити мережу. Для збільшення захищенності потрібен багаторівневий захист. Необхідно організувати компоненти захисту в рівні, щоб максимально використати їх можливості.

2.2. Розподілені системи виявлення вторгнень

Система виявлення вторгнень (*intrusion detection system – IDS*) виконує моніторинг мережного трафіка чи маніпуляцій з файлами хоста для того, щоб установити факти нетипового поводження чи некоректного використання. *IDS*

веде журнал вторгнень, розсилає попередження в режимі реального часу і, у деяких випадках, може зупинити атаку.

Основними компонентами IDS є мережні сенсори [3]. Сенсори виконують роль головної сполучної ланки IDS з обчислювальним середовищем. Вони збирають необхідну для виявлення вторгнення інформацію, фільтрують її і відсилають детекторам. На наступному етапі проводиться аналіз зібраних подій безпеки, виявлення в них вторгнень і вироблення повідомлень про підозрілу активність. Існує два типи сенсорів - мережні і хостові. Мережні сенсори здійснюють збір подій безпеки з мережного трафіка і забезпечують ними підсистему виявлення. Хостові сенсори роблять попередню фільтрацію потоку подій у системі. При цьому використовується моніторинг функціонування системи (використання ресурсів, виконання, входів у систему і т.д.), аналіз протоколів і системних/службових файлів і структур.

У зв'язку з безпосереднім контактом із системою, що захищається, на сенсори найчастіше покладається реалізація контрзаходів (закриття з'єднань, завершення процесів, реконфігурування мережних пристроїв і т.д.). Виявлення атак проводиться детектором за заданими критеріями виявлення (сигнатурам, шаблонам, правилам).

Атаки розрізняються складністю розпізнавання: деякі можуть бути легко виявлені по сигнатурі, інші ж вимагають статистичних методів виявлення [4].

У зв'язку з цим, сучасна IDS має кілька механізмів виявлення: сигнатурний пошук, пошук регулярних виразів і статистичний механізм розпізнавання вторгнень.

Однак, на жаль, системи виявлення вторгнень, покликані ідентифікувати і відбивати напади хакерів, самі можуть бути піддані несанкціонованим впливам, які можуть порушити працездатність цієї системи, що не дозволить їй виконувати поставлені перед нею задачі.

У загальному випадку сенсор системи виявлення атак являє собою підсистему, що одержує доступ до деякого джерела інформації, у якості якого може виступати мережний трафік, журнал реєстрації чи системні виклики. Потім дані попадають на механізм попередньої фільтрації, що відсіває те, що сенсор не може аналізувати.

Розглянемо можливі атаки на сенсор, починаючи із нихнього рівня ієрархії (рис. 2.3)

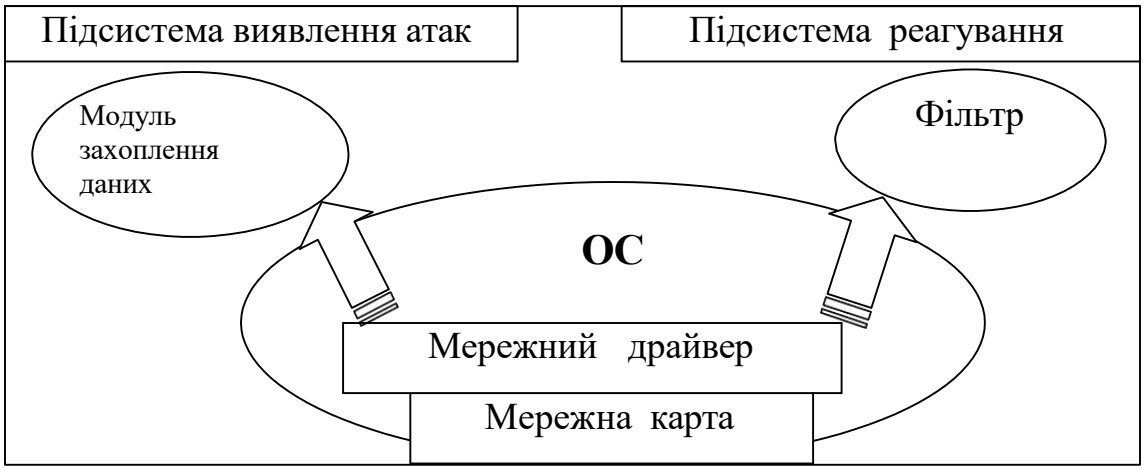

Рис 2.3. Схема проходження атаки на сенсор

1. Мережева карта. Цей компонент задіється для двох цілей – одержання доступу до мережного трафіку, у якому шукаються сліди атак (якщо мова не йде про спеціальні плати виявлення атак, що вставляються в шасі комутатора чи маршрутизатора, чи спеціальне програмне забезпечення виявлення атак для маршрутизатора), а також для передачі на консоль керування сигналів тривоги. З огляду на різні можливості по вилученому керуванню мережними картами (*RMON, DMI, ACPI, Wf* і т.д.) можна припустити, що атаки на мережну карту дуже навіть можливі.

2. Мережний драйвер. На даному рівні наприклад неправильна реалізація мережного стека, дозволяє посилати на сенсор певним чином сформовані пакети,

що приводить до падіння «у синій екран».

3. ОС. Наявність вразливостей у сучасних ОС, приводить до того що через цей компонент атаки на IDS більш ніж реальні.

4. Модуль захоплення даних. Якщо він оперує мережними пакетами, то досить послати на нього або нестандартні (тобто невідповідні RFC) пакети, або організувати лавину трафіка, яку нездатний обробити сенсор. Якщо він оперує журналом реєстрації, то можна переповнити цей журнал і старі події будуть перезаписані новими.

5. Фільтр. Досить увімкнути фільтрацію тих атак, що реалізує зловмисник, і вони не будуть виявлені.

6. Підсистема виявлення атак. У «сигнатурних» IDS є одне серйозне обмеження – варто змінити один байт у коді атаки і вона вже не буде виявлена.

7. Підсистема реагування. Навіть якщо IDS знайшла атаку, то досить не дати їй відреагувати на напад і ефективність системи виявлення вторгнень буде зведена до нуля. Основними варіантами реагування є: повідомлення на консоль, генерація *SNMP* чи e-mail, розірвання з'єднання.

Засоби захисту, покликані забезпечувати безпеку мережі, можуть служити й інструментом у руках кваліфікованого зловмисника. Наприклад, знаючи, що сенсор розриває з'єднання з вузлом, що атакує, можна реалізувати атаку, в адресі відправника якої вказати адресу якого-небудь з компонентів *IDS*. Тим самим *IDS* сама виступить як засіб для реалізації *DoS*-атаки. Ще один момент, якому можна використовувати для атак на систему виявлення вторгнень – механізм аутентифікації. Досить видалити ключ аутентифікації одного з компонентів *IDS* і процес аутентифікації вже не пройде. А, отже, компоненти не зможуть обмінюватися між собою інформацією. А якщо раптом так вийшло, що аутентифікація між компонентами взагалі не використовується, то зловмисник може створити помилковий сенсор, що вводить в оману консоль, чи помилкову консоль, що дає «потрібні» команди існуючим сенсорам.

Щоб поліпшити захист сенсорів системи виявлення мережного вторгнення, пропонується створити окрему мережу керування, використовувану винятково для зв'язку між сенсорами системи виявлення вторгнення, централізованим блоком збору даних системи виявлення вторгнення і пультами аналітиків (рис. 2.4).

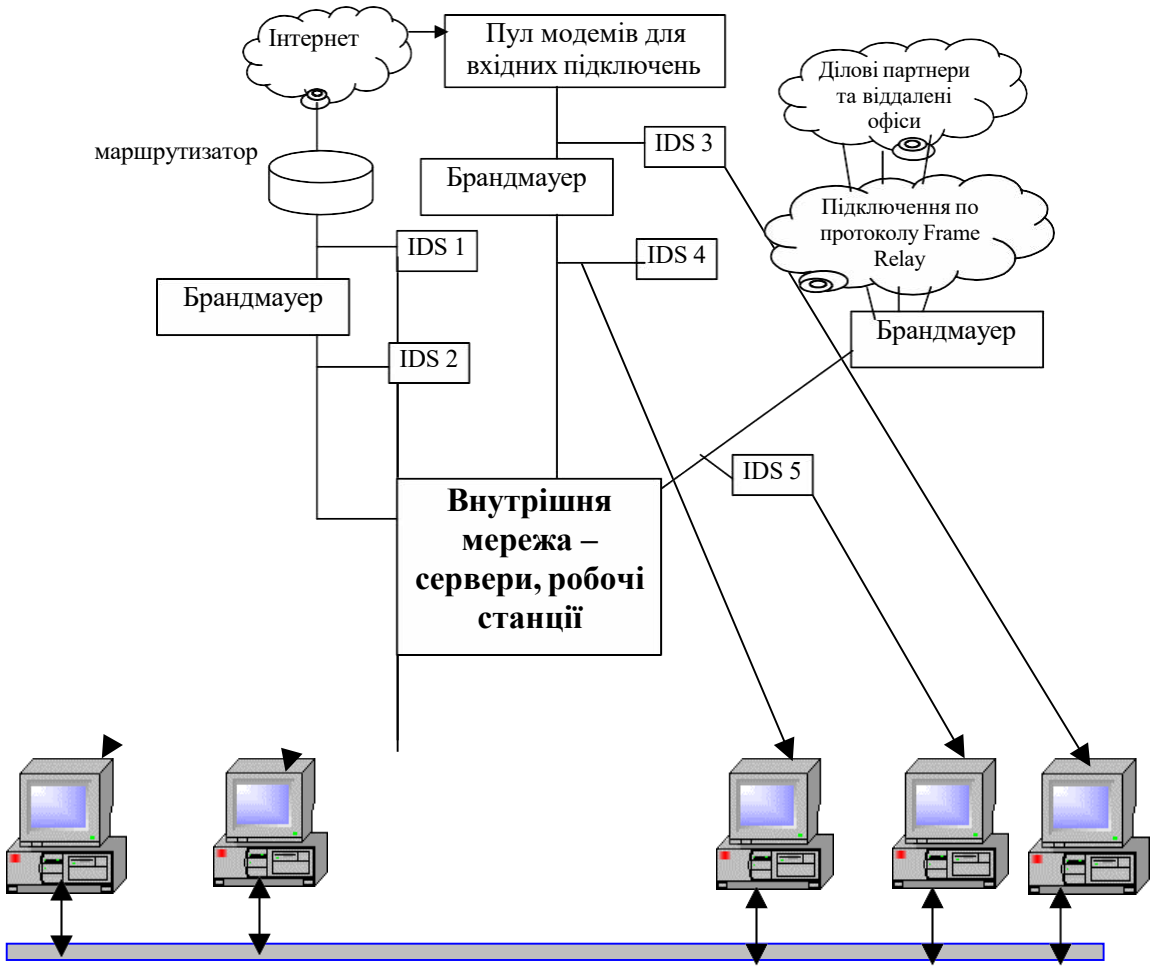

Рис. 2.4. Мережа керування системою виявлення вторгнень

У цій моделі кожен мережний сенсор системи виявлення вторгнення має не менш двох мережних інформаційних карт *(NIC).* Єдиною функцією однієї чи декількох мережних інформаційних карт є перегляд трафіка мереж, що перевіряються. Ці мережні інформаційні карти не передають трафік. Замість цього, остання мережна інформаційна карта підключається до окремої мережі

керування, що використовується тільки для передачі даних системі виявлення вторгнення і модифікації конфігурації.

Така архітектура ускладнює зловмисникам задачу знаходження й ідентифікації сенсора системи виявлення вторгнення, оскільки він не буде відповідати на запити, які спрямовані до контролюючої його мережної інформаційної карти. А тому що мережна інформаційна карта знаходиться в ізольованій мережі, зловмисники не зможуть досягти її. Крім того, деякі контролюючі мережні інформаційні карти є чистими мережними аналізаторами пакетів і не використовують IP-адресу. Якщо сенсор системи виявлення вторгнення використовує IP-адресу, і зловмисник знає її, то він може попередньо запустити проти нього атаку, щоб викликати стан відмовлення в обслуговуванні (*Denial of Service - DoS*), коли сенсор не може побачити його напад. Також зловмисник може спробувати іншим методом сховати чи заплутати трафік від сенсора.

Побудова окремої мережі керування має й інші переваги. Вона ізолює трафік керування так, щоб ніхто, хто ще контролює цю же саму мережу, не бачив зв'язку сенсорів. Це також не дозволяє сенсорам контролювати їхній власний трафік. Окрема мережа є гарним способом уникнути потенційних проблем, пов'язаних із проходженням даних сенсорів через брандмауери і незашифровані суспільні мережі.

Критично важливим є зміцнення безпеки сенсорів системи виявлення вторгнення, щоб звести ризик їхньої компрометації до мінімально можливого рівня. Якщо зловмисники одержать доступ до керування системою виявлення вторгнення, то вони зможуть відключити її чи реконфігурувати таким чином, що вона не буде реєструвати їхньої дії чи попереджати про них. Зловмисники також зможуть використовувати систему виявлення вторгнення для атак проти інших вузлів мережі. Підтримка високого рівня безпеки сенсорів є ключовим для створення стійкого і корисного рішення системи виявлення вторгнення.

2.3 Проактивна система захисту інформації в комп'ютерній мережі

Архітектура розподіленої проактивної системи

Проактивний сервіс в основному орієнтований не на усунення, а на попередження несправностей і являє собою сукупність стратегічних заходів, що повинні забезпечити оптимальну і безперебійну роботу мережі з урахуванням політики безпеки.

Проактивні системи спираються на сім базових принципів [21]:

Зв'язок з фізичним світом;

«Глибокі» мережні взаємодії;

Макрообробка;

Функціонування в умовах невизначеності;

Передбачення;

Замкнутий цикл керування;

Персоніфікація.

Орієнтація на системи, у яких людина не виконує керуючу функцію, чи на цілком автоматичні системи — загальна мета проактивних комп'ютерних систем організації безпеки корпоративних інформаційних ресурсів.

Отже, погрози конфіденційності, цілісності і приступності інтерфейсів, протоколів і послуг є найбільш узагальненим видом погроз, і універсальність проектованих систем захисту може бути заснована саме на цій не конкретній, а узагальненій погрозі. Для подібної системи не буде мати значення, які конкретно атаки організуються на телекомунікаційну систему – вони заздалегідь будуть неефективні.

Розглянемо, що означають конфіденційність, цілісність і приступність для інтерфейсів, протоколів і послуг. Кожен протокол має свої особливості, але в будь-якому випадку повинний забезпечувати взаємодію як мінімум двох об'єктів

(у цьому його концептуальна відмінність від алгоритму – чіткої послідовності операцій, що приводить до виконання поставленої задачі з досить великого класу однотипних задач, але без взаємодії). Отже, для всіх протоколів узагальнюючим є їхнє призначення – забезпечення взаємодії, і агент безпеки в даному випадку відповідальний за конфіденційність, цілісність і приступність цієї взаємодії. Інтерфейсів також існує багато, вони являють собою правила доступу до послуг. Отже, загальним для них буде забезпечення конфіденційності, цілісності і приступності правил доступу до послуг. Основною функцією всіх послуг є надання кому-небудь яких-небудь ресурсів (у тому числі і можливостей). Забезпечення безпеки – це захист ресурсу від неправомірного доступу і/чи використання, від підміни або ушкодження/знищення.

За основу підсистеми безпеки доцільно вибрати агентну технологію. Кожен агент буде діяти з урахуванням реальної ситуації на підзвітній йому ділянці (моніторинг у фоновому режимі). При цьому він є інтелектуальним, здатним діяти незалежно від інших агентів, хоча і пов'язаним з ними – якщо виникло порушення безпеки, яке можна дозволити на місці, то воно буде негайно виправлено агентом безпеки, без його зв'язку з іншими агентами або з контролюючим центром (повне розгалуження служб безпеки). Під агентом тут мається на увазі сутність, що володіє здатністю до формулювання цілей, навчанню, плануванню і прийняттю рішень в оточенні, що динамічно змінюється. Призначення агентів – спростити і поліпшити взаємодію користувачів зі складними програмними системами в слабоструктурованому динамічно змінюючомуся розподіленому середовищі шляхом адаптації до особливостей конкретного користувача. Агент, на відміну від традиційних програм, здатний не тільки взаємодіяти з цим середовищем, одержуючи від нього інформацію через свої сенсори, впливаючи на середовище за допомогою своїх эффекторів, але і змінювати своє поводження, навчаючись на власному досвіді.

Розглянемо особливості побудови пропонованої системи безпеки.

1. Окремі елементи даної системи вже існують. Це доводять приклади систем безпеки, наведені в першій частині розділу. Крім того, проактивно захищені системи використовуються, наприклад, у банківській справі – при банківських переведеннях через телекомунікаційні мережі загального призначення (Internet).

2. Система повинна бути розподіленою, тобто реалізуючою інформаційну технологію на підставі розподілу інформаційних ресурсів. розподіленої обчислювальної системи включає дані, засоби для їхньої обробки, активні компоненти. Інформаційними ресурсами розподіленої обчислювальної системи є оброблювані дані, програмне забезпечення, інформаційні складові апаратного забезпечення і інформацію про користувачів, сюди ж варто включати різні агенти, у тому числі агенти безпеки. Політика безпеки – безліч правил, що контролюють порядок обробки інформації, взаємодії підсистем і забезпечення захисту, – визначає безпеку розподіленої обчислювальної системи і архітектуру системи захисту. При цьому розподіленість обчислювальної системи веде до росту уразливості її інформаційних ресурсів і розширенню безлічі погроз безпеки. З погляду агентного підходу погрози безпеки також варто вважати агентами або мультиагентними системами (при розподіленій погрозі), абстрагуючи від дестабілізуючих факторів різної природи (апаратних, програмних, користувальницьких і ін.).

3. Безпека розподіленої обчислювальної системи – такий стан інформаційного мультиагентного середовища, при якому в умовах впливу дестабілізуючих факторів (погроз безпеки) забезпечується виконання функцій обробки даних, міжагентної взаємодії і захисту (самозахисту). Захист – невід'ємна, внутрішня властивість РОС.

Система складається з компонентів (інтелектуальних підсистем), що реалізують загальну політику безпеки (рис.2.5).

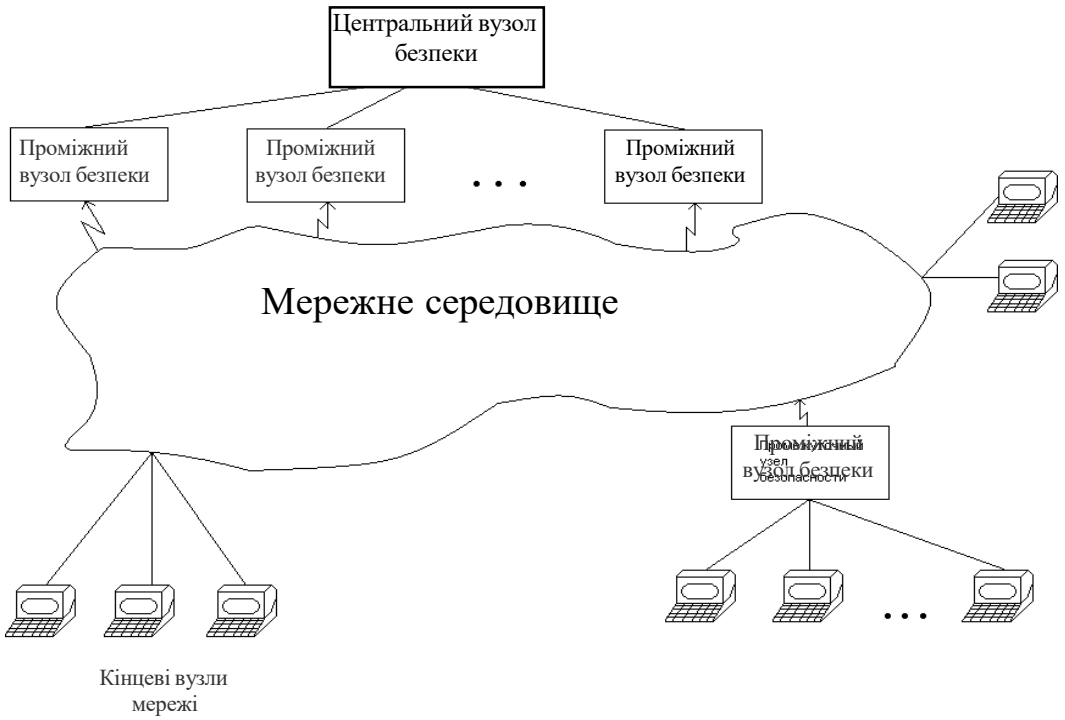

Рис. 2.5. Структура підсистеми захисту розподіленої обчислювальної системи

Розглянута архітектура самоподібних систем є новим рішенням в області інформаційних технологій і здатна вирішити проблеми ресурсного балансу між функціональними системними задачами, і задачами, що забезпечують їхнє безпечне виконання. При цьому властивість самоподібності дозволить значно спростити і поліпшити адміністрування навіть складних слабоструктурованих систем, у той же час мінімізуючи необхідний для забезпечення безпеки трафік. [1-44]

2.3. Висновок до розділу

Розглянуто та проаналізовано основні принципи захисту мережевого периметра комп'ютерної мережі ДІКС, основи побудови системи захисту мережного периметру.

Проаналізована динамічна пакетна фільтрація і рефлексивний список доступу. Багато проблем, з якими зіштовхується статична пакетна фільтрація, можуть бути частково вирішені за допомогою технології динамічної пакетної фільтрації. Ідея цієї технології полягає в тім, що фільтри проектуються «на льоту» по мірі необхідності, і припиняють роботу після розриву з'єднань. Рефлексивні списки доступу є прикладами технології динамічної пакетної фільтрації. В зовнішньому інтерфейсі встановлюється критерій, на підставі якого проходить відстеження визначених типів з'єднань. У випадку повернення трафіка він порівнюється зі списком доступу, який був динамічно створений відразу після того, як трафік вийшов з мережі.

Розподілені системи виявлення вторгнень. Система виявлення вторгнень (*intrusion detection system – IDS*) виконує моніторинг мережного трафіка чи маніпуляцій з файлами хоста для того, щоб установити факти нетипового поводження чи некоректного використання. *IDS* веде журнал вторгнень, розсилає попередження в режимі реального часу і, у деяких випадках, може зупинити атаку.

Проактивна система захисту інформації в комп'ютерній мережі. Архітектура розподіленої проактивної системи. Проактивний сервіс в основному орієнтований не на усунення, а на попередження несправностей і являє собою сукупність стратегічних заходів, що повинні забезпечити оптимальну і безперебійну роботу мережі з урахуванням політики безпеки.

РОЗДІЛ 3
ЗАХИСТ КОМП'ЮТЕРНОЇ МЕРЕЖІ ВІД РОЗПОДІЛЕНИХ АТАК

Метод, який часто використовується шкідливим програмним забезпеченням для приховування цільової системи, - атака на введення коду на основі хоста. Він дозволяє шкідливому програмному продукту виконувати свій код у зовнішньому процесовому просторі, що дозволяє йому працювати таємно та отримувати доступ до критичної інформації інших процесів. Оскільки існує безліч різних способів введення та виконання коду в зовнішньому процесовому просторі, необхідний загальний підхід, що охоплює всі ці можливості. Підходи, що фокусуються лише на деталях операційної системи низького рівня (наприклад, підключення *API*) недостатньо, оскільки підозрілий набір *API* постійно розширюється. Таким чином, підходи, орієнтовані на деталі операційної системи низького рівня, схильні до втрати нових атак. Крім того, такі підходи обмежуються інтимним знанням лише однієї операційної системи.

Судячи з результатів аналізу численних статей, монографій, матеріалів наукових і практичних конференцій, завдання захисту інформаційних ресурсів комп'ютерних мереж від атак з боку зовнішніх і внутрішніх порушників ніколи не втратить свою актуальність. У цей час опубліковані переліки декількох тисяч загроз та уразливостей інформаційно-комунікаційних систем. Зокрема, найбільш детальним описом такого роду є відкритий стандарт Європейського Союзу *IT Baseline Protection Manual* [8] обсягом більше чотирьох тисяч сторінок. Однак організація безпеки даних - не тільки систематизація, виявлення і відображення загроз, головне - управління ризиками, своєчасні превентивні заходи для зниження ризику загроз, щоденна

робота по системному забезпеченню безпеки [2]. Для вирішення даного завдання вже недостатньо виявляти і реагувати на дії порушників. Необхідно не тільки прогнозувати такі дії, виключати уразливості в системах мережного захисту, але і відволікати зловмисників від мережних вузлів, в яких здійснюється зберігання і обробка інформаційних ресурсів.

Більш як десятиліття тому виникло розуміння, що пряме протиборство з шкідливими мережними впливами є практично марним. Був зроблений цілком логічний висновок про необхідність застосування методів, узятих з арсеналу системного аналізу, дослідження операцій у військовій справі і, нарешті, радіоелектронної боротьби - радіоелектронної і радіорозвідки, радіоелектронної протидії, дезінформації та ін.

Новий підхід до виявлення атак на введення коду на базі хоста – це *Bee Master* [9]. Він застосовує парадигму *honeypot* до процесів обчислювальних систем і тим самим не спирається на деталі низького рівня. Основна ідея полягає в тому, щоб виявляти регулярні процесори обчислювальних систем як приманку для шкідливих програм. Цей підхід зосереджений на концепціях, таких як потоки або сторінки пам'яті, що присутні в кожній сучасній операційній системі. Тому *Bee Master* не страждає від недоліків низькорівневих підходів до обчислювальних систем.

Крім того, це дозволяє незалежному виявленню нападу на введення коду на основі хоста. Щоб перевірити можливості такого підходу, були отримані якісні і кількісні оцінки *Bee Master* на *Microsoft Windows* і *Linux*. Результати показують, що він досягає надійного та надійного виявлення для різних існуючих шкідливих сімей.

В даній дипломній роботі поставлена мета - вивчити метод управління процесом захисту інформаційної системи на основі теорії конфлікту і керованих марківських процесів. На основі такого досвіду побудувати алгоритмічні моделі

та вивчити динаміку боротьби зі зловмисником з використанням медових пасток та *Bee Master*.

Конфлікт не може розглядатися як оптимізаційна задача. При рівних ресурсах сторін "оптимальність" означає припинення конфлікту, а при нерівних - поразка більш слабкої сторони з ймовірністю одиниця. У той же час в конфлікті можливий виграш меншими силами. Проте, для досягнення виграшу з ймовірністю вище, ніж величина другого порядку малості, необхідно мати у своєму розпорядженні ресурсами одного порядку з ресурсами атакуючої сторони.

Конфлікт з розумним противником не може бути вирішена і в рамках теорії адаптації. Своїми активними діями противник з імовірністю, що прямує до одиниці, досягне максимального виграшу. Ми ж, адаптуючись до постійно погіршується умов, відповідно, опинимося в найбільш невигідній ситуації.

Тому основними завданнями, які необхідно вирішити для досягнення поставленої мети є:

- аналіз можливих стратегій конфлікту і вибір найбільш перспективних стратегій для даної задачі;

- вибір математичного апарату для опису процесів розвитку конфлікту;

- розробка математичної моделі конфлікту для отримання асимптотичних характеристик ефективності.

3.1 Технологія "медових пасток"

Технологія *Honeypot* (медової пастки) є одним з найбільш ефективних та доступних засобів виявлення та протидії атакам на мережні ресурси. . У мережі розташовується легкодоступна і приваблива для порушника мета, зовні невідрізнима від реальних ресурсів, єдине призначення якої - попастися на очі порушнику, спровокувати його на неправомірні дії і повідомити офіцеру

комп'ютерної безпеки про факт вторгнення. Іншими словами, *Honeypot* - це система виявлення спроб несанкціонованого доступу до інформаційних ресурсів. *Honeypot* імітує роботу реальної системи, що є потенційною метою хакерів і несанкціонованого доступу, відволікає на себе увагу і ресурси порушника, фіксує всі його дії і інформує службу безпеки про факти порушень. При цьому, в залежності від типу honeypot, імітуватися можуть будь-які системи, службовці потенційними об'єктами для атак: сервера, бази даних, мережні сервіси, файлові ресурси і т.д.

Переваги *Honeypot*-систем визначаються самим принципом їх роботи. Перш за все, це практично повна відсутність помилкових спрацьовувань. Оскільки *Honeypot* лише імітує реальну систему, і до нього не звертаються жодного реальні користувачів мережі, ні легальні мережні додатки, то будь-яка активність на *Honeypot* і будь-яка спроба звернення до нього є несанкціонованою і свідчить або про атаку, або про дослідження мережі із метою знайти вразливі місця в її захисту.

Визначення факту атаки є найважливішим моментом адміністраторів, так як дозволяє оперативно вжити заходів протидії. Але крім цього, *Honeypot* дозволяє також отримати інформацію, необхідну для вивчення дій порушника. Справа в тому, що *Honeypot* дозволяє зберегти сліди впливу для подальшого розслідування. Атаковану *Honeypot*-систему можна спокійно відключити і передати для аналізу власним або зовнішнім фахівцям з інформаційної безпеки, що зазвичай неможливо для реального сервера, наприклад сервера баз даних корпоративних додатків або поштового сервера.

За залишеним порушником слідах можна дізнатися про використовувані ним методи та засоби атаки, а також зробити висновки про її цілі. При цьому важливою особливістю *Honeypot*-систем є порівняно невелика кількість інформації, яку потрібно вивчати при розслідуванні інциденту. Реальні системи мережі протоколюють величезна кількість інформації і розслідування інцидентів

ІБ на основі логів численних мережних додатків і систем є досить трудомістким завданням. *Honeypot*, навпаки, містить лише потрібну інформацію, пов'язану з фактами порушень, тому що ніякої легальної активності на ньому не відбувається.

3.2 Місце *Honeypot* в системі безпеки промислового ДІКС

Як вже говорилося, технологія *Honeypot* є доступним і досить ефективним методом раннього попередження і виявлення вторгнень. З усього вищесказаного можна виділити два основних напрямки використання цій технології. Перше - це зниження ризику мережних атак на реальні системи. *Honeypot* дозволяє попереджати, виявляти і протоколювати діяльність порушника. Встановлений і грамотно налаштований *Honeypot* відверне увагу і ресурси порушника від реальних систем, дозволить виявити спробу атаки, надасть інформацію для її вивчення і дасть додатковий час для прийняття адекватних заходів захисту. Другий напрямок - отримання інформації для вивчення поведінки, методів та інструментарію порушників. Дослідницькі *Honeypot*-системи не зменшують ризик для ДІКС, але отримана з їх допомогою інформація може бути використана для побудови більш ефективних та надійних систем захисту реальних додатків і мереж.

На рис. 3.1 зображено схему найпростішої медової пастки.

Щоб основні ознаки *honeypot'a* були відсутні, вузол повинен обслуговвати зовнішній трафік, мати конфігурацію, відмінну від конфігурації за замовчуванням, легально використовуватися іншими учасниками мережі і т. д.

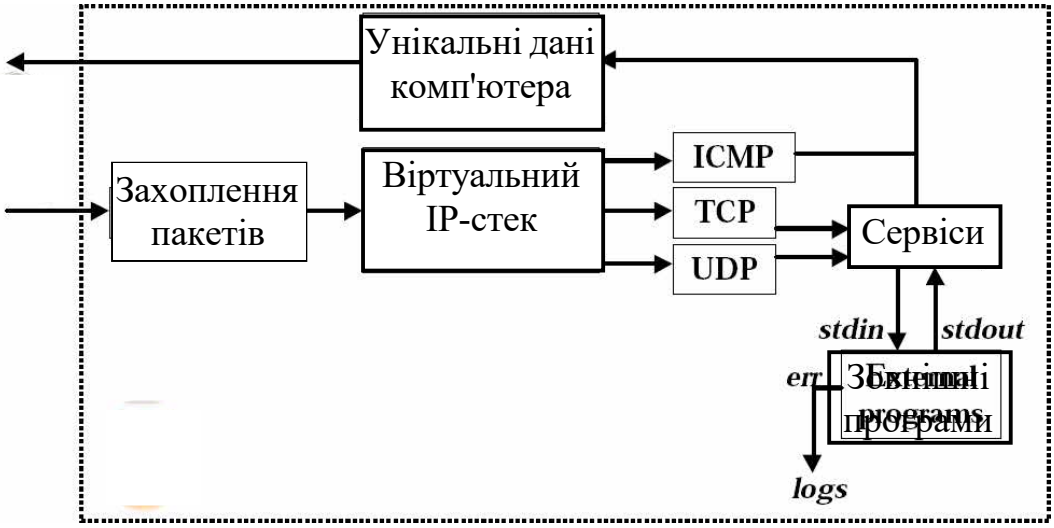

Рис. 3.1. Схема найпростішої медової пастки

Реальні і віртуальні приманки

Принади можуть бути реальними і віртуальними. Реальна приманка працює з виробничим програмним забезпеченням на виділеному апаратному обладнанні. Реальна приманка - одна з кращих мішеней, які можна запропонувати зломщикові. Вона виглядає і поводиться як справжній виробничий ресурс, і якщо дані на ній оновлюються, то зломщикові дуже важко здогадатися, що перед ним приманка.

Недолік реальних приманок полягає в тому, що для організації та управління ними, як правило, потрібно багато зусиль і часу. Для установки реальної приманки іноді необхідно стільки ж часу, скільки для інсталяції справжнього виробничого ресурсу. Ще один серйозний недолік полягає в тому, що важко перешкодити зломщикові, який захопив приманку, атакувати інший виробничий ресурс. У багатьох реальних принадах UNIX/Linux використовується механізм, який запобігає захопленню виробничих ресурсів (званий іноді механізмом управління даними - data-control mechanism), але лише деякі продукти Windows володіють такими функціями.

Віртуальні приманки є середовище емуляції, програмне забезпечення якої обмежує можливості зломщика. Як правило, потенційний збиток для виробничих ресурсів істотно зменшується або виключається повністю. Більшість віртуальних приманок може імітувати відкриті порти, закриті порти або порти з відповідає на запити службою.

Віртуальні приманки, які тільки відкривають порт і реєструють початковий запит зломщика, називаються простими слухачами порту (simple port listener). Більш високорозвинені слухачі порту можуть відповідати нескладними пакетами відкриття або закриття, що виглядає більш реалістично і привертає зломщика. Ці приманки записують інформацію, що посилається хакером, і відповідають відповідно до мережевим протоколом (наприклад, посилають пакет SYN). Принади залишають поза передачею ніяких інших даних, і спроба з'єднання зломщика ніколи не буває успішною. Такий обмін може дати адміністратора достатню інформацію, так як свідчить про несанкціоновану активності всередині периметра мережі і дозволяє звести ризик до мінімуму.

Силова протидія атакам і вторгненням в комп'ютерні мережі вимагає відволікання великих ресурсів і завершується успіхом лише в рідкісних випадках, наприклад, для випадку "розподілена атака - розподілений захист". У той же час розроблена в рамках загальної теорії конфлікту стратегія відволікання ресурсів противника на псевдосервіси може дати виграш навіть в разі переваги ресурсів атаки над ресурсами захисту.

Розглянемо моделі конфліктів "атака – захист" з затягуванням супротивника (хакера, зловмисника) у медову пастку хибного сервісу (псевдосервісу), а також динаміку розвитку конфлікту.

3.3 Розробка моделі конфлікту і аналіз стратегій атак та захисту

Відповідно до загальної теорії конфлікту процеси протиборства між атакуючої і захищається сторонами описуються диференційно-різницевими рівняннями або рівняннями з аргументами, що відхиляються [11]. Це припущення справедливо для дискретних систем з запізненням, якими є комп'ютерні мережі й розподілені інформаційні системи.

У загальному випадку

$$\begin{cases} z'_{ids}(t) = f_1\left(t, z_{ids}(t), \text{K}, z_{ids}(t-\tau_1), u_1(t), v_2(t-\tau_2), \xi(t)\right); \\ z'_{icm}(t) = f_2\left(t, z_{icm}(t), \text{K}, z_{icm}(t-\tau_2), u_2(t-\tau_2), v_1(t), \eta(t)\right), \end{cases} \quad (1)$$

де z_{ids} и z_{icm} – вектори стану систем S_{ids} и S_{icm} відповідно;

$u_1(t)$ и $u_2(t)$ – вектори управлінь в S_{ids} и S_{icm} відповідно;

$v_1(t)$ – вектор дій S_{ids} на S_{icm};

$v_2(t)$ – вектор дій S_{icm} на S_{ids};

$\xi(t)$ и $\eta(t)$ – вектори випадкових збурень, які діють на S_{ids} и S_{icm} відповідно;

τ_1 и τ_2 – запізнення у векторах S_{ids} и S_{icm} відповідно.

Ефективність E_1 системи S_{ids} й ефективність $Э_2$ системи S_{icm} на інтервалі спостереження T у загальному випадку являють собою нелінійні функціонали станів z_{ids}, z_{icm} и векторів $\xi(t)$, $\eta(t)$ відповідно. З рівняння (1) випливає їх взаємна залежність.

Якщо врахувати фактор нормалізації випадкових процесів у великих

системах [12], то можна застосувати для вирішення рівнянь (1) метод гаусовської апроксимації в малій околиці точок екстремуму E_1 і E_2. У цьому разі

вирази для ефективностей мають вигляд

$$E_1=\int_0^T z_{ids}(t)\,dt, \quad E_1 \to \max_{v_1}, \qquad E_2=\int_0^T z_{icm}(t)\,dt, \quad E_2 \to \max_{v_2}. \quad (2)$$

Мета кожної системи - максимально підвищити свою ефективність за рахунок зниження ефективності супротивної сторони. Однак результат докладених зусиль стане відомий тільки в момент часу T. На інтервалі спостереження $0 \le t \le T$ можна виробляти найкращі управління $u_1(t)$, дії $v_1(t)$ та прогнозувати кінцевий результат, тільки спираючись на припущення про стратегії поведінки супротивника й дані про поточні стани z_{ids} и z_{icm}. Включення в рівняння (1) функцій $v_1(t)$ означає відволікання частини ресурсу на формування захисних або контратакують впливів. Отже, необхідно вирішувати задачу конфлікту або з додатковим критерієм мінімізації частки ресурсу, що відводиться на захист, або з обмеженням на допустимий витрата цієї частки ресурсу. Схема моделі конфлікту [1] між сторонами атаки S_{icm} та захисту S_{ids}, модифікована для випадку застосування стратегій ескалації в псевдосервіси (пастки, хибні інформаційні системи), наведена у роботі [4]. Модель реального конфлікту, як правило, є нелінійною, але для отримання асимптотичних оцінок при досить великому інтервалі спостереження (і, відповідно, при великому числі кроків розвитку конфлікту) є припустимим робити покрокову лінеаризацію моделі з екстраполяцією на основі методів кореляції та регресії [13]. Для пошуку коефіцієнтів екстраполяції лінеаризованої моделі розроблено модифіковану покрокову процедуру з заміною та примусовим включенням незалежних змінних. При цьому усунення з вибірки незалежних змінних $X_1, X_2, \ldots, X_p$

(активні ресурси та псевдосервіси) відсутнього значення $X_i,\ 1 \le i \le p$ не є необхідним, оскільки воно може приводити до втрати про змінні

$X_1, X_2, \text{K}\, X_{i-1}, X_{i+1}, \text{K}\, X_p$ інформації, яка доставляється елементом X_i. Теоретично можна залишити цей елемент у вибірці та використати виміри, що містяться в ньому, для обчислення вектора середніх значень $\mathbf{X}$ та матриці коваріацій $\mathbf{R}_\mathbf{X}$.

У реальній ситуації для отримання цих даних приходиться використовувати наближені методи:

видалення елементів, лишаючи тільки комплектні елементи, тобто елементи з повністю присутніми значеннями;

підстановку середнього: замість відсутнього значення X_i підставляється середнє значення $\bar{x}_i$, завдяки чому результуюча вибірка комплектується до повного об'єму n;

попарного викреслювання, підстановки регресії тощо.

На жаль, для будь-якого зі згаданих методів їх статистичні властивості частіше за все невідомі, тому немає гарантій, що отримані оцінки будуть незміщеними. Тому елементи вибірки та/або змінні з відсутніми значеннями повинні бути видалені так, щоб забезпечити баланс між числом змінних і числом елементів, що залишилися. Іншими словами, максимізується число комплектних елементів вибірки: якщо елемент містить багато пропусків, його треба усунути. З іншого боку, якщо значення будь-якої змінної невідомо для більшості елементів, треба видалити цю змінну. Тоді можна застосовувати стандартні методи множинного регресійного аналізу [14].

На рис. 1 зображено математичну модель процесів розвитку конфлікту з передбаченням та виправленням помилкових припущень (модель типу "предиктор-коректор" [15]).

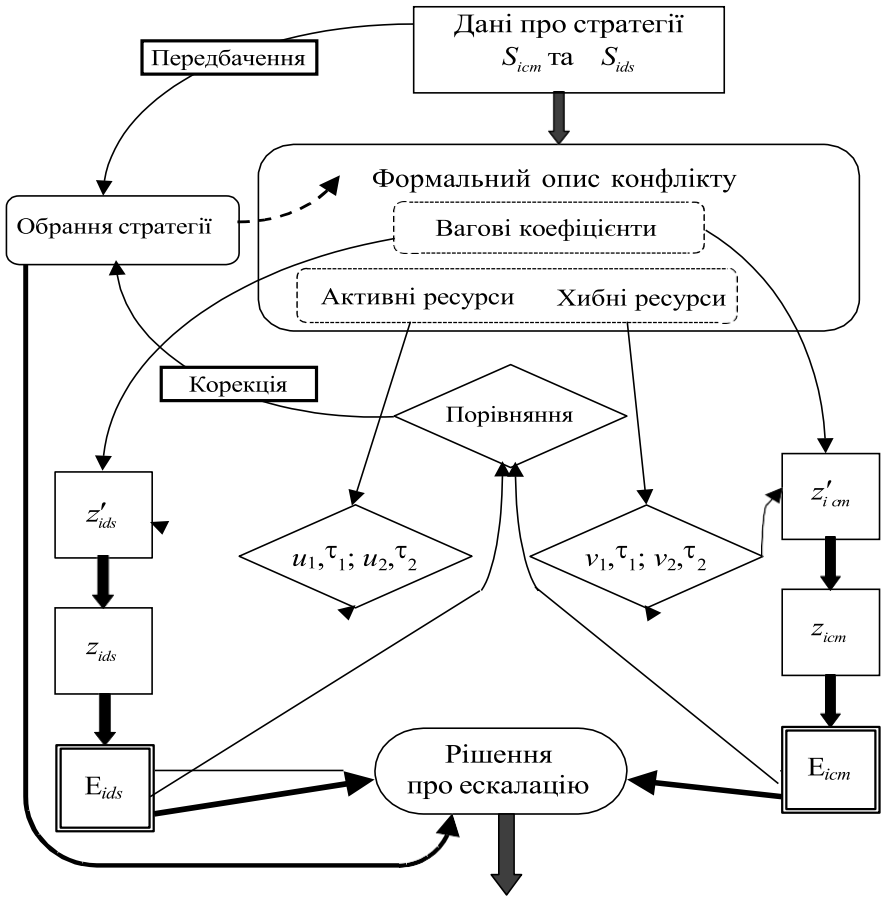

Рис. 3.2. Схема лінеарізованої моделі конфлікту з можливою ескалацією в псевдосервіси

Стратегії протидії і атак, розроблені відповідно до класичної теорії конфлікту [9] і модифіковані для конкретної розглянутої задачі, наведені в [4]. Тут же розглянемо набір найбільш наочних стратегій захисту:

- ешелонування рубежів захисту типу "зовнішня - демілітаризована - внутрішня зони безпеки";

- відмова від отримання - просте повернення підозрілого трафіку;

- розподілена відмова від отримання - трансляція підозрілого трафіку на кілька точок і повернення джерела з усіх цих точок;

- насичення рубежів захисту псевдосервісами з відтворенням добре відомих вразливостей - затягування противника в ескалаційну пастку;

реакція на агресивну поведінку хакера – демонстрація спокою;

реакція на нейтральну поведінку – демонстрація впевненості;

реакція на втрату інтересу – демонстрація розгубленості.

В системі захисту, заснованої на теорії конфлікту, передбачаються активні дії по відображенню атаки. Тут розглядаються теоретичні моделі і методи аналізу, прогнозу розвитку конфлікту і оптимізації послідовностей захисних дій. Щодо правових аспектів адекватності заходів контратаки передбачається лише, що оцінка цієї адекватності в технічних системах може бути зроблена досить точно і об'єктивно.

3.4 Динамічні характеристики процесу розвитку конфлікту з затягуванням у медову пастку (ескалацією в псевдосервіси)

Процес розвитку конфлікту є розгалуженим випадковим напівмарківським процесом, перехідні і фінальні ймовірності якого залежать від співвідношення стратегічних (S_{ids}, S_{icm}) й енергоінформаційних (E_{ids}, E_{icm}) ресурсів сторін. Поточний стан процесу можна записати в вигляді деякого функціоналу $\delta R = \Psi\lceil\lfloor \varphi(S_{ids}, E_{ids}), \varphi(S_{icm}, E_{icm})\rceil\rfloor$, яким характеризується інтегральний виграш від застосування тієї чи іншої стратегії з урахуванням інтенсивності її застосування. Власне стратегія оцінюється по своїй інформаційній цінності, а інтенсивність - з енергетичного ресурсу (наприклад, за кількістю точок, з яких проводиться розподілена атака). В якості першого наближення для вибору виду функціоналу можна взяти адитивну міру безлічі стратегій, а відносний вплив конкретної стратегії врахувати ваговими коефіцієнтами або функціями.

Розглянемо алгоритмічну модель конфлікту між розподіленими системами атаки і захисту. Схема процесу моделювання атакуючих і контратакуючих потоків зображена на рис. 2.

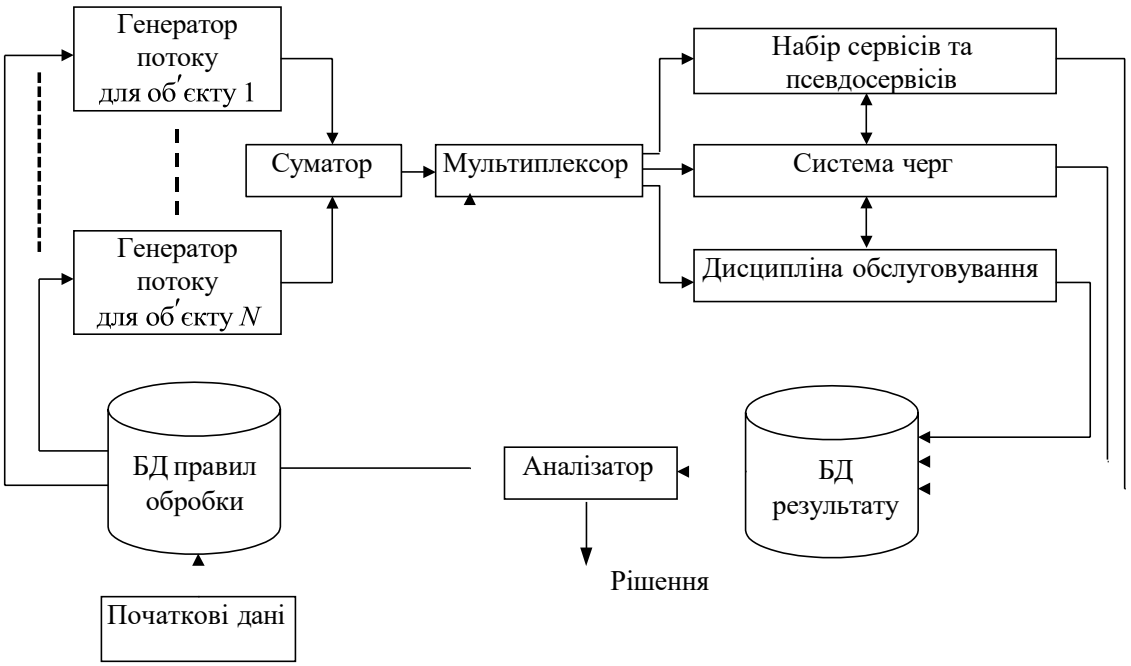

Рис. 3.3. Алгоритмічна модель формування медових пасток (псевдосервісів)

Як видно з рис. 3.3, рішення про вибір напрямку розвитку конфлікту приймаються на підставі результатів повного аналізу параметрів і стану системи, наявних вихідних даних і поточної інформації про характеристики мережного трафіку.

Мають місце послідовності дій і відповідних захисних заходів (пасивних, активних або й тих, і інших). Припустимо, що в результаті атаки ймовірність штатного функціонування об'єкта знижується, можливо, до нуля, а в результаті застосування відповідної захисного заходу ймовірність функціонування об'єкта підвищується, можливо, аж до вихідної величини. Таким чином, в кожен момент часу система може перебувати в одному з N можливих фазових станів ϕ_1,ϕ_2,K,ϕ_N, характеризують поточну ймовірність функціонування об'єкта. Відомі початковий стан системи (в початковий момент часу t_0 вона знаходиться в стані $\psi_0=\phi_i$) і однокрокові ймовірності переходу $\rho_{ik}=P\{\psi_l=\phi_k \mid \psi_{l-1}=\phi_i\}$,

$i,k=1,N$. Отже, якщо ігнорувати випадковий характер часу очікування і

цікавитися тільки моментами переходу, то процес $\psi_l = \psi(t_l)$ є вкладений однорідний ланцюг Маркова [6]. Імовірність переходу ρ_{ik} повністю визначається i-м станом об'єкта і результатами k-ї атакуючої дії.

Затримки τ_1 и τ_2 в системах S_{ids} и S_{icm} являють собою дискретні процеси $z_{ids}(\tau_1)$, $z_{icm}(\tau_2)$, які не обов'язково є марківськими. Однак це не критично для подальшого аналізу, оскільки самі величини ρ_{mn}, $m,n \in M$, дають вичерпну інформацію про еволюцію конфлікту.

Порівняємо кожному з ненульових елементів ρ_{ik} матриці ймовірностей переходу випадкову величину ζ_{ik} з функцією розподілу $F_{ik}(t) = F_{ik}(\tau_{ik} \le t)$. У розглянутій задачі випадкову величину ζ_{ik} будемо трактувати як час перебування атакується об'єкта в стані ϕ_i за умови, що наступним станом, в яке перейде об'єкт, буде ϕ_k. При цьому величина ζ_{ik} вважається не негативною і безперервною з щільністю ймовірності $w_{ik}(t)$. При такій інтерпретації величину ζ_{ik} можна назвати часом знаходження об'єкта в стані ϕ_i до переходу в стан ϕ_k.

Припустимо, що точка, яка відображає поведінку системи в просторі станів, залишиться в стані ϕ_i впродовж часу ζ_{ij}, до того, як вона перейде в ϕ_j (див. рис.

3.4 й 3.5). По досягненні стану ϕ_j «миттєво» (відповідно до матриці ймовірностей переходу $\{\rho_{ik}\}$) обирається наступний стан ϕ_n, $n=\overline{1,N}$. Тут «миттєвість» трактується в тому сенсі, що тривалість переходу є величиною другого порядку малості в порівнянні з мінімальною тривалістю перебування в поточному стані.

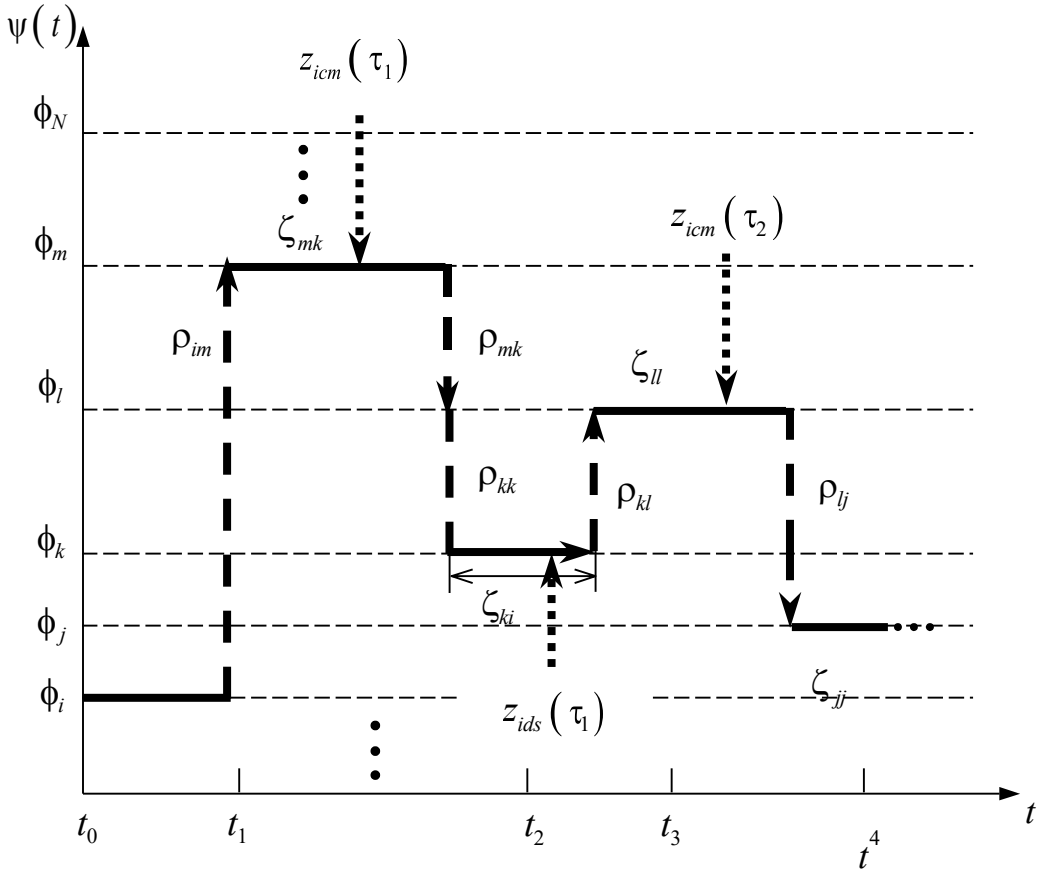

Рис. 3.4. Зміна ймовірностей функціонування об'єкта з системою захисту.

$$z_{icm}(\tau_n)\ \phi z_{ids}(\tau_n)$$

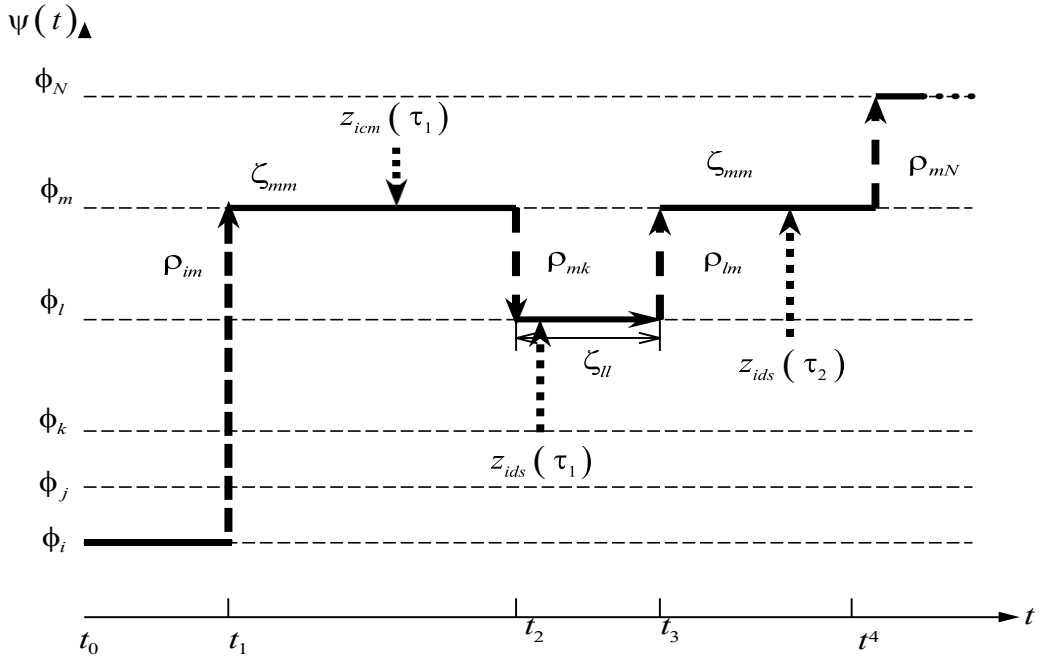

Рис. 3.5. Зміна ймовірностей функціонування об'єкта з системою захисту.

$$z_{ids}(\tau_n)\ \phi z_{icm}(\tau_n)$$

Якщо для точки, що відображає поведінку системи і знаходиться в -м стані, з імовірністю переходу ρ_{ll} знову обирається стан l, горизонтальна частина траєкторії руху точки позначається лінією зі стрілкою на кінці, як це зображено на графіках, див. рис. 3 и 4. Выраз $x \phi y$ означає домінування x над y.

Після того, як наступний стан ϕ_i обраний, час очікування в поточному стані ϕ_k вважається рівним ζ_{ki} з функцією розподілу $F_{ki}(t)$ або, відповідно, з щільністю імовірності $w_{ki}(t)$. Цей процес надалі необмежено триває. Кожен раз незалежно вибираються наступний стан і час очікування. Якщо через $\psi(t)$ позначити стан системи, в якому вона знаходиться в момент часу t, то отриманий випадковий процес є напівмарківським. При заданому початковому стані подальшу поведінку процесу повністю визначається матрицею ймовірностей переходу $\{\rho_{ik}\}$, $i,k=\overline{1,N}$, и матрицею функцій розподілу $\{F_{ki}(t)\}$.

Сучасний підхід до побудови систем виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак на інформаційне системи сповнений недоліків і уразливостей, що дозволяють, на жаль, зловмисні ним впливам успішно долати системи захисту інформації. Перехід від пошуку сигнатур атак до виявлення передумов визначення загроз інформаційної безпеки повинен сприяти тому, щоб докорінно змінити дану ситуацію, скоротивши дистанцію відставання в розвитку систем захисту від систем їх подолання.

Крім того, такий перехід повинен сприяти підвищенню ефективності управління інформаційною безпекою і, нарешті, більш конкретних прикладів

застосування нормативних та керівних документів, які вже стали стандартами.

Вельми перспективним напрямом подальшого розвитку систем інформаційного захисту представляються ескалаційні пастки з імітацією боротьби з супротивником шляхом стохастичного управління змінами уразливостей псевдосервісів (медових пасток). [1-44]

3.5. Висновки до розділу

Розглянуто та проаналізовано захист комп'ютерної мережі від розподілених атак. Метод, який часто використовується шкідливим програмним забезпеченням для приховування цільової системи, - атака на введення коду на основі хоста. Він дозволяє шкідливому програмному продукту виконувати свій код у зовнішньому процесовому просторі, що дозволяє йому працювати таємно та отримувати доступ до критичної інформації інших процесів. Оскільки існує безліч різних способів введення та виконання коду в зовнішньому процесовому просторі, необхідний загальний підхід, що охоплює всі ці можливості. Підходи, що фокусуються лише на деталях операційної системи низького рівня (наприклад, підключення *API*) недостатньо, оскільки підозрілий набір *API* постійно розширюється. Таким чином, підходи, орієнтовані на деталі операційної системи низького рівня, схильні до втрати нових атак. Крім того, такі підходи обмежуються інтимним знанням лише однієї операційної системи.

Розглянута технологія "медових пасток". Технологія *Honeypot* (медової пастки) є одним з найбільш ефективних та доступних засобів виявлення та протидії атакам на мережні ресурси. У мережі розташовується легкодоступна і приваблива для порушника мета, зовні невідрізнима від реальних ресурсів, єдине призначення якої - попастися на очі порушнику, спровокувати його на неправомірні дії і повідомити офіцеру комп'ютерної безпеки про факт вторгнення.

Проаналізовано місце *Honeypot* в системі безпеки промислового ДІКС.

Розроблено модель конфлікту і аналіз стратегій атак та захисту.

Відповідно до загальної теорії конфлікту процеси протиборства між атакуючої і захищається сторонами описуються диференційно-різницевими рівняннями або

рівняннями з аргументами, що відхиляються. Це припущення справедливо для дискретних систем з запізненням, якими є комп'ютерні мережі й розподілені інформаційні системи.

Розглянути динамічні характеристики процесу розвитку конфлікту з затягуванням у медову пастку (ескалацією в псевдосервіси).

Власне стратегія оцінюється по своїй інформаційній цінності, а інтенсивність - з енергетичного ресурсу (наприклад, за кількістю точок, з яких проводиться розподілена атака). В якості першого наближення для вибору виду функціоналу можна взяти адитивну міру безлічі стратегій, а відносний вплив конкретної стратегії врахувати ваговими коефіцієнтами або функціями.

ВИСНОВКИ

У дипломній роботі розглянуті питання організації системи захисту інформації в Домашній ІКС.

Дана тема має велике значення для сталого розвитку ДІКС. На сьогоднішній день розробка і впровадження мережних інформаційних систем є одним з найцікавіших і важливих завдань в області інформаційних технологій. У процесі дипломного проектування була вивчена структура обчислювальної мережі ДІКС, проаналізовані потоки інформації, що циркулюють у внутрішній мережі ДІКС, а так само потоки інформації, що циркулюють між філіями. Також представлена алгоритмічна схема передавання і зберігання інформації, організації електронного документообігу.

У дипломній роботі запропоновані додаткові заходи захисту інформації, розроблена архітектура системи захисту безпеки й обмеження доступу в корпоративну комп'ютерну мережу ДІКС:

мережний периметр вузлів та каналів передачі даних;

брандмауери та маршрутизатори з фільтрацією пакетів;

транслятори мережних адрес;

транслятори адрес основних та альтернативних портів;

підсистема захисту від розподілених мережних атак:

псевдосервіси з явними уразливостями ("медові пастки");

мережні псевдосервіси з уразливостями (мережні "медові пастки").

В якості базисного рішення для підсистеми захисту від розподілених мережних атак застосовано теорію конфлікту та адаптації степенів уразливості до поведінки атакуючого суб'єкта:

агресивна поведінка – демонстрація спокою;

нейтральна поведінка – демонстрація впевненості;

втрата інтересу – демонстрація розгубленості.

Такі зміни стратегій взаємодії системи захисту з атакуючим суб'єктом дозволяють утримувати його у постійній напрузі і усувають підозри в тому, що суб'єкт попав у медову пастку.

Для охорони конфіденційної інформації, що передається між філіями, використана технологія віртуальної корпоративної мережі ДІКС, що дозволяє реалізувати захист каналу передачі даних від перехоплення і підміни інформації. Для захисту внутрішньої інформаційної структури ДІКС використані антивірусні рішення.

Проксі-сервери застосовуються для наступних цілей:

· Забезпечення доступу з комп'ютерів локальної мережі в Інтернет.

· Кешування даних: якщо часто відбуваються звернення до одних і тих же зовнішніх ресурсів, то можна тримати їх копію на проксі-сервері і видавати за запитом, знижуючи тим самим навантаження на канал у зовнішню мережу і прискорюючи отримання клієнтом запитаної інформації.

· Стиснення даних: проксі-сервер завантажує інформацію з Інтернету і передає інформацію кінцевому користувачеві в стислому вигляді. Такі проксі-сервери використовуються в основному з метою економії зовнішнього трафіку.

· Захист мережі від зовнішнього доступу: наприклад, можна налаштувати проксі-сервер так, що комп'ютери будуть звертатися до зовнішніх ресурсів тільки через нього, а зовнішні комп'ютери не зможуть звертатися до термінальних вузлів взагалі (вони «бачать» тільки проксі-сервер).

· Обмеження доступу з корпоративної мережі до зовнішньої: наприклад, можна заборонити доступ до певних джерел, обмежити використання інтернету якимось локальним користувачам, встановлювати квоти на трафік або смугу пропускання, фільтрувати рекламу, підозрілий трафік і віруси.

· Анонімність доступу до різних ресурсів. Проксі-сервер може приховувати відомості про джерело запиту або користувача. В такому випадку зовнішній сервер бачить лише інформацію про проксі-сервер, наприклад, IP-адреси, але не має можливості визначити дійсне джерело запиту. Існують також спотворюючі проксі-сервери, які передають сторонньому серверу неправдиву інформацію про справжнього користувача.

Для управління використовується інтерфейс, який має великий набір інструментів з управління доступом користувачів по протоколах HTTP і FTP. Так само є можливість подивитися статистичні дані, такі, як часто відвідувані вузли, кількість «спійманих» вірусів і т.д.

Для взаємодії філії з центральним офісом по *VPN* каналу використовується термінал-сервер. Термінальний клієнт після встановлення зв'язку з термінальним сервером пересилає на останній вводяться дані (натискання клавіш, переміщення миші) і, можливо, надає доступ до локальний ресурсів (наприклад, принтер, дискові ресурси, пристрій читання смарт-карт, локальні порти (*COM* / *LPT*)). Термінальний сервер забезпечує середовище для роботи (термінальна сесія), в якій для роботи програм користувача. Результат роботи сервера передається на клієнта, як правило, це зображення для монітора і звук (при його наявності). Переваги схеми з використанням термінального сервера в повніше очевидні.

· Зниження навантаження на канал зв'язку

· Підвищення безпеки

· По *VPN* каналу передаються менш небезпечні дані.

Таким чином, поставлені завдання на дипломну роботу, виконані. Отримані результати можуть використовуватися (з відповідними змінами та доповненнями) для захисту інформації в корпоративних комп'ютерних мережах підприємств різного масштабу та призначення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. The Great IDS Debate: Signature Analysis Versus Protocol Analysis by Matt Tanase, Feb. 5, 2003/ Електронний ресурс: режим доступу: https://community.broadcom.com/symantecenterprise/communities/communi ty-home/librarydocuments/viewdocument?DocumentKey=b4c1f4bd-4199-4d9e-b61b-486b3df2d76c&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

2. CompTIA Security+ SY0-501 Cert Guide, Academic Edition, 2nd Edition By David L. Prowse - 560 pp.

3. Kurose J.F. Computer Networking: A Top-Down Approach, 7th Ed / James F. Kurose, Keith W. Ross. - Pearson Education, Inc., 2017. - 864 pp.

3. Stallings W. Computer Organization and Architecture, 10th Ed. / Pearson Education, Inc., Hoboken, NJ, 2016. - 864 pp.

4. Ng C.K. Honeypot Frameworks and their Applications: A New Framework /Chee Keong Ng, Lei Pan, Yang Xiang. - Springer Nature Singapore Pte Ltd., 2018. - 81 pp.https://www.projecthoneypot.org/

5. Lance Spitzner. Honeypots: Tracking Hackers. Addison Wesley, 2002. - 480 pp.http://www.iso27000.ru/standarty/bsi-it-baseline-protection-manual

6. Barabosch T. Bee Master: Detecting Host-Based Code Injection Attacks//Thomas Barabosch, Sebastian Eschweiler, and Elmar Gerhards-Padilla. - in Proceedings of 11th International Conference, DIMVA 2014, Egham, UK, July 10-11, 2014/

7. Diogenes Y. Cybersecurity - Attack and Defense Strategies / Yuri Diogenes, Erdal Ozkaya. - Packt Publishing Ltd., Livery Place,35 Livery Street, Birmingham, B3 2PB, UK, 2018. - 354 pp.

8. Cybersecurity Best Practices Guide For IIROC Dealer Members - Investment Industry Regulatory Organization of Canada, 2015. - 53 pp.

9. Joseph Migga Kizza J.M. Guide to Computer Network Security, Fourth Edition. - Springer International Publishing AG 2017. - 569 pp.

10. Zhu S.Y. Guide to Security in SDN and NFV: Challenges, Opportunities, and Applications. / Shao Ying Zhu, Sandra Scott-Hayward, Ludovic Jacquin, Richard Hill (Editors). - Springer International Publishing AG 2017, Gewerbestrasse 11, 6330 Cham, Switzerland, 2017. - 331 pp.

11. Stapelberg R.G. Handbook of Reliability, Availability, Maintainability and Safety in Engineering Design. Springer-Verlag London Limited, 2009. - 827 pp.

12. Csermely P. WEAK LINKS: The Universal Key to the Stability of Networks and Complex Systems. - Springer-Verlag Berlin Heidelberg 2009. - 404 pp.

13. Stavroulakis P. RELIABILITY, SURVIVABILITY AND QUALITY OF LARGE SCALE TELECOMMUNICATION SYSTEMS. - John Wiley & Sons, Ltd., The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England. 2003 - 353 pp.

14. Buttazzo G.C. Hard Real-Time Computing Systems (3rd Edition). Springer Science+Business Media, LLC 2011. - 521 pp.

15. Klein M.H. A Practitioner's Handbook for Real-Time Analysis / Mark H. Klein, Thomas Ralya, Bill Pollak, Ray Obenza. - KIuwer Academic Publishers, 1993. - 701 pp.

16. Ding D. Performance Analysis and Synthesis for Discrete-Time Stochastic Systems with Network-Enhanced Complexities / Derui Ding, Zidong Wang, Guoliang Wei. - CRC Press, Taylor & Francis Group, 6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL, USA, 2019. - 249 pp.

17. Krten R. QNX Neutrino RTOS. - QNX Software Systems Limited, 1001 Farrar Road, Kanata, Ontario, Canada, 2012. - 372 pp.

18. Stallings W. Data and Computer Communications, Tenth Edition. - Pearson Education, Inc., Prentice Hall, 1 Lake Street, Upper Saddle River, New Jersey, USA, 2014. - 889 pp.

19. Stallings W. WIRELESS COMMUNICATIONS AND NETWORKS, 2nd Ed. - Pearson Education, Inc., Upper Saddle River, NJ, USA, 2005. - 559 pp.

20. Crimes R.A. Honeypots for Windows. - APRESS, 2005. - 392 pp.

21. Joshi R.C. Honeypots A New Paradigm to Information Security / R.C. Joshi, Anjali Sardana. - Science Publishers, P.O. Box 699, Enfi eld, NH 03748, USA, 2001. - 323 pp.

22. Park J.H. Future Information Technology / James J. (Jong Hyuk) Park, Yi Pan, Cheon-Shik Kim, Yun Yang. - Springer-Verlag Berlin Heidelberg 2014. - 936 pp.

23. Шнайдер Б. Прикладная криптография, 2 изд. - М.: Диалектика, 2016. - 610 стр.

24. Шнайдер Б. Секреты и ложь. Безопасность данных в цифровом мире. СПб: Питер,2003. - 368 стр.

25. Орлов И.Я. Перспективные методы защиты информационных радиосистем от помех. - Нижний Новгород: Изд-во Нижегородского госуниверситета, 2006. –126 с.

26. Graham R. COMMUNICATIONS, RADAR AND ELECTRONIC WARFARE. - John Wiley and Sons, Ltd., The Atnum. Southern Gate, Chiche;ter, We;t Sussex, PO 19 8SQ, United Kmgdom. 2011. - 378 pp.

27. Mesarovic M.D. General Systems Theory: Mathematical Foundations. / M.D. Mesarovic, Yasuhico Takahara. - Academic Press, New York, 1975, xii+268 pp.

28. Marchau V.A.W.J. Decision Making under Deep Uncertainty: From Theory to Practice / Vincent A. W. J. Marchau, Warren E. Walker,Pieter J. T. M. Bloemen, Steven W. Popper - Springer Nature Switzerland AG, Gewerbestrasse 11, 6330 Cham, Switzerland, 2019. - 405 pp.

29. Myers G.J. The Art of Software Testing 3rd Ed. / Glenford J. Myers, Corey

Sandler, Tom Badgett. - John Wiley & Sons, Inc., 2012. - 256 pp.

30. Saaty T. L. The analytic hierarchy process / T. L. Saaty. - McGraw Hill, N.-Y., 1980, 288 pp.

31. Bonaventure O. Computer Networking : Principles, Protocols and Practice. - Release Sep 07, 2018. - 272 p.

32. Benslama M. Ad Hoc Networks Telecommunications and Game Theory / Malek Benslama Mohamed Lamine Boucenna Hadj Batatia. - John Wiley & Sons, Inc., 2015. – 141 pp.

33. Bendat J. Random Data: Analysis and Measurement Procedures. Fourth Edition / Julius S. Bendat, Allan G. Piersol. - John Wiley & Sons, Inc., Hoboken, New Jersey, 2010. - 640 pp.

34. Bensky A. Short-range Wireless Communication, 3rd Ed.- Elsevier, The Boulevard, Langford Lane, Kidlington, Oxford OX5 1GB, United Kingdom, 2019. - 462 pp.

35. Андрусяк А.І., Дем’янчук В.С., Юр’єв Ю.М. Мережа авіаційного електрозв’язку. – К.: НАУ, 2001. – 448 с.

36. Якість та ефективність системи організації повітряного руху // Биковцев І.С., Дем’янчук В.С., Клименко В.О., Майкова О.С., Матвієнко А.Г., Петрашевський А.О., Чередниченко Ю.А., Чорнобай В.М., Юр’єв Ю.М., Яковлєв О.І. – К.: ДП ОПР, 2010. – 316 с.

37. Afifi A. Statistical Analysis: A Computer Oriented Approach 2nd Edition / A. A. Afifi, S. P. Azen. - Academic Press; 2 ed., 1979. - 442 pp.