

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

Кафедра _____ **Комп'ютерних систем та мереж** _____

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
комп'ютерних систем та мереж

_____ (Жуков І.А.)

« ____ » _____ 2021 р.

ДИПЛОМНИЙ ПРОЄКТ
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ
"БАКАЛАВР"

Тема: _____ **Захист інформації в комп'ютерній корпоративній мережі** _____

Виконавець: _____ **Басок Б.О.** _____

Керівник: _____ **Малярчук В.О.** _____

Нормоконтролер: _____ **Журавель С.В.** _____

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, комп'ютерної та програмної інженерії

Кафедра комп'ютерних систем та мереж

Напрямок (спеціальність) 123 "Комп'ютерна інженерія"

(шифр, найменування)

ЗАТВЕРДЖУЮ

Завідувач кафедри

комп'ютерних систем та мереж

_____ (Жуков І.А.)

« ____ » _____ 2021 р.

ЗАВДАННЯ

на виконання дипломного проекту

Баска Богдана Олександровича

(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема проекту (роботи): Захист інформації в комп'ютерній корпоративній мережі

затверджена наказом ректора від "26" квітня 2021 року № 648/ст

2. Термін виконання проекту (роботи): з 24.05.2021 до 20.06.2021

3. Вихідні дані до проекту (роботи): Проаналізувати засоби захисту інформації в комп'ютерних корпоративних мережах. Розхлянути захист мережі від розподілених атак

4. Зміст пояснювальної записки (перелік питань, що підлягають розробці):
Стан проблеми захисту інформації підприємства. Захист мережевого периметра комп'ютерної мережі. Захист комп'ютерної мережі від розподілених атак.

5. Перелік обов'язкового графічного матеріалу:

Презентація PowerPoint

6. Календарний план

№ п/п	Етапи виконання дипломного проекту	Термін виконання етапів	Примітка
1	Ознайомитися з тематикою дипломних проєктів. Вибір теми.	24.04.2021 – 25.04.2021	
2	Узгодити технічне завдання	26.04.2021 – 01.05.2021	
3	Опрацювати літературні матеріали за темою дипломного проєкту	02.05.2021 – 05.05.2021	
4	Опрацювати проблеми захисту інформації підприємства	06.05.2021 – 15.05.2021	
5	Опрацювати проблему захист мережевого периметра комп'ютерної мережі підприємства	16.05.2021 – 01.06.2021	
6	Оформити текстові і графічні матеріали дипломної роботи	02.06.2021 – 11.06.2021	
7	Підготувати презентацію по дипломній роботі	12.06.2021 – 13.06.2021	
8	Захистити дипломний проєкт	14.06.2021	

7. Дата отримання завдання « 24 » квітня 2021 р. _____

Керівник дипломного проекту _____
(підпис) Малярчук В.О.

Завдання прийняв до виконання _____
(підпис студента) Басок Б.О.

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Захист інформації в комп'ютерній корпоративній мережі» містить 56с., 12 рис., 38 літературних джерел.

СИСТЕМА ЗАХИСТУ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ ПІДПРИЄМСТВА, КОМП'ЮТЕРНА МЕРЕЖА ПІДПРИЄМСТВА, ЗАХИСТ МЕРЕЖЕВОГО ПЕРИМЕТРА, СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ В КОРПОРАТИВНУ МЕРЕЖУ.

Актуальність теми. Задачі підвищення ефективності забезпечення системи захисту інформації підприємства, компонентів комп'ютерної мережі підприємства, інформаційна безпека, є актуальними.

Об'єкт та предмет дослідження. Корпоративна комп'ютерна мережа підприємства. Стан проблеми захисту інформації підприємства. Захист мережевого периметра комп'ютерної мережі. Захист комп'ютерної мережі від розподілених атак.

Мета дипломної роботи. Вирішення проблеми принципу захисту комп'ютерних мереж підприємств. 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 комп'ютерній мережі підприємства.

Методи дослідження. Методи аналітичних оглядів і аналізів початкових даних для побудови вирішення проблеми принципу захисту комп'ютерних мереж підприємств. Основні побудови системи захисту мережевого периметру. Технологія “медових пасток”. Honeypot в системі безпеки промислового підприємства. 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 підприємства.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, ТЕРМІНІВ.....	6
ВСТУП	7
РОЗДІЛ 1 ПРОБЛЕМА ЗАХИСТУ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ.....	11
1.1. Терміни та визначення.....	11
1.2. Основні принципи захисту комп'ютерних корпоративних мереж.....	12
1.3. Класифікація та системи виявлення комп'ютерних атак.....	14
Висновки до розділу	20
РОЗДІЛ 2 МЕРЕЖЕВИЙ ПЕРИМЕТР КОМП'ЮТЕРНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ ТА ЙОГО ЗАХИСТ	21
2.1. Основні принципи захисту мережевого периметру	21
2.2. Системи виявлення вторгень	27
2.3. Система проактивного захисту інформації в комп'ютерній корпоративній мережі.....	32
Висновки до розділу.....	35
РОЗДІЛ 3 РОЗПОДІЛЕНІ АТАКИ НА КОМП'ЮТЕРНУ КОРПОРАТИВНУ МЕРЕЖУ ТА ЇЇ ЗАХИСТ	36
3.1. Технологія Honeypot	38
3.2. Система безпеки промислового підприємства та місце технології Honeypot в системі.....	39
3.3. Створення моделі конфлікту, стратегії атаки та захисту.....	41
3.4. Процес розвитку конфлікту з затягуванням у медову пастку та його динамічні характеристики	44
Висновки до розділу	48
ВИСНОВКИ.....	50
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	51

Кафедра КСМ

НАУ 21 05 98 000 ПЗ

Виконав	Басок Б.О.			Захист інформації в комп'ютерній корпоративній мережі	Літера	Аркуш	Архів
Керівник	Малярчук В.О.					5	56
Консульт.					123 КС-434Б		
Норм. контр.	Журавель С.В.						
Зав. Каф.	Жуков І.А.						

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
LAN	–	локальна мережа
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

Питання систематизації захисту комп'ютерної мережі підприємства стає актуальнішим з кожним роком.

На даний момент збільшується кількість злочинів в сфері комп'ютерних систем. Спостерігається тенденція до диференціювання систем захисту комп'ютерних та об'єднаних мереж від загроз. Існує багато прикладів цих систем, звітів та протоколів, технологічних розробок, проектів, висновків та прогнозів, зроблені на основі перерахованого. З розвитком різноманіття ризиків і з удосконаленням сучасних мереж, рішення щодо захисту має бути підкріплене чіткими знаннями й досвідом у виконанні міждисциплінарних завдань. До переліку найрозповсюдженіших випадків атак і несанкціонованих вторгнень входить спеціальне використання небезпечного програмного коду (вірусів, хробаків, троянських програм), а також атаки типу *DoS* (відмова в обслуговуванні) і *DDoS* (розподілена відмова в обслуговуванні).

Безпека забезпечується декількома ключовими елементами, що мають складати цілісну та ефективну інфраструктуру захисту:

- управління доступом;
- управління погрозами;
- управління конфіденційністю;
- ведення контрольних журналів та моніторинг.

Аналіз виявлених атак на комп'ютерні мережі і системи проводиться давно. Ознаки атак, методи виявлення несанкціонованого проникнення в системи підприємств постійно досліджуються, диференціюються та удосконалюються. До того ж сюди можна включити дослідження в сфері побічних електромагнітних випромінювань і наведень, адже у електромагнітних атак є аналоги в комп'ютерно-мережному середовищі.

На сьогоднішній день дослідження в області захисту від комп'ютерних атак, розробки систем виявлення вторгнень та ін. спричиняють запровадження

програмних або апаратно-програмних рішень. Вони автоматизують процес контролю та фіксування подій, що відбуваються в комп'ютерній системі або мережі, а також проводить моніторинг ознак проблем безпеки. З тенденцією поширення та утворення різних типів і способів несанкціонованих проникнень в сторонні комп'ютерні мережі, системи виявлення атак є актуальними та невід'ємними частинами інфраструктури безпеки усіх установ, організацій і підприємств.

Виділяють системи виявлення аномальної поведінки (*anomaly detection*) та системи виявлення злочинної поведінки (*misuse detection*). Перші засновані на констатації деяких ознак, що описують правильну або допустиму поведінку об'єкта спостереження. Під «нормальною» або «правильною» поведінкою позначають дії, що виконуються об'єктом та не порушують політику безпеки. Системи виявлення злочинної поведінки характеризуються заделегідь відомими ознаками, що окреслює поведінку зловмисника. Найрозповсюдженішими способами виявлення злочинної поведінки є експертні та статистичні методи.

Як і більшість сучасних програмних продуктів, системи виявлення атак мають задовільняти конкретні потреби, а саме певні вимоги. Це можуть бути і теперішні технології розробки, і врахування особливостей сучасних інформаційних мереж, і здатність працювати паралельно з іншими програмами.

При створенні інфраструктури систем захисту комп'ютерних мереж необхідно пам'ятати про наступні фактори:

- інформаційна мережа розподілена як територіально, так і функціонально за означенням;
- атаки на комп'ютерну мережу удосконалились та набули високого рівня різноманіття;
- більшість несанкціонованих вторгнень, скояні зловмисниками, мають узгоджений та розподілений характер;
- найгірші наслідки несуть атаки на системи захисту інформації, що визначені в термінах та території й мають раптовий та випадковий характер;

- на розподілені атаки, як правило, не впливає силова протидія автономних термінальних вузлів мережі.

Перераховані фактори впливу на налагоджене функціонування інформаційних систем загального призначення аналогічно діють і на комп'ютерні мережі та системи підприємств. Проте, комп'ютерні мережі захисту підприємств принципово відрізняються побудовою, що спричинені специфікою комп'ютерних мереж та систем, які забезпечують чітку автоматизацію та роботизацію процесів підприємства. Найбільш впливова така відмінність – це фактор часу. Інформаційні системи та мережі мають бути релевантними та актуальними згідно сучасної ситуації. До того ж на підприємствах критичного застосування не можуть бути використані системи без врахування жорсткого реального часу.

Необхідно пам'ятати про такий важливий фактор впливу на комп'ютерну безпеку установи як наявність чи відсутність регіонально віддалених філій чи підрозділів. Тобто, якщо головне підприємство, зазвичай, має досконалу систему інформаційного захисту, то підрозділи з каналами обміну даними менше захищені (як за об'єктивними, так і за суб'єктивними причинами).

Однак, така територіальна віддаленість філій підприємства, що побудовані за одною схемою мережних сегментів, заснованою на ідентичних стандартах та протоколах, дає ряд різноманітних методів комплексного вдосконалення усіх вузлів та складових систем захисту. Неабияку роль грають заходи з організаційною роботою, на які треба звертати увагу.

Проведемо постановку основних завдань дипломної роботи, виходячи з вище перерахованих переконань:

Проаналізувати сучасний стан проблеми захисту комп'ютерної мережі підприємства та навести перелік незавершених завдань, щодо її вирішення.

Окреслити головні напрямки розробки складових системи захисту:

- мережний периметр вузлів та каналів передачі даних;
- брандмауери та маршрутизатори з фільтрацією пакетів;
- транслятори мережних адрес;

- транслятори адрес основних та альтернативних портів.

Провести розробку підсистеми захисту від розподілених мережних атак:

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

Запропонувати перелік рекомендацій щодо застосування систем силового, розподіленого захисту та псевдосервісів.

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

РОЗДІЛ 1

ПРОБЛЕМА ЗАХИСТУ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ

Особливість інформаційних та керуючих мереж підприємства відчутно відрізняються від особливостей інформаційних та керуючих мереж загального користування. Щоб точно пояснити цю особливість, основними характеристиками корпоративної мережі, дамо список термінів та визначень, які будуть використовуватися надалі. Джералами являються закони України, постанови органів державної влади, розробки науковців, дисертації тощо.

1.1. Терміни та визначення

Підприємства критичного призначення – це такі підприємства, які виконують наступні вимоги:

абсолютна захищеність протягом терміну експлуатації;

живучість, можливість працювати в несприятливих умовах хімічного, бактеріологічного або іншого забруднення, електромагнітного або радіаційного опромінення тощо;

спроможність виконувати свої функції у реальному часі, в найважчих умовах безперервно виконувати свої функції без затримок і збоїв.

До підприємств критичного призначення відносять ракетно-космічні комплекси, металургічної, хімічної, транспортної галузей, енергетичні (теплові, атомні електростанції) тощо.

Система реального часу – це система, яка повинна реагувати на події у зовнішньому по відношенню до системи середовищі або впливати на середовище в межах необхідних часових обмежень.

Кафедра КСМ				НАУ 21 05 98 000 ПЗ			
Виконав	Басок Б.О.			Проблема захисту корпоративної інформації	Літера	Аркуш	Архів
Керівник	Маларчук В.О.					11	56
Консульт.					123 КС-434Б		
Норм. контр.	Журавель С.В.						
Зав. Каф.	Жуков І.А.						

Система м'якого реального часу – затримка реакції вважається відновлювальною помилкою, яка може привести до збільшення вартості результатів і зниження продуктивності системи, але не є фатальною.

Приклад. Система не встигла опрацювати прийнятий пакет, це призводить до перерви на передавачу і повторній відправці (залежить від протоколу). При цьому дані не втрачаються і продуктивність не зменшується.

Система жорсткого реального часу не допускають жодних затримок реакції системи при будь яких умов, тому що:

можливі катастрофічні наслідки

в разі запізнення результати можуть бути даремні

у випадках в яких обробка події відбувається за більший ніж передбачено час, в даній системі вважається фатальною помилкою. Якщо така ситуація трапляється операція система має перервати дану операцію і блокувати її, щоб забезпечити надійність інших частин системи.

Головна різниця в системах жорсткого і м'якого реального часу така: система жорсткого реального часу не зволікає з реакцією на подію і виконує реакцію миттєво, тоді як система м'якого реального часу – має не спізнюватися з реакцією на подію.

Інформаційно-обчислювальні та управляючі корпоративні мережі – це комп'ютерні та телекомунікаційні, мережі всіх можливих різновидів. Як мають спільну властивість – такі мережі мають працювати в реальному часі. Для підприємств загального призначення може бути м'який 24 годинний реальний час, для підприємств критичного призначення обов'язково – жорсткий реальний час.

1.2. Основні принципи захисту комп'ютерних корпоративних мереж

Інформація це поняття яке дуже тісно пов'язане з комп'ютерними технологіями, системами зв'язку та мережами, зрозуміло, що питання захисту інформації в них стає надзвичайно важливим. Чесна конкуренція, базується на виконанні закону та норм моралі. Але часто буває, що підприємці в боротьбі

нехтують цими правилами намагаються отримати інформацію яка може нашкодити іншій стороні і використати її для досягнення власної вигоди. Недостатній контроль держави, недосконалість правоохоронної системи, змушує підприємців, виробництва та бізнес самостійно боротися з негативними процесами, щоб унеможливити витоку важливої конфіденційної інформації.

Існує багато причин посилення комп'ютерних злочинів які несуть за собою значні економічні, матеріальні та репутаційні втрати. Головними з них можна назвати:

- Поступова відмова від паперової технології передачі і збереження інформації і поступовий перехід на електронні носії, при цьому розвиток технологій захисту в таких носіях на даний момент недостатній;
- Реалізація глобальних мереж, та збільшення доступу до інформаційних ресурсів
- Підвищення складності програмних засобів.

У сучасному світі існує тенденція до збільшення випадків комп'ютерних злочинів. Виходячи з кількості загроз у сучасних мережах, реалізація захисту вимагає великий багаж знань та досвіду в багатьох вузькопрофільних дисциплінах. Поширеною загрозою є спеціальне використання небезпечного програмного коду (віруси, трояни, хробаки), а також атаки *DoS* (відмова в обслуговуванні) та *DdoS* (розподілена відмова в обслуговуванні).

Ключовими елементами забезпечення безпеки, які мають мати місце в створюваній інфраструктурі захисту: моніторинг; управління доступом; управління прогнозами; ведення контрольних журналів; управління конфіденційністю.

Ключове значення для захисту інформації в комп'ютерних мережах підприємства - це знаходження небезпечних атак та розробка систем виявлення та протидії атакам.

1.3. Класифікація та системи виявлення комп'ютерних атак

Неможливо уявити ефективний захист від мережесих атак без детальної класифікації, яка спрощує виявлення і протидію цим атакам. Зараз відносно велика кількість різних типів класифікаційних ознак. Як таких ознак може бути багато, поділяється на пасивні і активні, зовнішні і внутрішні атаки, свідомі й несвідомі тощо.

Класифікація комп'ютерних атак, яка застосовується у державних організаціях з захисту конфіденційної інформації:

- віддалене проникнення (англ. *remote penetration*) – атака яка реалізовує віддалене управління комп'ютером через мережу;
- локальне проникнення (англ. *local penetration*) – атака яка веде до несанкціонованого доступу до вузла;
- віддалена відмова в обслуговуванні (англ. *remote denial of service*) – такий тип порушує функціонування системи в рамках глобальної мережі;
- - локальна відмова в обслуговуванні (англ. *Local denial of service*) – тип атаки який, порушує функціонування системи в рамках локальної мережі.
- атаки з використанням мережесих сканерів (від англ. *Network scanners*) - засновані на використанні мережесих сканерів – такі програми визначають сервіси доступні для атаки;
- атаки з використанням сканерів вразливостей (від англ. *Vulnerability scanners*) - базуються на сканерах вразливостей - які здійснюють пошук вразливостей на вузлах, які далі будуть використані для атаки;
- атаки з використанням зломщиків паролів (від англ. *Password crackers*) - атаки, які базуються зломщиках паролів - програм, що підбирають паролі користувачів;

- атаки з використанням аналізаторів протоколів (від англ. *Sniffers*) - базуються на аналізаторах протоколів - прослуховуючих мережний трафік.

Класифікація яка буде на (рис. 1.1) являється закінченою і охоплює майже всі можливі дії потенційного зловмисника. Але для запобігання атакам і цього мало, бо використовуючи її в такому виді не дає можливості визначати елементи мережі, на які може бути здійснена та чи інша атака, а також те до чого може призвести успішна атака. А це означає що з побудови – моделі загроз безпеки, має починатися організація захисту інформації в корпоративній мережі.

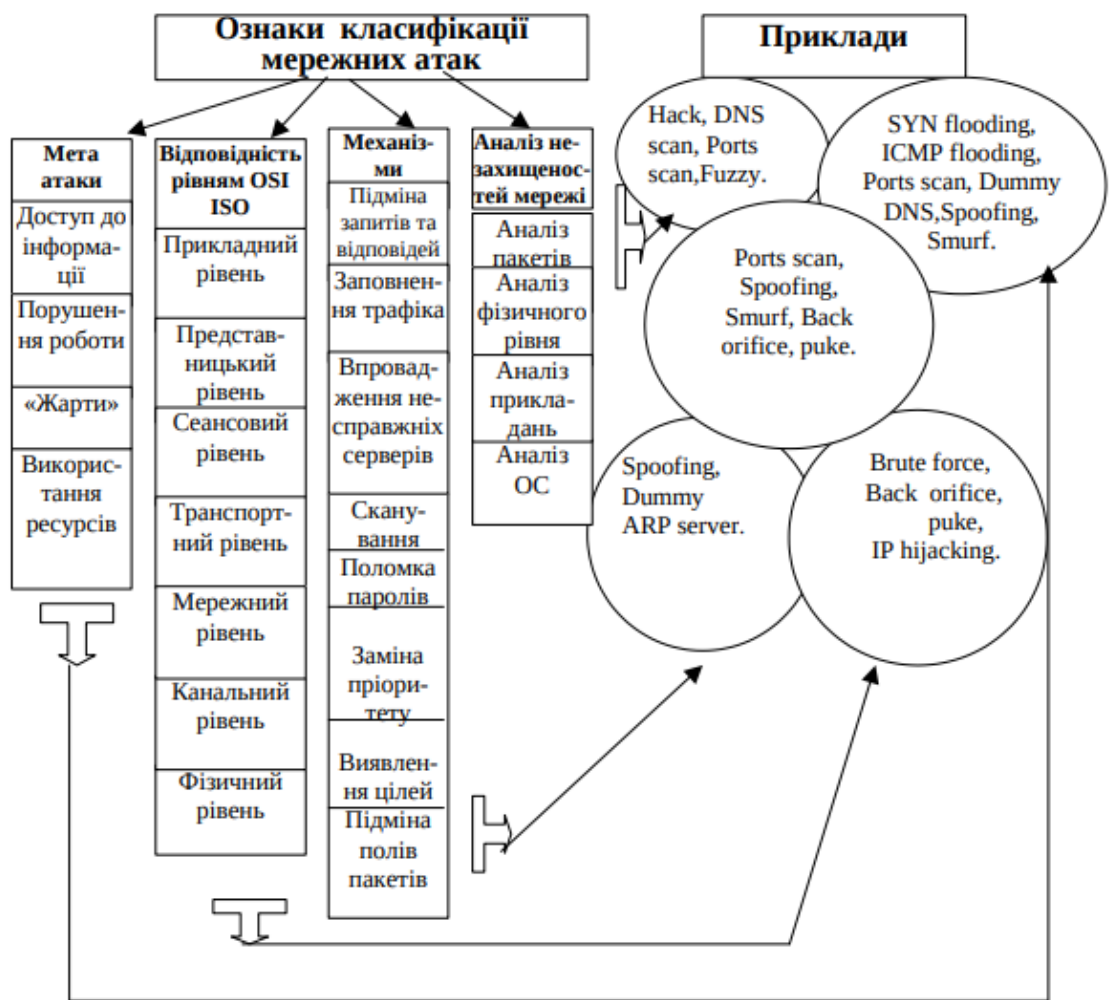


Рис. 1.1.Класифікація атак різних рівнів

Можливими загрозами для корпоративної мережі можна віднести також.

Аналіз трафіку являється методом отримання паролів та інших персональних даних куористувачів мережі. Аналіз роблять спеціалізовані

аналізатори - (*sniffer*), вони перехоплюють всі пакети, і визначають саме ті пакети як передають паролі та важливі персональні дані.

На даний момент досі використовуються протоколи в яких данні передаються в нешифровані(незахищені). Аналіз трафіку дає можливість перехопити дані, які найчастіше передаються протоколами *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*). Також часто перехоплюють паролі до пошт, номери кредитних карток, та іншої конфіденційної інформації.

Зараз існують протоколи, які дають змогу захищати мережу та шифрувати трафік. Але на даний момент такі протоколи не стали стандартними і не використовуються кожним користувачем. Заважає їх поширенню заборона на експорт сильної криптографії, яка діє в деяких країнах. Саме з таких причин впровадження цих протоколів в програмне забезпечення не відбувається, або відбувається не в повній мірі, що робить дані протоколи майже марними, оскільки шифри можуть бути розкриті за відносно не великий час.

Аналіз трафіку дає наступні можливості:

- зрозуміти принципи роботи обчислювальної системи, одержати однозначну відповідність подій і команд які відбуваються в системі. Такий результат досягається перехопленням і аналізом пакетів на каналному рівні. Розуміння принципу роботи дає змогу на практиці моделювати типові атаки.

- аналіз мережевого трафіку дає можливість перехопити потік даних, якими обмінюються об'єкти розподіленої ВС. Отже така атака заключається в отриманні доступу до інформації, якою об'єднуються абоненти. Можливість модифікувати трафік в такому випадку повністю відсутня, а аналіз можливий лише в середині одного сегменту. Найчастіше такою типологією перехоплюють ім'я та пароль користувача, якщо він передавався незахищеною мережею.

Аналіз мереженого трафіку - це пасивний вплив на мережу. Виконання такої атаки веде за собою порушення конфіденційності інформації всередині одного сегмента мережі на канальному рівні моделі *OSI*.

Проблемою безпеки мережі виступає також недостатня ідентифікація та аутентифікація віддалених об'єктів.

Головна проблема в виконанні однозначної ідентифікації повідомлень, що були передані об'єктами та суб'єктами взаємодії. Часто в розподілених ЗС данна проблема виконується наступним чином: під час розробки віртуального каналу об'єкти РВС обмінюються деякою інформацією, данна інформація ідентифікує канал. Називається даний обмін "рукостисканням" (*handshake*). Але не завжди для зв'язку розробляється окремий канал. Часто на практиці використовують відправку одиночних повідомлень без підтверджень.

Для адресації повідомлень в розподілених ЗС використовують мережеву адресу. Данна адреса унікальна для кожного об'єкта. Також таку адресу використовують для ідентифікації об'єктів обчислювальної системи. Але така адреса просто підробляється, а отже використовувати лише її для захисту не можна.

На рис. 1.2 зображені розповсюджені підходи до побудови систем виявлення атак

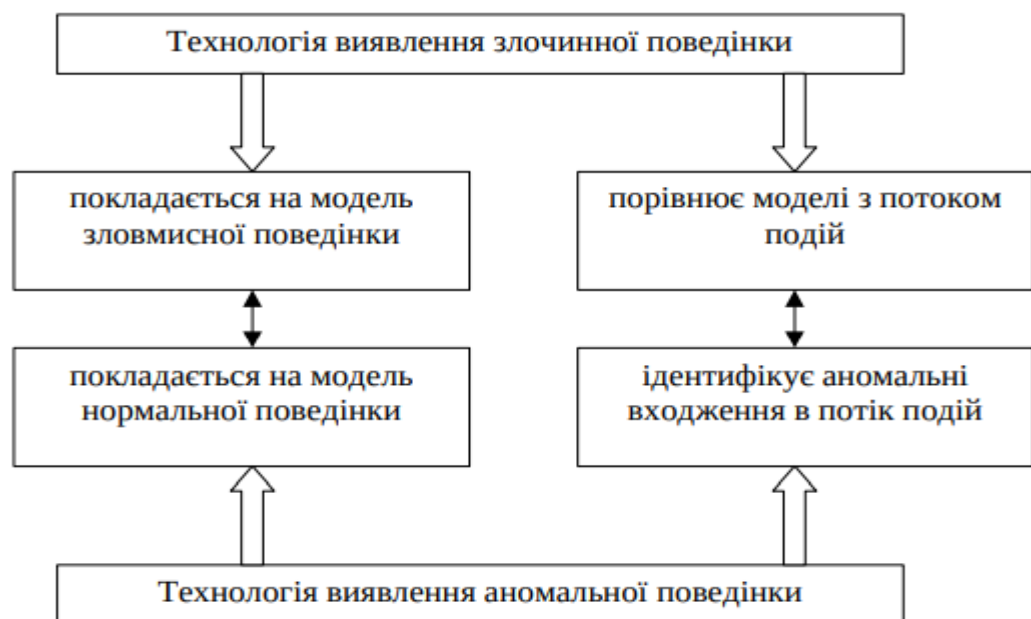


Рис. 1.2. Розповсюджені підходи до побудови системи виявлення атак

Коли будується система захисту корпоративної мережі завжди слід пам'ятати про наступні фактори:

- атаки на мережу бувають максимально різні;
- переважна більшість атак мають узгоджений характер;
- найнебезпечніші для системи захисту випадкові атаки;
- силова протидія автономним атакам в більшості випадків буде безрезультатною.

Данні фактори мають однаковий вплив і на мережі загального призначення і на корпоративні мережі. Проте система захисту комп'ютерної мережі підприємства має деякі принципові відмінності, які виходять з особливості систем які забезпечують роботу корпоративної мережі. Найбільша відмінність – час. Корпоративні мережі мають бути захищені системою реального часу. А на підприємствах критичної інфраструктури використовують лише системи жорсткого часу.

Ключовим в питанні інформаційної безпеки являється наявність або відсутність віддалених філій та підрозділів. Оскільки головне підприємство часто має кращу систему захисту інформації, а регіональні підрозділи як правило захищенні гірше. Але коли підрозділи і філії мають схожу архітектуру, це дає можливість удосконалити систему захисту. Важливе місце в цьому питанні мають організаційні заходи, на них має бути особлива увага.

Системи виявлення вторгнень (*IDS*) стрімко стали головними в будь-якій стратегії мережевого захисту. Останім часом вони набирають все більшої популярності, бо виробники покращують якість своїх продуктів. Аналіз – головна система виявлення несанкціонованих вторгнень. Під час аналізу перевіряється кожен пакет і визначається чи шкідливий він. Якщо пакет виявляється шкідливим оголошується тривога, це і є головною задачею *IDS*. Зараз є різні методи *IDS*. Кожен має як свої переваги, так і недоліки.

Основні поняття систем виявлення вторгнень (*IDS*). Такі пристрої, перевіряють як вхідний так і вихідний мережевий трафік. На відмінно від *firewall* вони не змінюють потік трафіку, а шукають недобросовісний трафік,

який може означати можливий напад або неправомірне використання, і оголошують тривогу для системного адміністратора.

Другий метод аналізу розглядає данні та трафік мережі, протоколи. Кожен пакет йде з протоколом. IDS розглядає ці протоколи згідно *RFC*. Кожен протокол має очікуване значення, якщо воно відрізняється ймовірно вторгнення.

IDS проглядає кожне поле всіх протоколів вхідних пакетів: *IP*, *TCP*, і *UDP*. Якщо є порушення протоколу, оголошується тривога. Спочатку *IDS* було дуже просто обійти. Але зараз це змінилось в кращу сторону. Аналіз протоколу дуже відрізняється від аналізу підпису, який використовує відомі характеристики атак для оголошення тривоги.

У системи аналізу сигнатури є кілька сильних сторін. Швидкість, коли повний аналіз пакету - досить важка задача. Правила легко написати, зрозуміти і налаштувати. Є підтримка для швидкого виробництва сигнатур для невідомих небезпек. Такі системи кращі за інші на первинному етапі. Аналіз, який базується на сигнатурі, швидко повідомляє якщо в системі все працює коректно, для оголошення тривоги має відбутися якась соблива подія. *IDS*, яка базується лише на аналізі сигнатур, має свої слабкі сторони. З часом швидкість роботи знижується. Це велика проблема, адже число сигнатур які перевіряються можуть рости дуже швидко. Кожна атака збільшує кількість сигнатур які перевіряються. Це сильно впливає на швидкодію.

У аналіза протоколів в свою чергу також є сильні та слабкі сторони, але вони відрізняються. Аналіз протоколів часто буває дуже повільним. Правила для перевірки важкі для написання і розуміння. Доводиться покладатися на виробника, оскільки вони важкі для самостійного налаштування. Зараз правила стають все складнішими і часто ігнорують загальні стандарти, протоколи і *RFC*, що створює додаткову проблему розробникам *IDS* і дає шанс для зловмисника.

IDS на основі аналізу протоколу працюють повільніше, ніж системи на основі сигнатури, вони більш «грунтовні» в сенсі масштабності і результатів. На жаль, такі системи іноді пропускають, 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. Два методи виявлення вторгнення - аналіз сигнатур і аналіз протоколу, справді різні, але якщо вивчити проблеми детальніше то можна побачити певну їх схожість. Ці інструменти досліджують дані про атаки і аномалії.

Обидва розглянутих методи, є детермінованими. Їх слабкість, в уповільненні з ростом числа можливих загроз, та в неможливості виявлення вперше створених нових загроз. Альтернативою таким методам виступають статичні методи з байєсівськи, мінімаксним підходами та методу максимальної правдоподібності. Використання цих методів найбільш поширений вид реалізації технології виявлення аномальної поведінки. Статистичні сенсори збирають різну інформацію про типову поведінку об'єкта і формують її у вигляді профілю.

Профіль - це набір параметрів які описують типову поведінку об'єкта. Він формується на основі статистики об'єкта, і для цього можуть застосовуватися стандартні методи математичної статистики.

Висновки до розділу

Розглянуто проблему захисту корпоративної інформації.

Проаналізовано інформаційно-обчислювальні та управляючі мережі підприємства – це комп'ютерні та телекомунікаційні, проводові або безпроводові мережі будь-яких різновидів. Вони мають спільну властивість – мережі мають працювати у реальному часі. Підприємств загального застосування можуть працювати в м'якому реальному часі, підприємства критичного призначення – лише жорсткий реальний час.

Розглянуто основні принципи захисту комп'ютерних корпоративних мереж

Розглянута класифікація комп'ютерних атак і систем їх виявлення. Створити ефективний захист від потенційних мережових атак неможливо без їх детального класифікації, що полегшує їх виявлення і створення протидії їм. В даний час велика кількість різних типів класифікаційних ознак.

РОЗДІЛ 2

МЕРЕЖЕВИЙ ПЕРИМЕТР КОМП'ЮТЕРНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ ТА ЙОГО ЗАХИСТ

2.1. Основні принципи захисту мережевого периметру

Мережевий периметр - це укріплена границя корпоративної мережі, що може включати: маршрутизатори; брандмауери; проксі-сервери; систему виявлення вторгнень; пристрої віртуальних приватних мереж; засоби антивірусного захисту; демілітаризовану зону (DMZ) і екрановані підмережі.

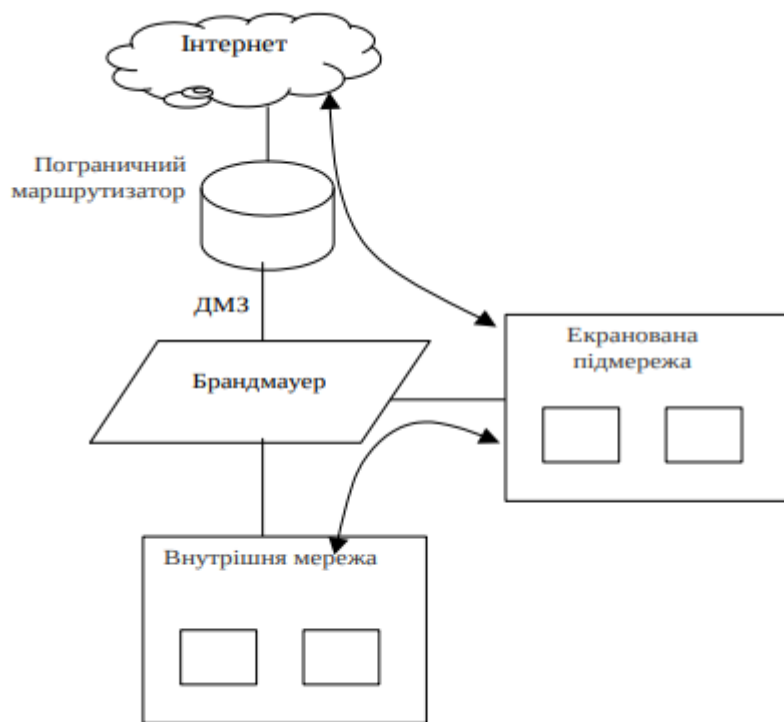


Рис. 2.1. Компоненти захисту мережевого периметра

Кафедра КСМ				НАУ 21 05 98 000 ПЗ			
Виконав	Басок Б.О.			Мережевий периметр комп'ютерної корпоративної мережі та його захист	Літера	Аркуш	Аркушів
Керівник	Маларчук В.О.					21	56
Консульт.					123 КС-434Б		
Норм. контр.	Журавель С.В.						
Зав. Каф.	Жуков І.А.						

Маршрутизатори – це пристрої, які здійснюють керування трафіком, що надходить у мережу, що виходить із мережі, або трафіком усередині самої мережі. Прикордонний маршрутизатор є останнім маршрутизатором, що контролює безпосередньо вхід/вихід в Інтернет.

Брандмауер, або міжмережевий екран, являє собою пристрій, що аналізує трафік з використанням набору правил, які дозволяють визначити, чи можна передавати цей трафік по мережі. Область дії брандмауера починається там, де закінчується область дії прикордонного маршрутизатора й він виконує набагато більш ретельну перевірку пакетів при фільтрації трафіку.

Проксі-сервер – це проміжний комп'ютер, який є посередником між комп'ютером (або мережею комп'ютерів) та *Internet*.

Система виявлення вторгнень - це система, що використовується для виявлення й повідомлення про всі вторгнення й потенційно небезпечні події у корпоративній мережі.

Під терміном демілітаризована зона мають на увазі невелику мережу, що містить ресурси загального користування, підключені безпосередньо до брандмауера або іншого фільтруючого пристрою, які й захищають її від вторгнень.

Екранована підмережа являє собою ізольовану мережу, з'єднану з певним інтерфейсом брандмауера або іншим фільтруючим трафік пристроєм.

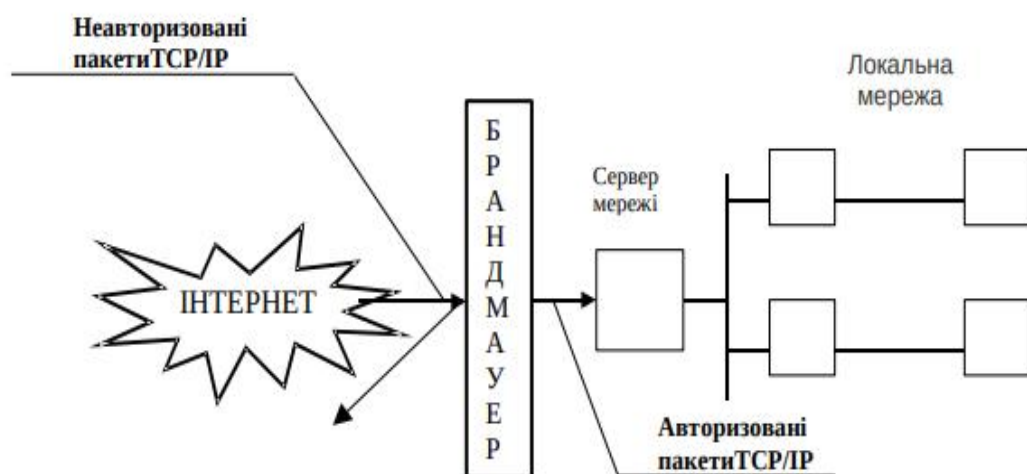


Рис. 2.2. Умовна схема розміщення та функціонування брандмауера

Роль брандмауера часто виконують маршрутизатори. Авжеж система брандмауера створюється на основі маршрутизаторів, які з'єднують мережу з Інтернетом, але може бути створена і на інших маршрутизаторах, для захисту тільки частини хостів чи підмереж.

Сучасні брандмауери умовно можна поділити на три категорії, хоча кожна з них сильно відрізняється один від одної, проте більшість можемо віднести до наступних категорій:

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

Проксі-брандмауер - це спеціалізована програма, яка забезпечує зв'язок між внутрішніми захищеними мережами й зовнішнім світом за допомогою інтернет-протоколів. Загалом кажучи, проксі працюють із програмами, заснованими на протоколі *TCP/IP*. Зазвичай проксі-сервери запускають кілька програм, які є захищеними. Це спеціалізовані програми, і кожний підтримуваний ними протокол повинен мати власну службу проксі або оброблятися загальним проксі. Проксі може бути також і прозорою програмою, що створюється для передачі пакетів у будь-який даний порт через кордони мережі.

Проксі діє по команді клієнта або користувача для доступу до послуг мережі й захищає кожну сторону від прямого рівноправного з'єднання. Клієнти встановлюють з'єднання, виконуючи три стадії організації з'єднання із проксі-сервером. Після цього проксі встановлює з'єднання з віддаленим сервером. Проксі-сервер висилає дані, які надійшли до нього від клієнта, на запрошуваний сервер, а також пересилає дані, отримані від цього сервера, клієнтові. В принципі, проксі-сервер є як сервером, так і клієнтом. Він є сервером відносно свого клієнта й клієнтом відносно запрошеного сервера. Етапи організації з'єднання через проксі вимагають різні рівні автентифікацій або довіри програмному забезпеченню, що буде використано для установки з'єднань.

Звичайно проксі-сервер працює на двосторонньому бар'єрному хості або шлюзі й підтримує кілька Інтернет-протоколів. Бар'єрними, або бастіонними, хостами є укріплені системи, сконфігуровані для роботи з Інтернетом.

Двосторонній шлюз складається з хост-системи із двома мережевими інтерфейсами: один інтерфейс для внутрішньої захищеної мережі й один для зовнішньої мережі. Ці хости забороняють прямий трафік між мережами й можуть використовуватися для функцій реєстрації й аудиту трафіку, який через них проходить. Хост не виконує маршрутизацію пакетів між двома з'єднаними мережами, оскільки перенаправлення IP пакетів неможливо. Двосторонній шлюз повністю блокує IP-трафік між зовнішньою й внутрішньою мережею. Проксі-сервери в шлюзі забезпечують служби й можливість з'єднання з Інтернетом. Щоб уникнути випадкового пересилання IP-трафіка може виявитися дуже корисним явна заборона можливості перенаправлення IP-пакетів.

У порівнянні з іншими типами брандмауерів, проксі-брандмауери володіють цілим рядом переваг. Внутрішні IP-адреси захищені від зовнішнього світу завдяки тому, що проксі-служби не допускають прямих з'єднань між зовнішніми серверами та внутрішніми комп'ютерами. Адміністратори мають можливість робити моніторинг порушень політики безпеки брандмауера, використовуючи для цього записи аудиту, які генеруються службами проксі. Використання проксі-брандмауерів дозволяє організувати захист, заснований на користувачах. Служби проксі ефективні при захисті від неавторизованого використання на однокористувацькій основі й здатні підтримувати строгу автентифікацію.

Проксі-брандмауери мають кращі можливості реєстрації, ніж брандмауери фільтрації й маршрутизації, і пропонують єдину точку для аудиту й керування. Користувачі не можуть увійти в проксі-сервери. У бастіонних хостах не потрібні жодні облікові записи. Проксі-служби працюють по команді користувачів. Проксі-сервер забезпечує централізовану точку для мережі, і спостереження за трафіком може виконуватися дуже ретельно. Однак, це може створити вузькі місця мережевого трафіку. Топологія внутрішньої захищеної мережі в проксі-брандмауерах є прихованою. Деякі проксі пропонують поліпшені засоби виконання аудиту, маючи інструменти для моніторингу трафіка. Проксі-брандмауери мають менш складні правила фільтрації, ніж брандмауери пакетних фільтрів. Правила в маршрутизаторі пакетної фільтрації менш складні,

ніж якщо маршрутизатору необхідно було відфільтровувати прикладний трафік і пересилати його декільком визначеним системам. Маршрутизатору необхідно дозволити тільки прикладний трафік, що направляється шлюзу прикладного рівня, а весь інший видалити.

Незважаючи на те, що проксі-брандмауери пропонують більш високий рівень безпеки в порівнянні із брандмауерами пакетної фільтрації, проте вони мають деякі недоліки. До них можна віднести наступне. Зниження продуктивності внаслідок додаткових запитів на обробку, необхідних для прикладних служб. Прикладні проксі працюють повільніше в порівнянні з пакетними фільтрами. Для кожної нової програми або протоколу, які необхідно пропустити через брандмауер, необхідно розробляти новий проксі. Доступним є лише обмежена кількість служб. Доступ до інших, непередставлених проксі-служб, залишається неможливим. Невід'ємні проблеми в операційних системах і їхніх компонентах можуть негативно вплинути на безпеку сервера брандмауера (firewall server). Проксі-служби уразливі перед помилками в операційних системах і помилками на прикладному рівні. Операційна система хоста, що містить проксі, залишається незахищеною перед зовнішніми погрозами й може бути атакована. Процес установки проксі-служби може виявитися досить складним для кожної програми, що використовує шлюз. Оскільки проксі-сервер може виявитися вузьким місцем у мережі, він може стати також і єдиною точкою збою.

Брандмауери експертного рівня забезпечують найвищий рівень захисту та високі параметри продуктивності. В ідеальному випадку брандмауер повинен бути прозорим (непомітним) для клієнтів мережі. На практиці вимогу щодо прозорості брандмауера так чи інакше порушують. 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 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)

Бачимо динамічні списки доступу, які формуються вихідними з'єднанням які мають таку ж функціональність, як таблиця стану, вони відслідковують інформацію про поточні сеанси зв'язку, щоб дозволити успішне проходження зворотного трафіка через маршрутизатор. Кожен запис починається з ключового слова *Permit*. Потім інформація про стан сеансу. Підтримується як *TCP*, так і *UDP*. Після протоколу адреса і порт призначення. Потім виводиться число відповідностей визначеному правилу, а тоді – час, після закінчення якого відбувається автоматичне видалення динамічно розміщеного списку.

Брандмауер з фільтрацією пакетів є найпоширенішим і найпростішим при реалізації для маленьких мереж із простою структурою. Проте він має ряд недоліків і менш бажаний, ніж інші приклади брандмауерів. Як правило, брандмауер з фільтрацією пакетів встановлюється на маршрутизаторі з фільтрацією пакетів, через який відбувається з'єднання з Інтернет (або підмережею), на якому конфігуруються правила фільтрації пакетів, що дозволяє

блокувати або фільтрувати пакети на підставі протоколів і адрес. Звичайно, з машин внутрішньої мережі надається повний доступ до Інтернету, а доступ з боку Інтернету до всіх або майже до всіх систем внутрішньої мережі блокується. Проте за допомогою маршрутизатора можна допускати вибірковий доступ до систем і сервісів.

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 розуміння безпеки це правило звичайно вказує на необхідність відкидання всіх пакетів, що не задовольняють жодному з інших правил.

2.2. Системи виявлення вторгень

Системи виявлення вторгень (*IDS – intrusion detection system*) відрізняються від традиційних міжмережних екранів, вони створені для виявлення недоліків у системі безпеки – несанкціонованого використання, атак на вузли, мережі та телекомунікаційні інфраструктури. *IDS* дозволяють зменшити збиток від атак кіберзлочинців, злому критичних вузлів і мережних пристроїв [3].

Основна задача *IDS* – помічати підозрілі дії в мережі і своєчасно повідомляти про них адміністратора (за допомогою подачі звукового сигналу, передачі повідомлення на консоль управління, відправлення *SMS*-повідомлення на мобільний телефон і т.п.), або навіть автоматично вносити зміни в налаштування *ACL* міжмережного екрану. Засоби *IDS* можуть переглядати потоки даних, знаходячи в них послідовності бітів, які можуть свідчити про сумнівні дії або події, або здійснювати моніторинг системних журналів і інших файлів стеження. Потрібно виявляти будь-яку ненормальну поведінку, яка може

свідчити про вторгнення. Існують різні різновиди *IDS*, але всі вони мають три загальних компоненти:

- Сенсори;
- Аналізатори;
- Адміністративні інтерфейси.

Сенсори збирають трафік або дані про дії користувачів, і відправляють їх аналізаторам, які шукають в них підозрілі дії. У разі виявлення аналізатором таких дій (на які він запрограмований), він відправляє відповідні повідомлення на адміністративний інтерфейс.

Існує два основних типи *IDS*:

- на рівні мережі (*network-based*), які відстежують весь мережний трафік;
- на рівні вузла (*host-based*), які аналізують дії в рамках однієї комп'ютерної системи [4].

IDS можуть бути налаштовані для виявлення атак, аналізу журналів аудиту, переривання з'єднань, повідомлення адміністратора про атаки, що відбуваються, для захисту системних файлів, вказівки на уразливості, які повинні бути враховані, а також, щоб допомогти слідкувати за діями окремих злоумисників. Сучасна *IDS* алючає в себе не один механізм виявлення: сигнатурний пошук, пошук регулярних виразів і статистичний механізм розпізнавання вторгнень. Але 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.

Сенсор системи виявлення атак - це підсистема, яка отримує 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.

Можливі атаки на сенсор розглянуто на рис. 2.3.

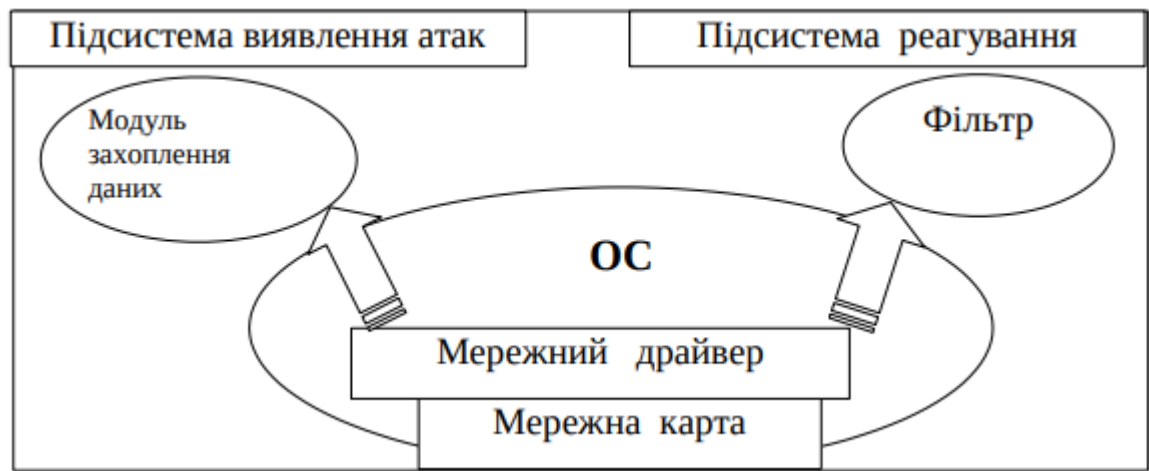


Рис. 2.3. Схема атаки на сенсор

1. Мережева карта. Компонент який використовується – отримання 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), і 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. Вразливість сучасних ОС, робить атаки на *IDS* більш ніж реальними.

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 мають забезпечувати безпеку, хоча можуть бути використані і зловмисниками. Якщо зловмисник має інформацію коли сенсор розриває з'єднання з вузлом, тоді може бути реалізована атака в адресі якої вказана будь-якого з компонентів *IDS*. Отже *IDS* може бути засобом організації атаки. Також для вторгнень може бути використаний механізм аутентифікації. Достатньо видалити ключ одного з компонентів *IDS* і процес аутентифікації вже не пройде. Компоненти не зможуть обмінюватися інформацією. А якщо це не потрібно то зловмисник може створити додатковий сенсор який може вводити в оману.

Для покращення захисту 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).

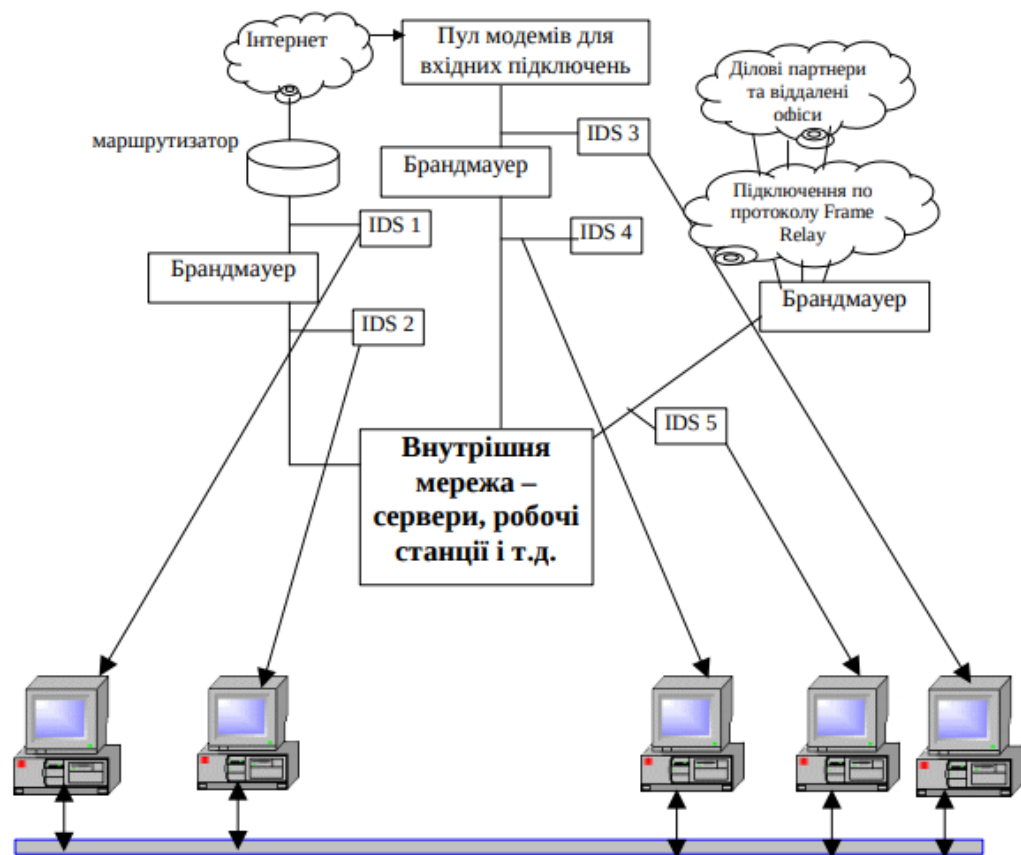


Рис. 2.4. Система виявлення вторгнень

В наведеній моделі всі мережеві сканери мають дві і більше мережних інформаційних карти (*NIC*). Функція мережових інформаційних карт – перегляд трафіку мережі яка перевіряється. Такі карти не створюють трафік. Натомість остання карта підключається до окремої мережі керування, і використовується лише для передачі даних системі виявлення вторгнень.

Таке рішення робить важчою задачу знаходження і ідентифікації сенсора для зловмисника, бо він не буде відповідати на запити які направлені коентролюючій мережних карти. Отже зловмисники не зможуть досягти ізолювану карту. Також деякі карти є справжніми мережними аналізаторами і не використовують IP-адресу. Коли сенсор використовує IP-адресу, та за умови що вона відома зловмиснику, він може використати її, і запустити проти нього атаку, щоб викликати збої та відмови.

Побудова окремої мережі має різні переваги. Така мережа ізолює трафік так, щоб ніхто хто не керує цією мережею не бачив зв'язків сенсорів. Таке рішення дозволяє контролювати власний трафік. Окрема мережа це хороша

можливість для уникнення можливих проблем таких як проходження даних сенсорів через брандмауери та нешифровані мережі.

Надзвичайно важливим є зміцнення безпеки сенсорів системи виявлення вторгнення, щоб знизити небезпеку компрометації. Якщо зломисникам вдається отримати доступ до керування системою виявлення вторгнень то вони можуть її відключити або конфігурувати її так, що вона не буде виявляти їх дії і попереджувати про них. Зломисники 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. Система проактивного захисту інформації в комп'ютерній корпоративній мережі

Проактивний захит направлений не на усунення, а на попередження помилок. Цпрактивний захист – це сукупність заходів, які мають гарантувати стабільну роботу мержі з урахуванням системи безпеки.

Сім базових принципів проактивної проактивні системи:

- Зв'язок з фізичним світом;
- Стійкі мережні взаємодії;
- Макрообробка;
- Функціонування в умовах невизначеності;
- Передбачення;
- Замкнутий цикл керування;
- Персоніфікація.

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

Погрози конфіденційності, цілісності і доступності інтерфейсів, протоколів і послуг є найбільш узагальненим видом погроз, і універсальність проєктованих систем захисту може бути заснована саме на цій не конкретній, а

узагальненій погрозі. Подібним системам не важливо які саме атаки будуть на систему, адже вони заздалегіть будуть неефективні.

Всі протоколи мають певні свої особливості, але всі вони повинні забезпечувати взаємодію не менше двох об'єктів (це і є головною різницею від алгоритму – послідовності операцій, яка веде до виконання поставленої задачі з досить великого класу однотипних задач, але без взаємодії). Для всіх протоколів загальним буде призначення – забезпечення взаємодії, і агент безпеки цьому випадку відповідальний за конфіденційність, цілісність і доступність цієї взаємодії. Багато існує і інтерфейсів, вони виглядають правила доступу до послуг. Загальним для них буде забезпечення конфіденційності, цілісності і доступності 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 та використання, від підміни, ушкодження або знищення.

За основу підсистеми безпеки потрібно вибрати агентну технологію. Кожен агент повинен 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 маємо на увазі, що володіє здатністю до формулювання цілей, навчання, 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, відрізняється від традиційних програм, може не лише взаємодіяти з цим середовищем, одержуючи від нього інформацію через свої сенсори, впливаючи на середовище за допомогою своїх ефекторів, а також змінювати своє поведіння, навчаючись на власному досвіді.

Особливості побудови пропонованої системи безпеки:

1. Деякі з елементів такої системи вже існують. Це доводять приклади систем безпеки, наведені в першій частині розділу. Проактивний захист системи використовують, для прикладу, у банківській справі – при банківських переведеннях через телекомунікаційні мережі загального призначення (Internet).

2. Данна система має обов'язково бути розподіленою, отже реалізовувати інформаційну технологію на основі розподілу ресурсів. Така обчислювальна система може включати дані, засоби обробки даних та активні компоненти. Оброблювальні дані є інформаційними ресурсами розподіленої обчислювальної системи. Політика безпеки – це ниска правил, які стежать за порядком обробки інформації, взаємодії підсистем і забезпечення системи захисту. Велика розподіленість системи призводить до зниження стійкості системи та збільшенню кількості загроз.

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.



Рис. 2.5. Підсистема захисту розподіленої обчислювальної системи

Архітектура яка була розглянута - це нове рішення в інформаційних технологіях і може вирішити проблеми балансу функціональних систем та задач які дозволяють постійне їх виконання. Характеристики даних систем дадуть можливість значно спростити і покращити керування навіть для слабоструктурованих систем, разом з тим зменшуючи необхідний для безпеки трафік.

Висновок до розділу

Під час роботи над розділом було розібрано головні принципи захисту мережевого периметра корпоративної мережі, а також захисту периметру.

Був проведений аналіз динамічної фільтрації та динамічного списку доступу. Проблеми з якими може зустрітися пакетна фільтрація, вирішуються динамічної пакетної фільтрацією. Суть її в тому, що фільтри створюються «миттєво» в момент необхідності та зупиняють роботу коли з'єднання буде розірване. Прикладом динамічної фільтрації виступають рефлексивні списки доступу. Визначення типів з'єднань відбувається на підставі встановлених в зовнішньому інтерфейсі критеріїв. Коли трафік повертається його порівнюють зі списком доступу, який був динамічно створений відразу після того, як трафік вийшов з мережі.

Розподілена система виявлення вторгнень (*intrusion detection system – IDS*) моніторить мережевий трафік та маніпуляції з файлами хоста для того, щоб установити факти нетипового поведіння чи некоректного використання. Також *IDS* веде журнал вторгнень, розсилає попередження в режимі реального часу і, інколи її вдається зупинити атаку.

Проактивний сервіс направлений не на усунення, а на попередження несправностей. Проактивний сервіс - це сукупність стратегічних заходів, які мають організувати оптимальну і безперебійну роботу мережі враховуючи політику безпеки.

РОЗДІЛ 3

РОЗПОДІЛЕНІ АТАКИ НА КОМП'ЮТЕРНУ КОРПОРАТИВНУ МЕРЕЖУ ТА ЇЇ ЗАХИСТ

Атака на введення коду на основі хоста – цей метод використовують програми для прихованої цільової атаки на систему. Даний метод дає змогу небезпечним програмам виконувати свій код у зовнішньому процесовому просторі, а це в свою чергу дає можливість робити це таємно і отримати доступ до секретної інформації інших процесів. Існує дуже багато способів вводу та виконання коду, а це означає що необхідний загальний підхід, який структурував би всі з цих підходів. Недостатньо лише підходів які фокусуються лише на ОС низького рівня, адже набір *API* весь час збільшується. Це означає, що підходи які орієнтуються на деталі ОС низького рівня, більше піддаються втраті нових атак. Такі підходи обмежуються лише знанням однієї операційної системи.

Роблячи висновки з результату аналізу багатьох статей, матеріалів, наукових робіт, монографічних матеріалів, питання захисту інформації завжди буде актуальним. На сьогоднішній день відомо кілька тисяч загроз для інформаційних систем. Найдетальнішим описом являється відкритий стандарт Європейського Союзу *IT Baseline Protection Manual* обсягом більше чотирьох тисяч сторінок[8]. Організація безпеки даних - не тільки систематизація, виявлення і відображення загроз, головне - управління ризиками, вчати і правильні дії для зниження ризику загроз, щоденна робота по системному забезпеченню безпеки [2]. Щоб вирішити дану проблему вже недостатньо виявляти і реагувати на дії порушників. Потрібно знаходити і виключати уразливі місця системи.

Кафедра КСМ				НАУ 21 05 98 000 ПЗ			
Виконав	Басок Б.О.			Розподілені атаки на комп'ютерну корпоративну мережу та її захист	Літера	Аркуш	Аркушів
Керівник	Малярчук В.О.					36	56
Консульт.					123 КС-434Б		
Норм. контр.	Журавель С.В.						
Зав. Каф.	Жуков І.А.						

Вже давно з'явилося розуміння того, що боротьба з шкідливим мережевим впливом не дає бажаного результату. Цілком логічно було застосовувати методи які відносяться до системного аналізу, радіоелектроніки, радіорозвідки, військової справи, дезінформації тощо.

Сучасним підходом для виявлення атак на введення коду став - *Bee Master*[9]. Він застосовує парадигму honeypot до процесів обчислювальних систем і тим самим не спирається на деталі низького рівня. Суть роботи полягає в тому, щоб виявляти регулярні процесори обчислювальних систем як «приманку» для шкідливих програм. Заснований такий підхід на концепціях, таких як потоки або сторінки пам'яті, які мають місце в сучасних операційних системах. Отже *Bee Master* не страждає від недоліків низькорівневих підходів до обчислювальних систем.

Також використання такого підходу дає змогу незалежно виявляти напад на введення коду на основі хоста. Для перевірки можливостей даного підходу, були отримані якісні і кількісні оцінки *Bee Master* на *Microsoft Windows* і *Linux*.

Метою моєї дипломної роботи – є вивчення методів управління процесом захисту інформаційної системи на основі теорії конфлікту і керованих марківських процесів. З отриманих результатів створити алгоритми та вивчити методи протидії злочинцям використовуючи «медову пастку» і *Bee Master*.

не потрібно розглядати конфлікт як оптимізаційне питання. При однакових ресурсах оптимальним буде завершення конфлікту, при не рівних швидше за все – поразка слабшої з сторін. Але все ж таки в конфлікті можна виграти і меншими силами. Але для такого результату обов'язково мають бути ресурси такі як в атакуючої сторони.

З сильним суперником конфлікт не вирішується теорією адаптації. Активними діями такий суперник з високою ймовірністю досягне перемоги. В той час ми, адаптуючись до погіршення умов, опиняємось в не вигідній ситуації.

Головні завдання які потрібно виконати:

- Вибір найперспективніших стратегій для можливого конфлікту;
- вибір математичного апарату для опису процесів розвитку конфлікту;

- розробка математичної моделі конфлікту для отримання асимптотичних характеристик ефективності.

3.1. Технологія Honeypot

Технологія *Honeypot* (медова пастка) — це ресурс, який виступає приманкою для зловмисників. Мета медової пастки — зазнати атаки або несанкціонованого дослідження, пізніше це дасть змогу дослідити стратегію зловмисника та визначити перелік засобів, за допомогою яких можуть бути завдані удари реально наявним об'єктам безпеки. *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. Медова пастка може імітувати будь-які потенційні для атак системи.

Переваги медової пастки закладені в принципі роботи даної технології. Головною перевагою є майже повна відсутність помилкових спрацювань. Медова пастка лише імітує роботу системи, звернутися до неї не можуть звичайні користувачі. Якщо на *Honeypot* надходить звернення - воно точно є несанкціонованим, і з впевненістю можна говорити про атаку на систему.

Вчасна фіксація атаки головна задача адміністраторів, це дає змогу ментально розпочати заходи для протидії атаці. Також дана технологія дає можливість опрацьовувати інформацію про порушника, структурувати його дії. *Honeypot* має можливість зберегти інформацію, а це в свою чергу дозволяє проводити розслідування. Систему на яку була зроблена атака відключають і перають спеціалістам для детального аналізу, а для реальної системи таку дію зробити неможливо.

Використовуючи дані зловмисника можна визначити методи та засоби атаки які він використовував. Для технології *Honeypot* потрібна відносно невелика кількість інформації яку потрібно вивчати під час розслідування. Для розслідування атаки на реальну систему потрібно враховувати величезну

кількість інформації, це є досить трудомісткою задачею. В свою чергу медова пастка містить лише основну інформацію яка має відношення до фактів, оскільки легальна діяльність не мала місця.

3.2. Система безпеки промислового підприємства та місце технології Honeypot в системі

Технологія Honeypot доступни та достатньо ефективий метод попередження і виявлення вторгнень. Виділяється два головних напрямки роботи технології:

- Зниження ризику атак на реальні системи;
- Отримання інформації для вивчення поведінки, методів і засобів злоумисників.

Honeypot дозволяє попереджати, виявляти і протоколювати діяльність порушника. Правильно налаштована медова пастка повинна відвертати увагу та ресурси злоумисника від реальної системи. Це надласть можливість виявити атаку та надаст інформацію про для її вивчення, а головне час для того щоб розібратися і прийняти правильне рішення.

Важливо розуміти, що *Honeypot*-система не зменшують ризик для підприємства, а дає змогу отримувати інформації, яка в свою чергу буде використана для створекння більш надійних мереж.

На рис. 3.1 наведено схему реалізації простої медової пастки.

Для того щоб не було ознак медової пастки, вузол повинен обслуговувати зовнішній трафік, конфігурація має відрізнятися від стандартної конфігурації тощо.

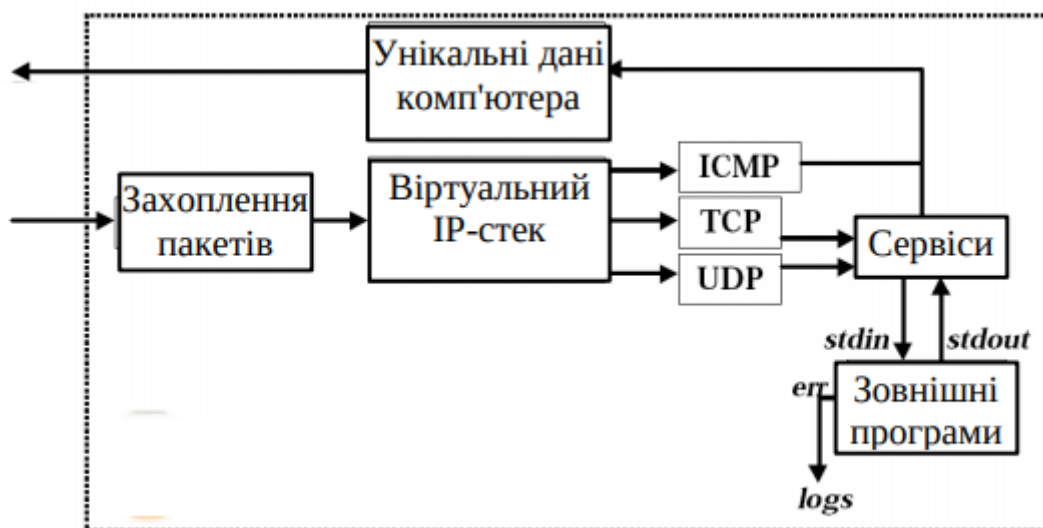


Рис. 3.1. Схемай найпростішої Honeypot системи

Приманки поділяються на реальні та віртуальні. Реальні приманки працюють на виділеному виробником апаратному забезпеченню. Реальна приманка найкраща мішень. Виглядає така мішень як реальний ресурс і зловмиснику дуже важко зрозуміти, що атака здійснюється на приманку.

Для управління реальними приманками потрібно багато знань та часу, а це в свою чергу головний недолік таких приманок. Іноді для того щоб встановити реальну приманку потрібно стільки ж часу як і для реального ресурсу. Також важко завадити зловмиснику якому вдалось захопити приманку атакувати інший ресурс. Багато реальних приманок *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 [9].

Віртуальні приманки в свою чергу програмним забезпеченням сковують дії дії зловмисника. Можливий збиток для ресурсів сильно знижується або повністю ліквідовується. Переважна більшість приманок імітують роботу відкритих портів, закритих портів.

Приманки які лише відкривають порт і реєструють запит зломщика мають назву – слухачі порту. Досконаліші слухачі порту відповідають простими пакетами відкриття/закриття, такі дії привертають увагу зломщика. Вони

записують інформацію яка надсилається зловмисником та відповідають у відповідності з протоколом. Приманки залишаються поза передачею і спроба з'єднання хакера не буде успішною. Дані дії дають адміністраторам достатньо інформації і дають можливість знизити ризик до мінімуму.

Як вже говорилось вище, си лова протидія вторгненням та атакам в мережі вимагає використання великих ресурсів, а виконати успішно дану прротидію вдається в рідких випадках. Тоді як стратегія відволікання ресурсів противника (розроблена в рамках загальної теорії конфлікту) часто дає перевагу навіть тоді коли ресурси нападника перевищують ресурси захисників.

Детальнішезупинимось на моделі конфліктів "атака – захист" яка дає можливість затягувати супротивника (хакера, зловмисника) у медову пастку псевдосервісу, а також перебіг розвитку конфлікту.

3.3. Створення моделі конфлікту, стратегії атаки та захисту

Для опису процесу протиборства атакуючої сторони і сторини захисту використовуються диференційно-різницеві рівняння, або рівняння з аргументами, що відхиляються [11]. Дана гіпотиза має місце для дискретних систем з запізненнями, даними запізненнями виступають мережі розподіленої інформаційної системи.

В загальному випадку

$$\begin{cases} z'_{ids}(t) = f_1(t, z_{ids}(t), \dots, z_{ids}(t - \tau_1), u_1(t), v_2(t - \tau_2), \xi(t)); \\ z'_{icm}(t) = f_2(t, z_{icm}(t), \dots, z_{icm}(t - \tau_2), u_2(t - \tau_2), v_1(t), \eta(t)), \end{cases} \quad (3.1.)$$

де Z_{ids} і Z_{icm} - вектори стану систем S_{ids} і S_{icm} відповідно;

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

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

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

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

τ_1 і τ_2 - запізнення у векторах S_{ids} і S_{icm} відповідно.

Враховуючи фактори нормалізації випадкових процесів у великих системах для вирішення рівнянь (1) метод гаусовської апроксимації в малій околиці точок екстремуму E_1 і E_2 . В такому випадку рівняння матиме вигляд:

$$E_1 = \int_0^T z_{ids}(t) dt, \quad E_1 \rightarrow \max_{v_1}, \quad E_2 = \int_0^T z_{icm}(t) dt, \quad E_2 \rightarrow \max_{v_2} \quad (3.2.)$$

Для кожної системи основне завдання підвищити свою ефективність і максимально знизити ефективність противника. Проте результат даних намагань стає відомий лише в певний момент часу T . На інтервалі спостереження $0 \leq t \leq T$ можна виробляти найкращі управління $u_1(t)$, дії $v_1(t)$ та прогнозувати кінцевий результат. Задачі конфлікту необхідно вирішувати з мінімальною часткою ресурсу, який дається для захисту. Реальний конфлікт частіше всього відбувається нелінійно, для того щоб отримати інформацію на великому відрізку (а отже, при значній кількості кроків розвитку конфлікту) припустимим буде допустити покрокове спрощення (зведення до лінійного виду) на основі методів кореляції та регресії [14]. Щоб знайти коефіцієнти моделі розробили спеціальну покрокову схему, яка включає в себе заміну та виключення незалежних змінних. При цьому у вибірці можна залишити незалежні змінні X_1, X_2, \dots, X_p . Можливо залишити даний елемент у вибірці та використати виміри, що містяться в ньому, для обчислення вектора середніх значень X та матриці R_x .

Для кожного з методів властивості в більшості випадків залишаються невідомими, а отже немає жодних гарантій, що результати які будуть отримані виявляться незміщеними. Через це елементи вибірки, змінні без значень завжди видаляються, це дає змогу зберегти баланс змінних та числових елементів, які залишаються в мережі. Збільшується число елементів вибірки, елементи які містять багато пропусків мають бути усунені. Коли значення змінної невідоме, для більшості елементів, таку змінну необхідно видалити. Після таких маніпуляцій дозволляється використувати методи множинного регресійного аналізу [15]. На рис. 3.2. наведено математичну модель типу "предиктор-

коректор" , модель процесів розвитку конфлікту з передбаченням та виправленням помилкових припущень .

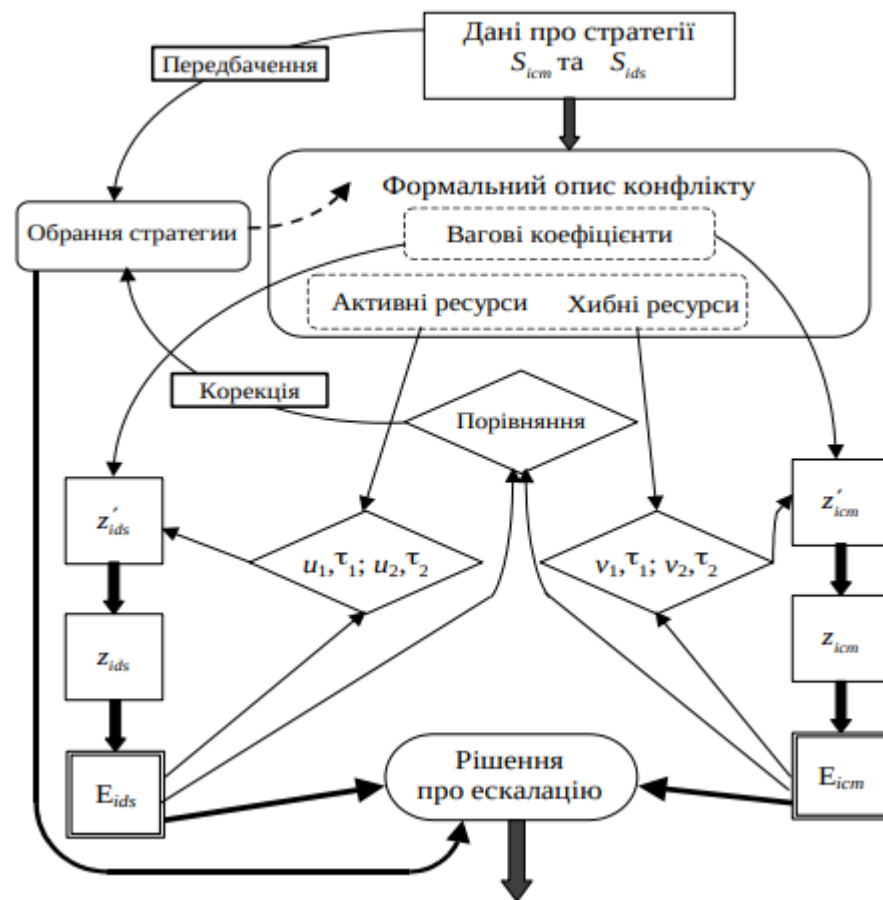


Рис. 3.2. Модель конфлікту з можливою ескалацією в псевдо сервіс

Розробляються стратегії для протидії атакам згідно класичної теорії конфлікту [6] та модифікуються в залежності з завданням [5].

Розберемо наглядні стратегії захисту:

- відмова від отримання - звичайне повернення трафіку невідомого походження;
- розподілена відмова від отримання – підозрілий трафік транслюється на багато точок;
- насичення псевдосервісамі рубежів захисту 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[10].

Активні дії по відображенню атаки передбачаються в системі захисту яка була заснована на теорії конфлікту. В такій системі захисту розглядаються як теоретичні моделі так і методи аналізу того як буде розвиватися конфлікт і максимальній оптимальності послідовностей дій захисту. Правові аспекти заходів. То вони передбачають тільки оцінку адекватності в системах, така оцінкам має бути досить об'єктивною.

3.4. Процес розвитку конфлікту з затягуванням у медову пастку та його динамічні характеристики

Перебіг конфлікту – це розгалужений випадковий процес, перехідні та фінальні властивості якого залежать вхідних ресурсів учасників конфлікту.

Стан конфлікту описується у вигляді певного функціоналу $\delta R = \Psi[\varphi(S_{ids}, E_{ids}), \varphi(S_{ism}, E_{icm})]$, даним функціоналом характеризується перевага через використання певного плану. План оцінюють по його характеристикам, враховуючи інтенсивність застосування. Інтенсивність оцінюється з енергетичного ресурсу (можна оцінювати за точками з яких відбувається атака). Оцінку стратегії проводять згідно її інформаційної цінності. Першим з приближених для вибору функціоналу беруть аддитивну міру стратегій. Вплив стратегії вибирають враховуючи вагові коефіцієнти або функції.

Більш детально зупинемось на алгоритмі конфлікту, який умовно відбувся між розподіленими атакуючими і захисними системами . Процес атакуючих і контратакуючих потоків зображена на рис 3.3.

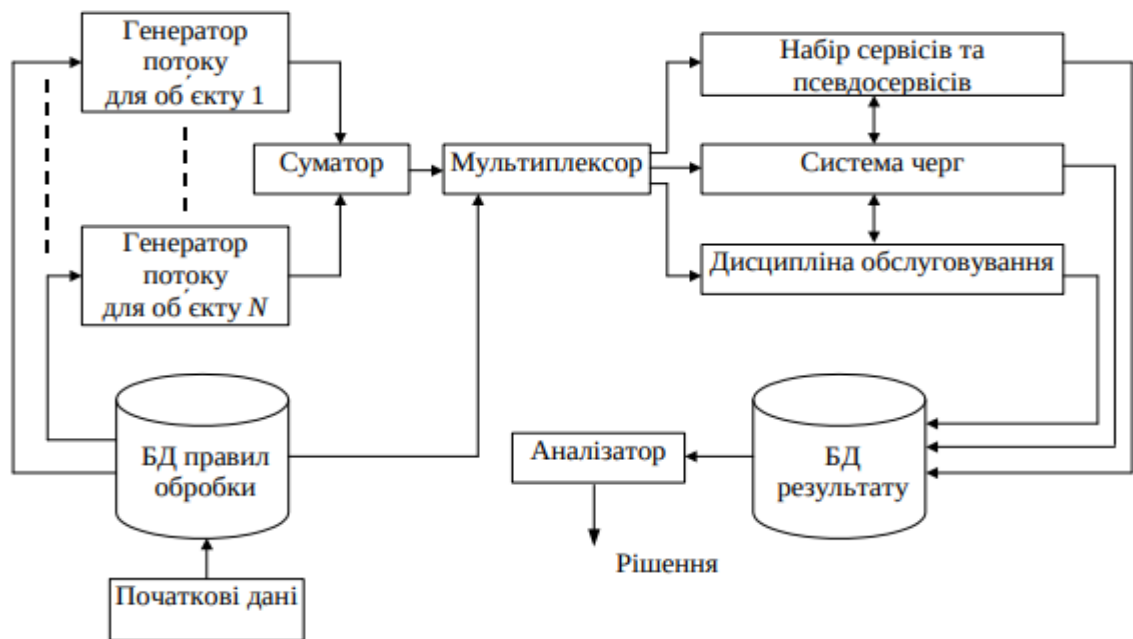


Рис. 3.3. Алгоритм створення псевдосервісів

З рис 3.3. розуміємо, що розвиток конфлікту визначається на основі результатів повного аналізу системи, від вихідних даних та поточної інформації про характеристики трафіку мережі.

Повина виконуватися послідовність заходів захисту як пасивних так і активних (можуть бути і ті і ті). Уявімо, що наслідком атаки можливість нормальної роботи певного об'єкта знижується, може навіть до нуля, і в наслідок використання певного захисного засобу, функціонування системи може бути відновлено. Отже, в будь який момент часу система може перебувати в одному з N станів, $\phi_1, \phi_2, \dots, \phi_n$, характеризує поточну ймовірність функціонування об'єкта. Відомий початковий стан системи (в початковий момент часу t_0 вона знаходиться в стані $\psi_0 = \phi_i$) і однокрокові ймовірності переходу. Значить, якщо ігнорувати випадковий характер часу очікування і цікавитися тільки моментами переходу, то процес $\psi_1 = \psi(t_1)$ є вкладений однорідний ланцюг Маркова [6]. Можливість переходу ρ_{ik} буде визначатися повністю i -м станом, та k -ї атакуючою дією.

Затримки τ_1 та τ_2 в системах S_{ids} та S_{icm} являються дискретними процесами, дані процеси не обов'язково мають бути марківськими. Проте це не є важливим для аналізу, адже величини ρ_{mn} , $m, n \in M$, дають повну інформацію про розвиток конфлікту.

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 (дивитися рис 3.4 та 3.5). По досягненні стану ϕ_j «миттєво» переходить лр наступного стану. Під «миттєвість» розуміємо, що тривалість переходу є величиною другого порядку в порівнянні з мінімальною тривалістю перебування в поточному стані.

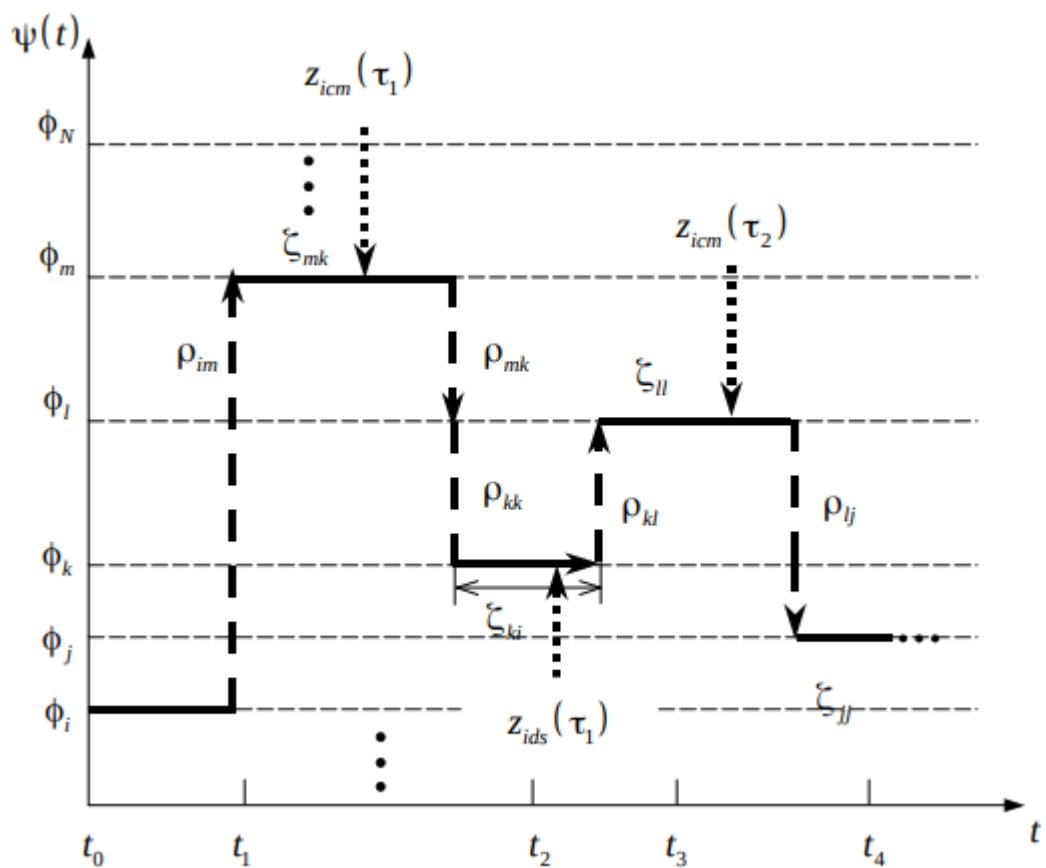


Рис. 3.4. Зміна ймовірностей функціонування об'єкта з системою захисту

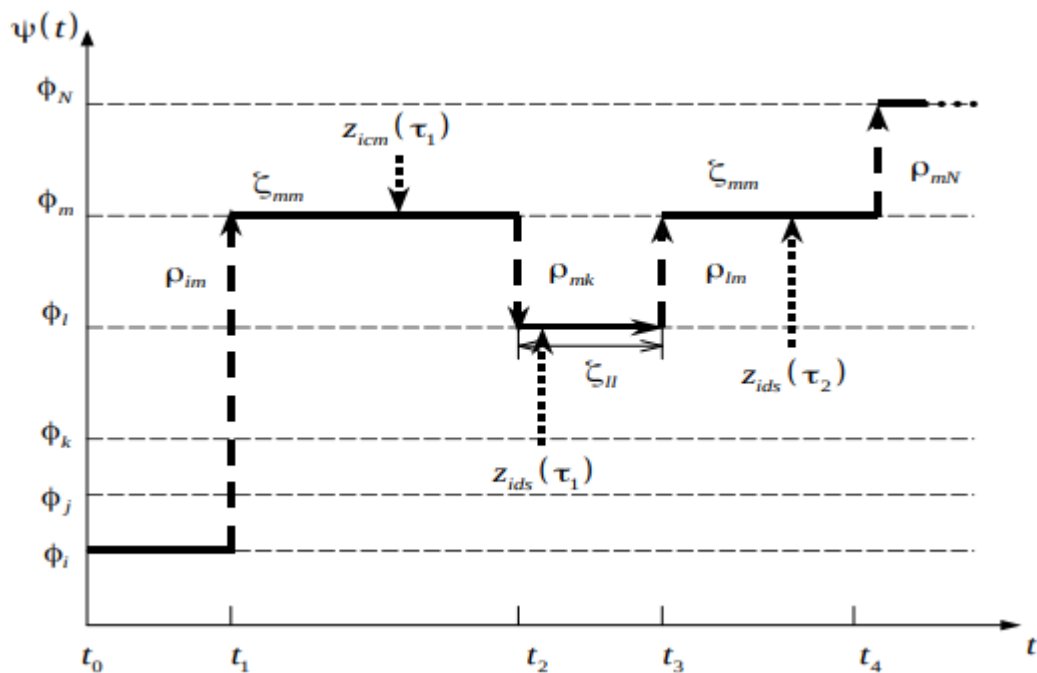


Рис. 3.5. Зміна ймовірностей функціонування об'єкта з системою захисту

Якщо для точки, що відображає поведінку системи і знаходиться в n -м стані, з імовірністю переходу ρ_{n1} знову обирається стан 1, горизонтальна частина траєкторії руху точки позначається лінією зі стрілкою на кінці, як це зображено на графіках, див. Рис 3.4 та 3.5.

На даний час системи виявлення вторгнень в корпоративні мережі та виявлення означ атаки на системи та мережі має безліч недоліків, а це в свою чергу дозволяє зловмисникам долати системи захисту інформації. Заміна пошуку сигнатур на визначення умов визначення загроз інформаційної безпеки мусить сприяти допомогти різко змінити цю ситуацію на кращ і дати можливість захисним технологіям зрівнятися з атакуючими. Також данна заміна значно підвищує ефективність керування безпекою. Дає змогу більш конкретно на прикладах використовувати нормативні та керівні документи та стандарти. Максимально перспективним напрямом подальшого розвитку систем інформаційного захисту представляються ескалаційні пастки з імітацією боротьби з супротивником шляхом стохастичного управління змінами уразливостей псевдосервісів (медових пасток). [1-38]

Висновки до розділу

В результаті написання даного розділу було розглянуто та проаналізовано захист комп'ютерної корпоративної мережі від розподілених атак. Одним з основних методів які часто використовують зловмисники для приховання своєї атаки - це атака на введення коду на основі хоста. Цей метод дає змогу шкідливому програмному продукту виконувати свій код у зовнішньому процесоровому просторі, а це в свою чергу дає змогу працювати таємно та отримати доступ до критичної інформації процесів. На даний момент існує велика кількість способів введення та виконання коду. Але необхідний один загальний підхід який б включав би в себе всі ці можливості.

Недостатньо використовувати лише підходи які фокусуються на операційних системах низького рівня. Тому що набір API постійно розширюється. Через цю особливість такі підходи мають схильність до втрати нових атак. Обмеженні такі підходи знанням лише однієї операційної системи.

Технологія яка була розглянута *Honeypot* (медової пастки) є одним з найбільш ефективних та доступних засобів виявлення та протидії атакам на мережні ресурси. Суть технології полягає в тому, щоб розмістити в мережі легкодоступну і привабливу мету, ззовні яка нічим не відрізняється від справжніх ресурсів. Призначення має лише одне – потрапити на очі зловмиснику, та спровокувати його злочинні дії, та повідомити адміністратору про факт вторгнення.

Було визначено місце *Honeypot* в системі безпеки корпоративної мережі. Розроблено модель конфлікту і аналіз стратегій атак та захисту. Спираючись на теорію конфлікту процеси протистояння між атакуючою стороною та стороною захисту описуються диференційно-різницею рівнянням. Дане припущення справедливе для дискретних систем. До таких систем відносять комп'ютерні мережі та розподілені інформаційні системи.

Розглянуто основні динамічні характеристики процесу розвитку конфлікту з медовими пастками. 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 аддитивну міру безлічі стратегій, а відносний вплив конкретної стратегії врахувати ваговими коефіцієнтами або функціями.

ВИСНОВКИ

У дипломній роботі досліджено питання системи захисту інформації в комп'ютерній мережі підприємства.

Ця тема грає велику роль у концепції сталого розвитку підприємства. Розробка, впровадження та використання мережних інформаційних систем виявлення атак є головною задачею в сфері інформаційного забезпечення установ. Під час написання дипломного проєкту було вивчено та представлено:

- Структура обчислювальної мережі підприємства;
- Аналіз потоків інформації (як у внутрішній мережі, так і між підрозділами підприємства);
- Алгоритм передачі та збереження інформації (схема процесу документообігу).

Ця тема грає велику роль у концепції сталого розвитку підприємства. У дипломній роботі надані перелік додаткових заходів щодо захисту інформації, розробка архітектурної системи захисту безпеки й обмеження доступу в корпоративну інформаційну мережу підприємства:

- 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").

Під час написання дипломного проєкту було вивчено та представлено:

- Структура обчислювальної мережі підприємства;
- Аналіз потоків інформації (як у внутрішній мережі, так і між підрозділами підприємства);

- Алгоритм передачі та збереження інформації (схема процесу документообігу).

Основним рішенням щодо запобігання розподілених атак на комп'ютерні мережі та системи підприємства було обрано теорію конфлікту та адаптації степенів уразливості до поведінки атакуючого об'єкту, а саме:

- агресивна поведінка – демонстрація спокою;
- нейтральна поведінка – демонстрація впевненості;
- втрата інтересу – демонстрація розгубленості

Дані зміни концепцій взаємодії системи захисту з атакуючим суб'єктом надають можливість утримувати його у постійній напрузі і виключає підозри в тому, що суб'єкт потрапив у медову пастку.

З метою охорони анонімної інформації, якою обмінюються філії підприємства, використана технологія віртуальної корпоративної мережі підприємства, що створює умови для реалізації захисту каналу передачі даних від перехоплення і підміни інформації. Для збереження внутрішньої схеми побудови комп'ютерної інфраструктури підприємства використані антивірусні рішення.

Проксі-сервіси використовуються для наступних цілей:

- Доступ з локальної комп'ютерної мережі в Інтернет.
- Кешування даних: при регулярному зверненні до одних і тих самих зовнішніх ресурсів, можна отримати їх копію на проксі-сервері і видавати за запитом. До того ж це допомагає знизити навантаження на канал обміну інформації у зовнішню мережу і прискорює отримання клієнтом потрібної інформації.
- Стиснення даних: завантажуючи інформацію з Інтернету, проксі-сервер передає її у стисненому вигляді. Так проксі-сервери працюють з метою економії зовнішнього трафіку.
- Захист мережі від зовнішнього доступу: параметри налаштування проксі-серверу дозволяють зробити можливим звертання до зовнішніх ресурсів

тільки через нього, а зовнішні комп'ютери не зможуть звернутися до термінальним вузлів взагалі (вони можуть «бачити» тільки проксі-сервер).

- Обмеження доступу з корпоративної мережі до зовнішньої: проксі-сервер дозволяє заборону доступу до певних ресурсів, обмеження використання інтернету певним локальним користувачам, встановлення квоти на трафік чи смугу пропускання, фільтрування рекламного контенту та підозрілі трафіки чи віруси.

- Конфіденційність доступу до різних ресурсів. Проксі-сервер приховує інформацію про джерело запиту або користувача. Тобто зовнішній сервер «бачить» лише дані проксі-серверу (наприклад, IP-адресу), але визначити дійсне джерело запиту – неможливо. Також бувають спотворюючі проксі-сервери, що передають сторонньому серверу «фейкову» інформацію про існуючого користувача.

Для управління використовується інтерфейс, що має широкий набір параметрів та інструментів з управління доступом користувачів по протоколам HTTP та FTP. Також є можливість проаналізувати та сформулювати статистичні дані, такі, як часто відвідувані вузли, кількість «спійманих» вірусів та ін.

При потребі взаємодії підрозділу з центральним офісом через VPN-канал використовується термінал-сервер. Термінальний клієнт після встановлення зв'язку з термінальним сервером пересилає на останній та вводять дані (натискання клавіш, переміщення миші) і далі, можливо, дозволяє доступ до локальних ресурсів (наприклад, принтер, дискові ресурси, пристрій читання смарт-карт, локальні порти (*COM / LPT*)). Термінальний сервер створює середовище для роботи (термінальна сесія). Як результат роботи серверу передаються зображення монітору чи звук (при його присутності).

До переваги схеми використання термінального серверу можемо віднести забезпечення безпеки та зниження навантаження на канал зв'язку.

Отже, завдання дипломного проєктування виконані. Отриманні знання та інформація надалі можуть бути використані для захисту корпоративної інформації в комп'ютерних мережах чи системах підприємств чи установ, не залежно від масштабу, територіального розміщення чи призначення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. The Great IDS Debate: Signature Analysis Versus Protocol Analysis by Matt Tanase, Feb. 5, 2003/ Електронний ресурс: режим доступу:
2. <https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=b4c1f4bd-4199-4d9e-b61b486b3df2d76c&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments>
3. CompTIA Security+ SY0-501 Cert Guide, Academic Edition, 2nd Edition By David L. Prowse - 560 pp.
4. 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.
5. <https://www.projecthoneypot.org/>
6. Lance Spitzner. Honeypots: Tracking Hackers. Addison Wesley, 2002. - 480 pp.
7. <http://www.iso27000.ru/standarty/bsi-it-baseline-protection-manual>
8. 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/
9. 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.
10. Cybersecurity Best Practices Guide For IIROC Dealer Members - Investment Industry Regulatory Organization of Canada, 2015. - 53 pp.
11. Joseph Migga Kizza J.M. Guide to Computer Network Security, Fourth Edition. - Springer International Publishing AG 2017. - 569 pp.

12. 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.
13. Stapelberg R.G. Handbook of Reliability, Availability, Maintainability and Safety in Engineering Design. Springer-Verlag London Limited, 2009. - 827 pp.
14. Csermely P. WEAK LINKS: The Universal Key to the Stability of Networks and Complex Systems. - Springer-Verlag Berlin Heidelberg 2009. - 404 pp.
15. Stavroulakis P. RELIABILITY, SURVIVABILITY AND QUALITY OF ARGE SCALE TELECOMMUNICATION SYSTEMS. - John Wiley & Sons, Ltd., The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England. 2003 - 353 pp.
16. Buttazzo G.C. Hard Real-Time Computing Systems (3rd Edition). Springer Science+Business Media, LLC 2011. - 521 pp.
17. Klein M.H. A Practitioner's Handbook for Real-Time Analysis / Mark H. Klein, Thomas Ralya, Bill Pollak, Ray Obenza. - Kluwer Academic Publishers, 1993. - 701 pp.
18. 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.
19. Krten R. QNX Neutrino RTOS. - QNX Software Systems Limited, 1001 Farrar Road, Kanata, Ontario, Canada, 2012. - 372 pp.
20. Гома X. UML Проектирование систем реального времени, параллельных и распределенных приложений, Пер. с англ. - М.: ДМК Пресс, 2011. - 704 с.
21. 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.
22. Stallings W. WIRELESS COMMUNICATIONS AND NETWORKS, 2nd Ed. - Pearson Education, Inc., Upper Saddle River, NJ, USA, 2005. - 559 pp.

23. Crimes R.A. Honeypots for Windows. - APRESS, 2005. - 392 pp.
24. Joshi R.C. Honeypots A New Paradigm to Information Security / R.C. Joshi, Anjali Sardana. - Science Publishers, P.O. Box 699, Enfield, NH 03748, USA, 2001. - 323 pp.
25. 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.
26. Шнайдер Б. Прикладная криптография, 2 изд. - М.: Диалектика, 2016. - 610 стр.
27. Шнайдер Б. Секреты и ложь. Безопасность данных в цифровом мире. СПб: Питер, 2003. - 368 стр.
28. Орлов И.Я. Перспективные методы защиты информационных радиосистем от помех. - Нижний Новгород: Изд-во Нижегородского госуниверситета, 2006. - 126 с.
29. Graham R. COMMUNICATIONS, RADAR AND ELECTRONIC WARFARE. - John Wiley and Sons, Ltd., The Atrium, Southern Gate, Chichester, West Sussex, PO 19 8SQ, United Kingdom. 2011. - 378 pp.
30. Бутковский А.Г. Структурная теория распределенных систем. М.: Наука, 1977. - 320 стр.
31. Дружинин В.В., Конторов Д.С., Конторов М.Д. Введение в теорию конфликта. - М.: Радио и связь, 1989. - 288 с.
32. Mesarovic M.D. General Systems Theory: Mathematical Foundations. / M.D. Mesarovic, Yasuhico Takahara. - Academic Press, New York, 1975, xii+268 pp.
33. 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.
34. Myers G.J. The Art of Software Testing 3rd Ed. / Glenford J. Myers, Corey Sandler, Tom Badgett. - John Wiley & Sons, Inc., 2012. - 256 pp.

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

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

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

38. 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.