ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»
МІНІСТЕРСТВА ОСВІТИ І НАУКИ УКРАЇНИ
Кафедра комп'ютерних інтелектуальних систем та мереж

КОЛОС Олександр Юрійович

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

ДОСЛІДЖЕННЯ ТА РОЗРОБКА МОДЕЛЕЙ ОЦІНКИ ЗАХИЩЕННОСТІ КОМП’ЮТЕРНИХ МЕРЕЖ

Спеціалізація – Комп'ютерні системи та мережі
Спеціальності – 123 - Комп`ютерна інженерія

Керівник: Тішин Петро Металінович
К.ф-м.н, доцент

Одеса – 2021

З А В Д А Н Н Я

НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТУ

Колос Олександр Юрійович
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Дослідження та розробка моделей оцінки захищеності комп'ютерних мереж

керівник проекту (роботи) Тішин П.М., к.ф-м.н, доцент,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом ректора ОНПУ від "__" ____2020 року № _____

2. Строк подання студентом проекту (роботи) 01.12.2021

3. Вихідні дані до проекту (роботи) завдання на дослідження

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1) Проблеми захищеності комп'ютерних мереж, типи загроз та їх виявлення

2) Аналіз моделей виявлення вторгнень

3) Моделі визначення вторгнень на основі сценаріїв та загроз

4) Модель оцінки захищеності комп'ютерних мереж

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) Характеристика роботи; Аналіз мережевого трафіку; Типи загроз; Опис структури зловмисника; Формування послідовностей вторгнення; Модуль управління сигнатурами; Визначення родових сигнатур, Оцінка мережевого трафіку; Модуль аналізу вторгнення; Модель виявлення вторгненнь; Система оцінки аналізу вторгненнь; Оцінка результату роботи, Переваги використання моделей

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Проблеми захищеності комп'ютерних мереж, типи загроз та їх		
	виявлення		
2	Аналіз моделей виявлення вторгнень		
3	Моделі визначення вторгнень на основі сценаріїв та загроз		
4	Модель оцінки захищеності комп'ютерних мереж		
	Ілюстративний матеріал		

Студент _____ _____
(підпис) (прізвище та ініціали)

Керівник проекту (роботи) _____ _____
(підпис) (прізвище та ініціали)

Відомість кваліфікаційної роботи магістра

№	Найменування	Кільк.	Примітка
1	Пояснювальна записка	66	
2	Характеристика роботи	1	
3	Аналіз мережевого трафіку	1	
4	Типи загроз	1	
5	Модуль управління сигнатурами	1	
6	Визначення родових сигнатур	2	
7	Оцінка мережевого трафіку	1	
8	Модуль аналізу вторгнення	1	
9	Модель виявлення вторгненнь	1	
10	Система оцінки аналізу вторгненнь	1	
11	Оцінка результату роботи	1	
12	Переваги використання моделей	1	
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
24			

				АМДР.ЗАМ151.0101			
Зм. Лист	№ докум.	Підпис	Дата				
Розробив	*Колос О.Ю*			Дослідження та розробка моделей оцінки захищеності комп'ютерних мереж	Літ.	Лист	Листів
Перевірив	*Тішин ПМ*					*1*	*1*
Реценз.					«Одеська політехніка»		
Н. Контр.					ІКС КІСМ ЗАМ151		
Затвердив							

АНОТАЦІЯ

Колос О. Ю. Дослідження та розробка моделей оцінки захищеності комп'ютерних мереж – кваліфікаційна робота магістра. Одеса, 2021: 66 стр., 8 рис., 2 табл., 12 джерел.

Об'єкт дослідження – процеси виявлення вторгнень у комп'ютерні мережі.

Предмет дослідження – комп'ютерні мережі.

Мета роботи – оцінка ступені захищеності комп'ютерних мереж з визначенням зменшення витрат часу на виявлення вторгнень у мережу та зменшення кількості помилкових сигналів про вторгнень, за рахунок використання нечітких моделей опису процесів порушення безпеки та їх ініціаторів

В роботі виконано аналіз сучасних систем виявлення вторгнень, їх типів та методів, на яких виявлення вторгнень базується. Також виявлено, що найбільш розповсюдженими на сьогоднішній час є сигнатурні методи виявлення вторгнень. Зазначено, що даний підхід є трудомістким та не дає гарантій виявлення невідомих мережевих атак. Виходячи з виявлених недоліків, в дослідженні запропоновано використовувати сімейство нечітких моделей, які описують процес вторгнення з позиції невизначеності та дозволяють виявляти сигнатури процесів вторгнення у комп'ютерні мережі. Разом з тим, рекомендовано проводити нечітку класифікацію виявлених сигнатур вторгнень для виявлення загальних ознак мережевих атак.

На основі розроблених моделей розроблена структура системи виявлення вторгнень з використанням інтелектуальних засобів опису процесів вторгнення. Проведено оцінювання ступені захищеності комп'ютерних мереж з використанням запропонованої системи виявлення вторгнень.

СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ, МЕРЕЖЕВІ АТАКИ, НЕЧІТКІ МОДЕЛІ, МОДЕЛІ ВТОРГНЕНЬ, КОМП'ЮТЕРНІ МЕРЕЖІ, ОЦІНКА ЗАХИЩЕНОСТІ.

ABSTRACT

Kolos O. J. Research and development of models for assessing the security of computer networks - master's thesis. Odessa, 2021: 66 pages., 8 figs., 2 tables, 12 sources.

The object of research is intrusion detection processes on computer networks.

The subject of research is computer networks.

The aim of the work is to assess the degree of security of computer networks with the definition of reducing the time spent on detecting network intrusions and reducing the number of false intrusion signals, through the use of fuzzy models to describe security breaches and their initiators

The analysis of modern intrusion detection systems, their types and methods on which intrusion detection is based is performed. It was also found that the most common to date are signature intrusion detection methods. It is noted that this approach is time consuming and does not guarantee the detection of unknown network attacks. Based on the identified shortcomings, the study proposes to use a family of fuzzy models that describe the process of intrusion from the standpoint of uncertainty and allow to detect signatures of intrusion processes in computer networks. However, it is recommended to perform a fuzzy classification of detected intrusion signatures to identify common signs of network attacks.

Based on the developed models, the structure of the intrusion detection system was developed using intelligent means of describing intrusion processes. The degree of security of computer networks was evaluated using the proposed intrusion detection system.

INVASION DETECTION SYSTEMS, NETWORK ATTACKS, FUZZY MODELS, INVASION MODELS, COMPUTER NETWORKS, SECURITY ASSESSMENT.

ЗМІСТ

Вступ 5
1 Проблеми захищеності комп’ютерних мереж, типи загроз та їх виявлення 8
1.1 Типові атаки на комп’ютерні мережі 8
1.1.1 Аналіз існуючих рішень виявлення вторгнень 10
1.1.2 Аналіз рішень запобігання вторгнень до мережі 12
1.2 Обмеження систем виявлення та запобігання вторгнень 13
1.3 Сигнатурний аналіз вторгнень 15
1.4 Аналіз вторгнень за поведінкою 16
1.5 Висновки до розділу 18
2 Аналіз моделей виявлення вторгнень 20
2.1 Використання умовної ймовірності 20
2.2 Продукційні та експертні системи 21
2.3 Аналіз зміни станів 23
2.4 Спостереження за вводом даних 23
2.5 Методи, засновані на моделюванні поведінки зловмисника 24
2.6 Висновки до розділу 29
3 Моделі визначення вторгнень на основі сценаріїв та загроз 30
3.1 Невизначеність параметрів вторгнень 32
3.2 Моделювання послідовностей вторгнень 38
3.3 Моделі ініціаторів вторгнення 45
3.4 Висновки до розділу 50
4 Модель оцінки захищеності комп’ютерних мереж 51
4.1 Визначення ступеню близькості сигнатур вторгнень 51

4.2 Процес оцінки мережевого трафіку 54
4.3 Оцінка реакцій на вторгнення 57
4.4 Загальна структура системи виявлення вторгнень 58
4.5 Висновки до розділу 59
Висновки 63
Перелік посилань 65

ВСТУП

Актуальність. Основною метою забезпечення захисту комп'ютерних мереж є досягнення такого стану системи, коли вторгнення та атаки в її роботу неможливі. Логічно, що досягнення такого стану або неможливе, або досягається непомірно високими витратами коштів, часу та обмеженнями для користувачів цільової мережі.

В такому разі цілі інженерів та адміністраторів мереж зміщуються на досягнення стану мережі, в якому рівень захисту організований на рівні, відповідному цінностям активів, які захищаються.

Для визначення факту вторгнення використовується множина механізмів, робота яких заснована на аналізі функціонування мережі, зокрема:

– аналіз мережевого трафіку всередині мережі;

– аналіз мережевого трафіку з мережі Інтернет та до неї;

– аналіз процесів кінцевих пристроїв мережі;

– аналіз процесів на мережевому обладнанні.

Для забезпечення цього можна використовувати різноманітні підходи, такі як:

– пасивний моніторинг мережі;

– активний моніторинг мережі;

– фільтрація трафіку;

– антивірусний захист та ін.

Серед цієї множини заходів, окремим ефективним засобом є використання спеціальних систем виявлення вторгнень. Робота даного класу апаратних або програмних засобів зосереджена на аналізі подій в мережі та на її обладнанні, для визначення того, чи є на об`єкті аналізу підозріла

активність. Для цього система вимушена збирати увесь трафік, який проходить в мережі, проте, обсяг інформації, яку збирає система - це компроміс між витратами та адекватністю. Система, яка у всіх деталях, може зазнати втрат продуктивності. Малий об’єм інформації може оказатись недостатнім для адекватного аналізу.

Існує дві основні категорії методів виявлення вторгнень: виявлення аномалій і виявлення зловживань.

Перший тип використовує моделі відомої поведінки користувачів і процесів, виявляючи відхилення від стандартної поведінки.

Головна перевага систем виявлення аномалій полягає в тому, що вони можуть виявляти раніше невідомі атаки. Можна виявити будь-яке порушення, незалежно від того, передбачено воно моделлю потенційних загроз чи ні. Проте перевага виявлення раніше невідомих атак часто не співставляється з кількістю помилкових висновків про вторгнення.

При використанні другого типу виявлення, визначають, що йде не так, як повинно. Такі системи містять сигнатури і виявляють відповідність цим описам.

Основна перевага систем виявлення зловживань полягає в тому, що вони зосереджуються на аналізі даних і, зазвичай, породжують дуже мало помилкових тривог. Головним недоліком визначення тільки вже відомих атак, для яких вже існує сигнатура.

Таким чином, необхідність досліджувати методи та моделі для систем виявлення вторгнень, які дозволяють сумісно використовувати переваги сигнатурних методів виявлення та методів виявлення аномалій для оцінки захищеності комп’ютерних мереж є актуальною науковою проблемою.

Об’єктом даного дослідження визначено процеси виявлення вторгнень у комп’ютерні мережі, які потребують аналізу та створення цифрових сигнатур.

Предметом даного дослідження визначено комп’ютерні мережі та системи виявлення вторгнень у комп’ютерні мережі, які дозволяють

оперативно та з адекватним рівнем достовірності визначати факт втручання в систему.

Метою роботи є оцінка ступені захищеності комп’ютерних мереж з визначенням зменшення витрат часу на виявлення вторгнень у мережу та зменшення кількості помилкових сигналів про вторгнень, за рахунок використання нечітких моделей опису процесів порушення безпеки та їх ініціаторів

Практичною значимістю результатів такого дослідження є те, що використання моделей інтелектуального аналізу трафіку, які засновані на нечітких моделях описання поведінки зловмисників під час вторгнення, описання етапів реалізації самого вторгнення та автоматизація цих процесів, а також процесів визначення реакції на ці вторгнення дозволять своєчасно реагувати на вторгнення в мережу, моделювати атаки на систему з ціллю формування нових сигнатур. Також є доцільним визначення спільних рис для однотипних атак, що дозволяє визначати характерні ознаки вторгнень, що в свою чергу, дозволяє створювати групи вторгнень і визначати факт вторгнення на основі відповідності до сигнатури групи, а не поодинокої сигнатури.

1 ПРОБЛЕМИ ЗАХИЩЕНОСТІ КОМП'ЮТЕРНИХ МЕРЕЖ, ТИПИ ЗАГРОЗ ТА ЇХ ВИЯВЛЕННЯ

1.1 Типові атаки на комп'ютерні мережі

Програмні комплекси часто мають уразливості. Це ненавмисні вади або прогалини в програмних кодах, якими гіпотетично можна скористатися. Наприклад, може бути недолік, який дозволяє кіберзлочинцю отримати доступ до захищених, в іншому випадку, даних. Програмісти часто шукають ці уразливості і, коли вони виявляють уразливість, вони аналізують її, розроблюють спеціальну програму для виправлення вразливості, а потім видають цей патч у новому випуску програмного забезпечення. Однак це процес, який вимагає часу. Коли недолік стане відомим, хакери у всьому світі можуть почати намагатися його використати; іншими словами, розробники мають нульовий день, щоб знайти вирішення проблеми, отже, такі недоліки можна назвати "вразливість нульового дня".

Якщо хакеру вдається скористатися уразливістю, перш ніж розробники програмного забезпечення зможуть знайти виправлення, ця експлуатація стає відомою як атака нульового дня. Вразливості з нульовим днем можуть мати майже будь-яку форму, оскільки вони можуть проявлятися як будь-який тип ширшої вразливості програмного забезпечення. Наприклад, вони можуть мати вигляд шифрування відсутніх даних, введення SQL, переповнення буфера, відсутність авторизації, непрацездатних алгоритмів, перенаправлення URL-адрес, помилок або проблем із захистом пароля. Це ускладнює пошук вразливих місць за нульового дня, що в деякому сенсі є гарною новиною, оскільки це також означає, що хакерам буде важко їх

знайти. Але це також означає, що важко ефективно захиститися від цих вразливостей.

Важко захиститися від можливості атаки нульового дня, оскільки вони можуть мати різну форму. Майже будь-який тип вразливості безпеки може бути використаний як нульовий день, якщо виправлення не буде створено вчасно. Крім того, багато розробників програмного забезпечення навмисно намагаються не публікувати вразливість, сподіваючись на те, що вони можуть випустити виправлення до того, як будь-які зловмисники виявлять наявність вразливості. Є кілька рекомендацій, які можуть допомогти захисти мережу від атак нульового дня:

– інформування про вразливості. Експлойти з нульовим днем незавжди розголошуються, але іноді ви почуєте про вразливість, яку потенційно можна використати. Якщо ви стежите за новинами та звертаєте увагу на випуски постачальників програмного забезпечення, можливо, ви встигнете застосувати заходи безпеки або відповісти на загрозу, перш ніж вона буде використана.

– оновлення програмного забезпечення системи. Розробники постійно працюють над тим, щоб постійно оновлювати та виправляти програмне забезпечення, щоб запобігти можливості використання. Коли виявляється вразливість, це лише питання часу, коли вони випустять виправлення. Однак від команди розробників залежить, щоб ваші програмні платформи постійно оновлювались. Найкращий підхід - увімкнути автоматичне оновлення, щоб програмне забезпечення оновлювалось регулярно і без необхідності втручання вручну.

– застосування додаткових заходів безпеки. Необхідно переконання, що використовуються рішення безпеки, які захищають від атак з нульовим днем, оскільки цих заходів безпеки може бути недостатньо, щоб повністю захистити вас від атак з нульовим днем.

Однак, усі ці заходи, на сьогоднішній день, виконуються вручну адміністраторами, або лише частково автоматизовані. Тому, для захисту від таких атак, можливо два взаємно доповнюваних підходи:

– автоматизація відстеження інформації про наявні вразливості. Це досягається створенням програмного забезпечення, яке контролює підписки на отримання інформації, або самостійно оброблює відповідні ресурси;

– автоматизація відстеження, перевірки та здійснення оновлень системи, зокрема оновлень безпеки;

– використання спеціалізованих систем виявлення вторгнень, функціонування яких не засноване на виявленні шаблонів поведінки мережевих об’єктів, а використовує адаптивні алгоритми оцінки поведінки в мережі.

Основними особливостями та перевагами таких систем є:

- контроль та аналіз діяльності користувача та системи;
- аудит системних файлів та інших конфігурацій та операційної системи;
- оцінює цілісність файлів системи та даних;
- проведення аналізу закономірностей на основі відомих атак;
- виявлення помилок в конфігурації системи;
- виявлення та попередження, якщо системі загрожує небезпека.

1.1.1 Аналіз існуючих рішень виявлення вторгнень

Моделі систем виявлення вторгнень визначаються класифікованими за декількома напрямками.

Мережеві системи виявлення вторгнень контролюють трафік в окремих мережах або підмережах шляхом постійного аналізу трафіку та порівняння його з відомими атаками в бібліотеці. У разі виявлення атаки сповіщення надсилається системному адміністратору. Він розміщується здебільшого у важливих точках мережі, щоб він міг стежити за трафіком, що прямує до різних пристроїв мережі та з них. Система розміщується вздовж межі мережі або між мережею та сервером. Перевагою цієї системи є те, що її можна

легко розгорнути і з низькою вартістю без необхідності завантаження для кожної системи.

Система виявлення вторгнень хоста: система працює на окремих системах, де постійно контролюється мережеве підключення до системи, тобто вхідні та вихідні пакети, а також проводиться аудит системних файлів, і у разі будь-яких розбіжностей адміністратор системи попереджається приблизно те саме. Ця система контролює операційну систему комп'ютера. IDS інстальована на комп'ютері. Перевага цієї системи полягає в тому, що вона може точно контролювати всю систему і не вимагає встановлення будь-якого іншого обладнання.

Система виявлення вторгнень господаря. Виходячи з методу роботи: система виявлення вторгнень на основі підписів: Ця система працює за принципом узгодження. Дані аналізуються і порівнюються з підписом відомих атак. У разі будь-якої відповідності видається попередження. Перевага цієї системи полягає в тому, що вона має більшу точність і стандартні сигнали тривоги, зрозумілі користувачеві.

Система виявлення вторгнень на основі аномалій: вона складається із статистичної моделі звичайного мережевого трафіку, яка складається із використовуваної смуги пропускання, протоколів, визначених для трафіку, портів та пристроїв, які є частиною мережі. Він регулярно контролює мережевий трафік і порівнює його зі статистичною моделлю. У разі будь-якої аномалії або розбіжності адміністратор отримує попередження. Перевагою цієї системи є те, що вона може виявляти нові та унікальні атаки.

На основі функціонування системи виявлення вторгнень на основі в аномалій є система пасивного виявлення вторгнень: вона просто виявляє тип роботи зловмисного програмного забезпечення та видає попередження системі або адміністратору мережі. Потім адміністратор вживає необхідних дій.

Система виявлення реактивних вторгнень: вона не тільки виявляє загрозу, але й виконує певні дії, скидаючи підозріле з’єднання або блокуючи

мережевий трафік із підозрілого джерела. Він також відомий як система запобігання вторгненню.

1.1.2 Аналіз рішень запобігання вторгненням до мережі

Системи запобігання вторгнень - це активні вбудовані пристрої, які можуть скидати пакети атаки або відключати з'єднання, перш ніж вони дістануться хоста. IPS фокусується на тому, що робить атака - її поведінці, яка не змінюється. На додаток до використання сигнатур, IPS використовують набір правил, що представляють або допустиму, або шкідливу поведінку. Потім трафік у реальному часі порівнюється з набором правил і допускається, або блокується. IPS виявляють проникнення на основі аналізу стану трафіку, що проходить через них. Пристрій IPS повинен використовувати Stateful Inspection для здійснення розширеного захисту від нових типів атак, а також захисту від зростаючої частоти та масштабів DDoS-атак. Вони виконують повторну збірку сегмента TCP, аналіз трафіку, перевірку протоколу програми та узгодження підписів для ідентифікації атаки. Кожна з цих функцій впливатиме на пропускну здатність мережі в певній мірі, залежно від розміру та можливостей мережі, тому дуже важливо знати поточні потреби та очікувану потребу майбутнього зростання сервісів. У великих корпоративних мережах та системах може виникнути вузьке місце та збої в роботі системи, якщо IPS або пропускна здатність / магістраль мережі не можуть обробити очікувану пропускну здатність. Якщо IPS не вдається, потік пакетів зупиняється і мережа стає недоступною, це те, чого не можна допускати. Отже, існує низка факторів, які необхідно враховувати при розробці IPS. Єдиний ефективний спосіб дізнатись, як пристрій IPS вплине на вашу мережу, - це провести тестування у реальному середовищі. Деякі функції, які були найпоширенішими і полягали у використанні шаблонів підписів для визначення, чи має місце атака. Це, як правило, проблема із блокуванням або моніторингом, коли в мережі дуже великі набори підписів, за якими пристрій IPS повинен встигати; ускладнює утримання затримки. Рішення полягає в тому, щоб переконатися, що вибраний продукт здатний

підтримувати підписи, а також надати добре побудований інтерфейс, який легко зрозуміти та орієнтуватися.

Основним недоліком систем виявлення вторгнень є їх нездатність відрізнити друга від ворога. Користувачі всередині системи можуть мати нешкідливу діяльність, позначену системою виявлення вторгнень, що призводить до блокування мережі на невизначений проміжок часу, доки технічний фахівець не зможе виявити проблему та скинути систему виявлення на місце. Для бізнесу, який залежить від швидких дій щодо матеріалів, орієнтованих на кінцеві терміни, це може призвести до різкої втрати доходу та довіри клієнтів, оскільки партнери можуть передати бізнес в іншу компанію з більш надійною мережею.

1.2 Обмеження систем виявлення та запобігання вторгнень

Системи виявлення вторгнень (IDS) та системи запобігання вторгненню (IPS) вважаються загальнодоступними засобами безпеки. Найпоширеніший тип системи сидить у мережі та перевіряє всі вхідні пакети. IDS / IPS призначені для перевірки вхідних пакетів, щоб перевірити, чи не є вони частиною шкідливої атаки та викиду або попередження про пакети, які є. Але, як і більшість технологій, IDS / IPS мають численні обмеження та підводні камені, які постачальники цих систем не розголошують. Розмірковуючи, як найкраще захистити мережу організації та роботу IDS / IPS, слід врахувати наступні п’ять основних обмежень.

Виявити чи запобігти численним загальним методам атаки. Навіть із встановленим IDS / IPS та постійним моніторингом вхідних мережевих пакетів трафіку існує багато поширених типів атак та методів, які дозволяють уникнути виявлення. Більшість технологій IDS / IPS використовують оцінку пакетів на основі правил або підписів, намагаючись зіставити пакети з відомими шкідливими шаблонами. Проблема цієї методології полягає в тому,

що IDS / IPS необхідно постійно оновлювати, щоб вловлювати останні відомі атаки. Лише кілька обчислюваних змін атаки дозволять уникнути відповідності відомого підпису атаки системи, і часто система не може обробляти зашифровані пакети, які дозволяють зловмисним пакетам просканувати IDS / IPS. На додаток до основних обмежень щодо того, як IDS / IPS виявляє атаки, вони також не можуть виявляти атаки, які покладаються на слабку аутентифікацію. IDS / IPS не може виявити зловмисного актора, що «законно» входить у критичну систему, оскільки паролем користувача адміністратора був пароль123. IDS / IPS краще ловить вхідні атаки, якщо його попередження переглядаються в поєднанні з журналами та попередженнями інших пристроїв, хостів та програм, що працюють у мережі.

Можливість нападу на самі системи. IDS / IPS сприйнятливі до багатьох тих самих атак мережевого протоколу, якими є хости, які він намагається захистити. Найчастіше ці атаки можна використовувати для спроби збою IDS / IPS. У разі успіху хакери можуть здійснити подальші атаки, звільнені від IDS / IPS, які їх турбують.

Налаштування на зменшення кількості помилкових сигналів. Коли IDS / IPS виявить трафік, який він вважає підозрілим, він надішле попередження. Залежно від IDS / IPS, це може бути у формі журналу або повідомлення, яке зазвичай надсилається до центрального управління журналом або системі SIEM. IDS / IPS надсилатиме багато помилкових сповіщень, якщо вони не налаштовані правильно. Налаштування займає багато часу, зусиль та знань доменів конкретного середовища, щоб виправитись, і, як правило, це постійний процес, оскільки середовище змінюється з часом. Навіть найрозумніше програмне забезпечення IDS / IPS, що має можливості навчання, може виконувати лише найосновніші форми само налаштування, що займає багато часу, протягом якого часто буде підніматися помилковий сигнал.

Найбільш досконало налаштовані IDS / IPS з низькою швидкістю помилкової тривоги все ще не можуть допомогти в одній критичній області:

надання вказівок щодо того, як реагувати на вторгнення або спроби вторгнення. Знання того, як реагувати на вторгнення, є не менш важливим для знання про вторгнення. Навіть якщо система є IPS і скидає пакети атаки, все одно може знадобитися вжити заходів реагування, щоб зловмисник не міг повернутися і зробити ще одну успішну спробу вторгнення.

Найкращою системою виявлення та запобігання вторгнень залишається людина, яка здійснює цілодобовий моніторинг журналів мережі та оповіщень, у тому числі з IDS / IPS - вдосконалений брандмауер, якщо людина не переглядає попередження, що надходять від нього. Людина повинна залучатись цілий день щодня, щоб оцінювати попередження IDS / IPS у контексті інших дій у мережі, щоб можна було вжити відповідних заходів проти реальних загроз.

1.3 Сигнатурний аналіз вторгнень

Методи виявлення, що базуються на підписах, використовуються з перших днів моніторингу безпеки. Сканери вірусів використовували підписи для ідентифікації заражених файлів, а найдавніші системи виявлення вторгнень (IDS) значною мірою покладались на визначення підписів. У попередні роки вони забезпечували належний захист, доки супротивники не стали більш просунутими. Погані актори виявили методи ухилення від підписів, залишивши перше покоління систем виявлення, що базуються на підписах, погано обладнаними для захисту організацій від загроз. Намагаючись визначити довгострокове рішення для цих загроз, були створені нові методи пошуку наслідків атак, а не виявлення унікальних характеристик зловмисників. Це забезпечує перевагу потенційного виявлення невідомих загроз, але ця техніка не обходиться без власних викликів.

Виявлення на основі підпису - це процес, коли встановлюється унікальний ідентифікатор відомої загрози, щоб загрозу можна було

ідентифікувати в майбутньому. У випадку антивірусного сканера, це може бути унікальний шаблон коду, який прикріплюється до файлу, або він може бути таким же простим, як хеш відомого поганого файлу. Якщо цей конкретний зразок або підпис буде виявлено знову, файл може бути позначений як заражений. Оскільки зловмисне програмне забезпечення стало більш досконалим, автори зловмисного програмного забезпечення почали використовувати нові методи, такі як поліморфізм, щоб змінювати шаблон кожного разу, коли об’єкт поширюється з однієї системи на іншу. Таким чином, проста відповідність шаблону не була б корисною, окрім невеликої купки виявлених пристроїв. У системах виявлення мережі, таких як IDS, підписи визначаються для пошуку характеристик у мережевому трафіку.

Одним з найпоширеніших методів визначення є Snort - правило сопіння. Правило Snort визначає характеристики в одному або ряді мережевих пакетів для виявлення зловмисної поведінки. Наприклад, правило Snort може бути написане для ідентифікації командно-керуючого (C2) трафіку між зараженим пристроєм та супротивником, незалежно від того, де містяться сервери противника. Незважаючи на те, що противникам складніше затушувати мережеві пакети, щоб уникнути підпису, відносно легко зашифрувати трафік, ускладнюючи процес виявлення.

1.4 Аналіз вторгнень за поведінкою

На відміну від виявлення на основі підписів, аналіз поведінки не займається пошуком унікальних характеристик конкретної загрози, а саме результатами. У виявленні кінцевих точок це означає розгляд того, чого намагається досягти будь-який окремий процес. Незалежно від відбитків пальців, якщо виконуваний файл намагається отримати ескалацію привілеїв, це ні до чого доброго не призведе. Розглядаючи поведінку мережі, це може бути ще складніше. Деякі продукти створюють базову лінію для звичайних

шаблонів руху, а потім викликають попередження про наявність аномалій. Інші намагаються визначити, коли конкретні зв’язки ведуть себе несподівано. Перевага аналізу поведінки полягає в тому, що він має потенціал виявлення невідомих загроз. Одним з побічних ефектів є те, що він схильний до помилкових спрацьовувань. Додатковий контекст допомагає впорядкувати ці результати, але коли хибних спрацьовувань перевершує кількість справжніх виявлення, рішення може спричинити більше проблем, ніж варто. Крім того, аналіз поведінки може бути набагато більш ресурсоємним, тому покладання на нього для виявлення відомих загроз може коштувати дорого і ризикує пропустити загрозу, яку легко визначити за допомогою підпису.

Збалансований і шаруватий захист у глибину. Обидва методи виявлення корисні для збалансованого та багаторівневого захисту кібербезпеки. Принцип Парето («правило 80/20») є корисним контрастом для розуміння того, як вісімдесят відсотків інцидентів у вашому середовищі буде легко ідентифікувати шляхом виявлення на основі підписів. Насправді підписи є найефективнішим методом виявлення відомих загроз, а це означає, що він залишається принципово важливою методологією. З іншого боку, двадцять відсотків питань не можуть бути ідентифіковані підписами, але, ймовірно, спричинять вісімдесят відсотків проблем. Якщо ваша організація зазнає цілеспрямованої атаки, швидше за все, її не буде легко ідентифікувати або відома загроза. Отже, поведінковий аналіз є безсумнівно важливим.

Сучасні засоби захисту кібербезпеки збалансовані та багаторівневі, що означає включення методів виявлення як відомих, так і невідомих загроз. Ефективні організації можуть легко ідентифікувати, запобігти та розподілити відомі загрози, використовуючи рішення на основі підписів - і доповнити цю техніку рішеннями на основі поведінки, щоб уловлювати невідомі загрози, які може пропустити рішення на основі підпису

1.5 Висновки до розділу

В даному розділі було розглянуто типи систем виявлення вторгнень та їх основні механізми, які використовуються в процесі виявлення вторгнення.

При цьому було досліджено наступну класифікацію систем та їх особливості:

– мережеві системи виявлення вторгнення призначені для аналізу трафіку та виявлення певних ознак того, що в мережі виконується вторгнення;

– хостові системи виявлення вторгнень здійснюють контроль на локальному сервері чи хості.

В обох випадках, рішення виявлення вторгнень здійснює аналіз копії трафіку без втручання в структуру трафіку або впливаючи на його інтенсивність. З одного боку це має позитивну ознаку, яка полягає в тому, що немає впливу на оригінальний мережевий трафік. З іншого боку, при такому підході, факт вторгнення може бути виявлений занадто пізно, коли зловмисні дії вже спричинили втрати для системи.

Іншою класифікацією систем виявлення вторгнень є за методом виявлення. В даному випадку визначають два основні варіанти виявлення вторгнень — сигнатурний та поведінковий аналіз.

В першому випадку аналіз здійснюється на основі відомих ознак вторгнення, аналогічно антивірусним програмам. Це дозволяє точно визначати відомі атаки та загрози методом співвідношення цифрового сліду трафіку із відомим шаблоном.

В другому випадку аналіз здійснюється на основі дослідження нормальної роботи мережі чи системи, після чого, в штатному режимі роботи, система визначає аномалії, тобто відхилення від нормальної роботи системи чи мережі.

На основі даного аналізу було визначено наступні особливості систем виявлення вторгнення:

– виявлення вторгнень базується на основі відомих фактів про зловмисні дії людини чи процесу в системі;

– створення шаблонів, як сигнатурних, так і поведінки, вимагають витрат часу, наявності спеціалістів, які здатні створювати маркери для шаблонів, та навчання системи.

Таким чином, в ході аналізу існуючих рішень виявлення вторгнень до комп'ютерних мереж, було визначено, що для оцінки захищеності мереж необхідно розробити моделі, які здатні описувати характерні ознаки вторгнень в мережу з урахуванням невизначеності, що дозволить створювати нечіткі моделі вторгнень. Також прийнято, що створені нечіткі моделі можуть застосовуватись для опису груп атак, які певною міру схожі між собою.

Такий підхід може дати наступні переваги:

– скорочення часу створення сигнатур;

– скорочення часу аналізу мережевого трафіку, за рахунок первинного аналізу приналежності до групи атак, замість точного пошуку відповідності;

– як мінімум збереження точності виявлення вторгнень.

Усе це дозволить вирішити основні задачі дослідження по зменшенню часу аналізу за рахунок уніфікації процесу створення сигнатур та підтримки заданого рівня хибних спрацьовувань системи виявлення, що в свою чергу дасть змогу оцінити ступень захищеності комп'ютерних мереж.

2 АНАЛІЗ МОДЕЛЕЙ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Використання тільки методів виявлення аномалій не гарантує виявлення всіх порушень безпеки, тому в більшості СОВ існує технології розпізнавання зловживань. Виявлення вторгнень-зловживань ґрунтується на прогностичному визначенні атак і подальшим спостереженням за їх появою. На відміну від виявлення аномалії, де образ - це модель нормального поведінки системи, при виявленні зловживання він необхідний для подання несанкціонованих дій зловмисника. Такий «образ» стосовно виявлення зловживань називається сигнатурою вторгнення. Формується сигнатура на основі тих самих вхідних даних, що і при виявленні аномалій, тобто на значеннях параметрів оцінки. Сигнатури вторгнень визначають оточення, умови і спорідненість між подіями, які призводять до проникнення в систему або будь-яким іншим зловживанням. Вони корисні не тільки при виявленні вторгнень, але і при виявленні спроб здійснення незаконних дій. Частковий збіг сигнатур може означати, що в системі, що захищається мала місце спроба вторгнення.

2.1 Використання умовної ймовірності

Для визначення зловживань потрібно визначити умовну ймовірність:

P (Вторгнення | Патерн подій).

Тобто, іншими словами, визначається ймовірність того, що якісь безліч або безлічі подій є діями зловмисника.

Далі використовується формула Байеса

$$P(I \mid A_1, A_2, \ldots, A_n) = P(A_1, A_2, \ldots, A_n \mid I) \frac{P(I)}{P(A_1, A_2, \ldots, A_n)} \quad (9)$$

де I - вторгнення, а A1 ... An - послідовність подій. Кожна подія - це сукупність параметрів оцінки захищається системи.

Для прикладу розглянемо мережу університету як систему, для якої необхідно визначити умовну ймовірність вторгнення. Експерт безпеки, що працює з таким типом мереж, може, використовуючи свій досвід, визначити емпіричний кількісний показник - ймовірність вторгнення P (вторгнення) = P (I). Далі, якщо всі звіти про вторгнення і попередніх їм події в подібних мережах звести до табличного вигляду, можна визначити наступну умовну ймовірність:

P (A1 ... An | I) = P (Послідовність подій | Вторгнення).

Аналізуючи безліч записів аудиту без вторгнень, можна отримати P (Послідовність подій | ¬Вторгнення). Використовуючи ці дві умовні ймовірності, можна легко визначити ліву частину рівняння Байеса

$$P(sequence) = (P(ES \mid \neg I) - P(ES \mid \neg I))P(I) + P(ES \mid \neg I) \quad (10)$$

де *sequence* - послідовність подій; ES - виступає як послідовність подій, а I – вторгнення

2.2 Продукційні та експертні системи

Головна перевага використання продукційних систем полягає в можливості поділу причин і рішень виникаючих проблем.

Приклади використання таких систем в СОВ описані досить широко. Така система кодує інформацію про вторгнення в правилах умовного виду: if (якщо) причина then (то) рішення, причому при додавання правил причина відповідає події, що реєструються підсистемою збору інформації СОВ. У частині правила кодуються умови (причини), необхідні для атаки. Коли всі умови в лівій частині правила задоволені, виконується дія, задана в правій його частині.

Основні проблеми додатків, що використовують даний метод, які зазвичай виникають при їх практичному застосуванні:

– недостатня ефективність при роботі з великими обсягами даних;

– важко врахувати залежну природу даних параметрів оцінки.

При використанні продукційних систем для виявлення вторгнень можна встановити символічний прояв вторгнення за допомогою наявних даних.

Використання даних систем також може бути пов’язане з наступними труднощами:

– відсутність вбудованої або природної обробки порядку послідовностей в аналізованих даних. База фактів, відповідна лівій частині «продукції», використовується для визначення правій частині. У лівій частині продукційного правила всі елементи об'єднуються за допомогою зв'язку «і».

– вбудована експертиза може бути доброю лише в тому випадку, якщо модельовані навички адміністратора безпеки не суперечливі. Це практичне міркування, можливо, стосується браку централізованості зусиль експертів безпеки в напрямку створення вичерпних множин правил:

– виявляються лише відомі вразливості;

– існує певний програмний інжиніринг, пов'язаний з установкою (підтримкою) баз знань. При додаванні або видаленні будь-якого з правил повинно змінюватися інші безлічі правил;

− об'єднання різних вимірів вторгнень і створення пов'язаної картини вторгнення призводить до того, що приватні причини стають невизначеними. Обмеження продукційних систем, в яких використовується невизначена причина, добре відомі.

2.3 Аналіз зміни станів

Цей метод був описаний в STAT і реалізований в USTAT. Сигнатура вторгнення представляється як послідовність переходів між станами системи, що захищається. Патерни атаки (сукупність значень параметрів оцінки) відповідають якомусь стану системи і мають пов'язану з ними логічну функцію. Якщо ця функція виконується, то вважається, що система перейшла в цей стан. Наступні стани з'єднані з поточним лініями, які представляють собою необхідні події для подальших переходів. Типи можливих подій вбудовані в модель і відповідають значенням параметрів оцінки за принципом один до одного [10, 11].

Патерни атаки можуть тільки задати послідовність подій, тому більш складний спосіб визначення подій не підтримується. Більш того, відсутній загальний механізм цілей, які можна було б використовувати для визначення часткової відповідності атак, замість цього використовується проста вбудована логічна функція.

2.4 Спостереження за вводом даних

Для виявлення атак в даній технології використовується моніторинг за натисканням користувача на клавіші клавіатури. Основна ідея - послідовність натиснень користувача задає патерн атаки. Недоліком цього підходу є відсутність досить надійного механізму перехоплення роботи з клавіатурою

без підтримки операційної системи, а також велика кількість можливих варіантів представлення однієї і тієї ж атаки. Крім того, без семантичного аналізатора натискань різного роду псевдоніми команд можуть легко зруйнувати цю технологію. Оскільки вона спрямована на аналіз натискань клавіш, автоматизовані атаки, які є результатом виконання програм зловмисника, також можуть бути не виявлені.

2.5 Методи, засновані на моделюванні поведінки зловмисника

Одним з варіантів виявлення зловживання є метод об'єднання моделі зловживання з очевидними причинами. Його суть полягає в наступному: є база даних сценаріїв атак, кожна з яких об'єднує послідовність поводжень, що становлять атаку. У будь-який момент часу існує можливість того, що в системі має місце одне з цих підмножин сценаріїв атак. Робиться спроба перевірки припущення про їхню наявність шляхом пошуку інформації в записах аудиту. Результатом пошуку є якась кількість фактів, достатню для підтвердження або спростування гіпотези. Перевірка виконується в одному процесі, який отримав назву антісіпатор. Антісіпатор, ґрунтуючись на поточній активної моделі, формує наступну можливу безліч поводжень, яку необхідно перевірити в записах аудиту, і передає їх планувальнику. Планувальник визначає, як передбачувана поведінка відбувається в записах аудиту і трансформує їх у системно-аудіто-залежний вираз. Ці вирази повинні складатися з таких структур, які можна було б просто знайти в записах аудиту, і для яких була б досить висока ймовірність появи в записах аудиту.

У міру того як підстави для підозр деяких сценаріїв накопичуються, а для інших - знижуються, список моделей активностей зменшується. Обчислення причин вбудовано в систему і дозволяє оновлювати ймовірність появи сценаріїв атак в списку моделей активності.

Переваги:

– з'являється можливість зменшити кількість істотних обробок, необхідних для одного запису аудиту; спочатку спостерігаються більш «грубі» події в пасивному режимі, і далі, як тільки одне з них виявлено, спостерігаються більш точні події;

– планувальник забезпечує незалежність подання від форми даних аудиту.

Недоліки:

– при застосуванні даного підходу у особи, відповідальної за створення моделі виявлення вторгнення, з'являється додаткове навантаження, пов'язана з призначенням змістовних і точних кількісних характеристик для різних частин графічного представлення моделі;

– ефективність цього підходу була продемонстрована створенням програмного прототипу; з опису моделі не ясно, як поведінки можуть бути ефективно складені планувальнику, і який ефект це матиме на систему під час роботи;

– цей підхід доповнює, але не замінює підсистему виявлення аномалій.

Недоліки сучасних систем виявлення можна розділити на дві групи - недоліки, пов'язані зі структурою СОВ, і недоліки, що відносяться до реалізованих методів виявлення.

Ефективність. Часто методи системи намагаються виявити будь-яку зрозумілу атаку, що призводить до ряду незадовільних наслідків. Наприклад, при виявленні аномалій істотно споживаються ресурси - для будь-якого профайла потрібні оновлення для кожного з спостережуваних подій. При виявленні зловживань зазвичай використовуються командні інтерпретатори експертних систем, за допомогою яких кодуються сигнатури. Дуже часто ці командні інтерпретатори обробляють свою власну безліч правил і, відповідно, також споживають ресурси. Більш того, безліч правил допускає лише непрямі залежні послідовності зв'язків між подіями.

Портативність. До цих пір більшість СОВ створюється для використання на конкретному обладнанні, і досить важко використовувати їх в іншій системі, де потрібно реалізувати схожу політику безпеки. Наприклад, завдання з переміщення СОВ із системи, в якій підтримується тільки одноріневий список доступу, в систему з багаторівневою досить складне, і для його вирішення потрібні значні доробки. Основною причиною цього є те, що багато СОВ спостерігають за певними пристроями, програмами конкретної ОС. Також слід зауважити, що кожна ОС розробляється для виконання конкретних завдань. Отже, переорієнтувати СОВ на інші ОС досить складно, за винятком тих випадків, коли ОС розроблені в якомусь загальному стилі.

Право на оновлення. Дуже складно відновити існуючі системи новими технологіями виявлення. Нова підсистема повинна взаємодіяти з усією системою, і часом неможливо забезпечити універсальну можливість взаємодії.

Для установки СОВ дуже часто потрібні додаткові навички, істотно відрізняються від навичок в області безпеки. Наприклад, для поновлення безлічі правил в системах виявлення зловживань потрібні спеціалізовані знання експертної системи. Подібне можна сказати і про статичні вимірювання системи виявлення аномалій.

Продуктивність і допоміжні тести - важко оцінити продуктивності СОВ в реальних умовах. Більш того, відсутня загальний набір правил для тестування СОВ, на підставі яких можна було сказати про доцільність використання даної системи в конкретних умовах і отримати якісь кількісні показники.

Відсутність хороших способів тестування.

Недоліки методів систем виявлення:

– неприпустимо високий рівень помилкових спрацьовувань і пропусків атак;

– слабкі можливості по виявленню нових атак;

– більшість вторгнень неможливо визначити на початкових етапах;

– важко, іноді неможливо, визначити атакуючого, цілі атаки;

– відсутність оцінок точності і адекватності результатів роботи;

– неможливо визначати «старі» атаки, що використовують нові стратегії;

– складність виявлення вторгнень в реальному часі з необхідною повнотою в високошвидкісних мережах;

– слабкі можливості з автоматичним виявленням складних координованих атак;

– значне перевантаження систем, в яких функціонують СОВ, при роботі в реальному часі;

Подальші напрямки вдосконалення пов'язані з впровадженням в теорію і практику СОВ загальної теорії систем, методів теорії синтезу та аналізу інформаційних систем і конкретного апарату теорії розпізнавання образів, так як ці розділи теорії дають конкретні методи дослідження для області систем СОВ.

До цього часу не описано СОВ як підсистема інформаційної системи в термінах загальної теорії систем. Необхідно обґрунтувати показник якості СОВ, елементний склад СОВ, її структура та взаємозв'язок з інформаційною системою.

У зв'язку з наявністю значної кількості факторів різної природи, функціонування інформаційної системи та СОВ має вірогідний характер. Тому актуальним є обґрунтування виду вірогідних законів конкретних параметрів функціонування. Особо слід виділити завдання обґрунтування функції втрати інформаційної системи, заданої відповідно до її цільової функції та області параметрів функціонування системи. При цьому цільова функція повинна бути визначена не тільки на експертному рівні, але й у відповідності з сукупністю параметрів функціонування всієї інформаційної системи та задачами, що покладаються на неї. Тоді показник якості СОВ буде

визначатися як один з параметрів, що впливають на цільову функцію, а його допустимі значення - допустимі значеннями функції втрати.

Після обґрунтування законів та функцій реальної задачі є отримання формалізованими методами оптимальної структури СОВ у вигляді сукупності математичних операцій. Таким чином, задача синтезу структури СОВ може бути вирішена. На основі отриманих математичних операцій можна розрахувати залежності показників якості функціонування СОВ від параметрів її функціонування, а також від параметрів функціонування інформаційної системи, тобто буде можливим реальний аналіз якості функціонування СОВ.

Складність застосування до СОВ формалізованого апарату аналізу та синтезу інформаційних систем полягає в тому, що конкретні інформаційні комплекси та його підсистеми СОВ складаються з різнорідних елементів, які можуть бути описані різними розділами теорії (системи масового обслуговування, кінцеві автомати, теорія ймовірностей, теорія розпізнавання образів та т.д), то є, об'єкт дослідження є агрегативним. Тому математичні моделі можна отримати тільки для окремих складових частин СОВ, що ускладнює аналіз і синтез СОВ в цілому, але подальша конкретизація застосування формалізованого аналізу та синтезу дозволить оптимізувати СОВ.

На підставі викладеного можна зробити висновок про те, що в практичній діяльності накопичений значний досвід вирішення проблем виявлення вторгнень. Популярні системи СОВ в значній мірі будуються на емпіричних схемах виявлення вторгнень, подальше вдосконалення СОВ пов'язано з конкретизацією методів синтезу та аналізу складних систем, теорії розпізнавання образів у застосуванні до СОВ.

2.6 Висновки до розділу

Існує велика кількість реалізацій систем виявлення вторгнень (СОВ), які мають свої переваги та недоліки. Серед систем, використання яких відходіть на задній план можна назвати сигнатурні методи. Використання шаблонів атак та зловмисного програмного забезпечення не є остаточно бездієвим підходом до виявлення вторгнень, але не захищає мережі та системи від атак, які були модифіковані, або взагалі знов розроблені. Отже, використання сигнатурних методів та моделей може використовуватись як перша лінія захисту від вторгнень.

Найбільш перспективними сучасними методами виявлення вторгнень є використання моделей з нечіткою логікою, машинного навчання та аналізу великих даних.

Використання моделей обробки великих даних надає інструменти для обробки та візуалізації журналів події з множини пристроїв та систем, які надсилаються до системи моніторингу у режимі реального часу. Такі дані перетворюються в спеціальні датасети, які в подальшому можуть виступати як вхідні дані у системах машинного навчання та систем висновків.

Машинне навчання дозволяє автоматизувати обробку великих даних та класифікувати події в інформаційних системах та мережах. Такі системи можуть бути першим ланцюгом в центрах кібербезпеки та захисту інформації, де в першу чергу необхідно приймати рішення про наявність інцидентів безпеки на цільовій системі чи її відсутності. Такий підхід дозволяє скоротити час аналізу та підвищити продуктивність аналізу інцидентів.

Нечіткі системи дозволяють автоматизувати аналіз вторгнень на так званих розмитих випадках, коли неможливо події в системі визначити до конкретної категорії інцидентів чи загроз.

3 МОДЕЛІ ВИЗНАЧЕННЯ ВТОРГНЕННЬ НА ОСНОВІ СЦЕНАРІЇВ ТА ЗАГРОЗ

В ході магістерського дослідження було виявлено, що основними факторами, які впливають на виникнення вторгнень в комп'ютерну мережу та призводять до порушення інформаційної безпеки є інциденти, які виникають в системі, а також ступінь шкоди у випадку їх реалізації. Ступінь шкоди при цьому, може бути заданий з використанням ступеня впливу, а оцінку інциденту необхідно визначити з використанням множини взаємозалежних параметрів. Для того, щоб визначити інциденти, необхідно оцінити сценарії, реалізація яких призводять до виникнення загроз і інцидентів, котрі сприяють реалізації даних сценаріїв.

Моделі загроз, які сприяють виникненню небезпеки та моделі атак, які сприяють виникненню інцидентів в мережі використовуються для виявлення вторгнень у мережі завчасно до їх виникнення або під час їх реалізації. При цьому, в процесі аналізу, важливо зосереджуватись не тільки на конкретних атаках, а й визначати характерні властивості груп атак. Такий підхід дозволяє здійснювати класифікацію сценаріїв по певним критеріям, та виявляти мережеві вторгнення, спираючись на інформацію про загальне сімейство атак, а не намагатись визначати конкретну атаку.

Сценарії загроз або атак описують процеси, які протікають в інформаційній системі або мережі. Дані сценарії здійснюються під впливом виникнення певних загроз або групи загроз, і надають можливість описувати послідовність дій, які протікають в мережі та призводять до виникнення інцидентів безпеки.

Враховуючи специфічність протікання атак в мережі, було виявлено чотири основні типи сценаріїв, які характеризують їх з позиції IT-загроз:

– безпосередні атаки. Тип сценаріїв, який описує послідовність дій по реалізації вразливостей, вірусів, дій інсайдерів та ін. Основною відмінністю особливістю даних сценаріїв є процес опису послідовності дій, які сприяють реалізації даних сценаріїв;

– помилковість дій. Даний тип опису сценаріїв дозволяє визначати помилкові дії або повну бездіяльність користувачів мережі, які можуть бути пов'язані з недостатньою кваліфікацією або компетентністю користувачів, кваліфікацією інженерів та адміністраторів і т. п. В даному випадку, у зв’язку характерними особливостями даних сценаріїв, виконується оцінювання на основі певних показників ймовірності виникнення конкретних помилок;

– програмні та апаратні збої. В даному типі сценаріїв здійснюється опис системних збоїв, які можуть виникати під впливом випадкових або спеціальних внутрішніх або зовнішніх факторів. В даному типі сценаріїв, на відміну від помилок, описується нечітка оцінка очікування збою;

– відмови. Відрізняються від збоїв тривалими періодами бездіяльності об'єкта або його повним виходом з ладу.

Способи моделювання комп'ютерних атак, які відомі на даних момент, в більшості, спираються на ймовірнісні методи опису процесів порушення безпеки. Однак, як було виявлено в ході дослідження, такі варіанти опису не завжди повністю виправдовує себе, у зв'язку з тим, що дані оцінки мають апріорний характер, або вимагають використання умовної ймовірності. Також, ймовірнісні підходи не дозволяють оцінювати процеси в умовах обмежених знань про характер протікання атаки. Все це дає можливість ефективно оцінити сценарії, які здійснюються в умовах невизначеності та постійної загрози.

Беручі до уваги такі складності, було прийняте рішення використовувати нечітку логіку, а саме, нечіткі множини та числа, в якості математичного апарату для моделювання характеристик протікання атак.

3.1 Невизначеність параметрів вторгнень

В ході надання опису невизначених та нечітких параметрів атаки виникає необхідність описувати розмиті значення, які вони приймають в процесі реалізації моделі. Для уникнення багатозначності трактування семантичних характеристик одного й того самого параметру в ситуаціях, які відрізняються, було побудовано так званий повний ортогональний семантичний простір, який дозволить в подальшому визначати області нечітких значень усіх параметрів незалежно від розглянутої системи.

Для проектування повного ортогонального семантичного простору (ПОСП) певного нечіткого параметру P можна визначити множину нечітких значень $D_i = \{p_i^k\}_{k=1..K_i}$, в якої K_i – це кількість нечітких значень, які приймає *i*-й параметр, при описі нечітких чисел з використанням трикутної функції приналежності, яка позитивно визначена на інтервалі (p_{ib}^k, p_{ie}^k), де $p_{ib}^k, p_{ie}^k \in D$ - граничні значення початку та кінця інтервалу відповідно, а D_i – це базова множна нечітких значень параметра p_i. Для того, щоб побудовані множини D_i визначалися як ПОСП, необхідно, щоб вони задовольняли наступним аксіомам.

Припустимо, що параметру p_i відповідає набір певних чисел $\{a_{ij}\}_{j=0}^n$, який можна визначити відношенням

$$a_{ij} = a_i + \frac{(b_i - a_i)}{n_i} j, j = 0 \ldots n_i, \quad (3.1)$$

де $D_i = [a_i, b_i]$ – деякий носій множини, заданий на дійсній осі, а n_i – ціле число

З використанням даного набору чисел з (3.1) можна побудувати повний ортогональний семантичний простір $_A(i)$, терми якого визначаються формулою

$$A_{ij} = \left\{ \begin{array}{c} (a_i, a_i, a_{i1}), j = 0 \\ (a_{ij-1}, a_{ij}, a_{ij+1}), 1 \le i < n_i \\ \left(a_{in_i} - 1, a_{in_i}, a_{in_i} + 1\right), i = n_i \end{array} \right\} \quad (3.2)$$

В даній системі, значення $A = (a_{min}, a, a_{max})$ визначають трикутне нечітке число, функція приналежності $\mu_A(x)$ якого визначається за наступною формулою

$$\mu_A(x) = \left\{ \begin{array}{c} 0, x < a_{min}, x > a_{max}, \\ \frac{x - a_{min}}{a - a_{min}}, a_{min} \le x \le a, \\ 1, x = a \\ \frac{a_{max-x}}{a_{max} - a}, a \le x \le a_{max} \end{array} \right\} \quad (3.3)$$

У загальному випадку, нечітке трикутне число $S_i = (s_{i,min}, s_i, s_{i,max})$, яке описує визначені значення параметрів p_i, не співпадатиме з жодним з нечітких значень з ПОСП $_A$. Для визначення ступеню відповідності визначеного значення будь-якого з нечітких значень з ПОСП $_A$, можна використовувати довільні метричні відносини.

В наступному виразу задається матрична форма

$$f_d(A_{ij}, S_i) \quad (3.4)$$

де $f_d(A_{ij}, S_i) = |s_i - a_{ij}|$

В такому випадку можна стверджувати наступне.

Теорема 1. Нехай дане ПОСП $_A(i)$ визначене співвідношеннями (3.2). А відповідність нечіткого трикутного числа $S_i = (s_{i,min}, s_i, s_{i,max})$, нечіткому значенню A_{ij} из ПОСП $_A(i)$, встановлюється за допомогою відношень (3.3)-(3.4). Тоді нечітке число $S_i(\ )$ визначається за допомогою відношення

$$S_i(\ ) = \left\{ \begin{array}{l} A_{i,\left[\frac{s_i - a_i}{b_i - a_i} n_i\right]+1}, \frac{s_i - a_i}{b_i - a_i} n_i - \left[\frac{s_i - a_i}{b_i - a_i} n_i\right] > 0.5 \\ A_{i,\left[\frac{s_i - a_i}{b_i - a_i} n_i\right]}, \frac{s_i - a_i}{b_i - a_i} n_i - \left[\frac{s_i - a_i}{b_i - a_i} n_i\right] \le 0.5 \end{array} \right\}$$

Застосовуючи отриманий результат можна описати кілька допоміжних моделей.

Позначимо через $x = \{x_b, x, x_e\}$, $y = \{y_b, y, y_e\}$ и $z = \{z_b, z, z_e\}$ деякі нечіткі числа с функціями приналежності виду (3). Тоді відповідно можна написати

$$z = x@y = \alpha z_\alpha = \alpha x_\alpha @ y_\alpha \qquad (3.5)$$

де $x_\alpha, y_\alpha, z_\alpha - \alpha$ - рівні нечітких значень x, y, z відповідно, а символом @ визначається один з символів. При цьому справедливі наступні відношення

$$x_\alpha + y_\alpha = \{x_{\alpha b} + y_{\alpha b}, x_{\alpha e} + y_{\alpha e}\}$$

$$x_\alpha - y_\alpha = \{x_{\alpha b} - y_{\alpha b}, x_{\alpha e} - y_{\alpha e}\}$$

$$x_\alpha * y_\alpha = \left\{ \begin{array}{l} min(x_{\alpha b} * y_{\alpha b}, x_{\alpha b} * y_{\alpha e}, x_{\alpha e} * y_{\alpha b}, x_{\alpha e} * y_{\alpha e}) \\ max(x_{\alpha b} * y_{\alpha b}, x_{\alpha b} * y_{\alpha e}, x_{\alpha e} * y_{\alpha b}, x_{\alpha e} * y_{\alpha e}) \end{array} \right\}$$

$$\frac{x_\alpha}{y_\alpha} = \frac{x_\alpha * 1}{y_\alpha} = \left\{ min\left(\frac{x_{\alpha b}}{y_{\alpha b}}, \frac{x_{\alpha e}}{y_{\alpha b}}, \frac{x_{\alpha b}}{y_{\alpha e}}, \frac{x_{\alpha e}}{y_{\alpha e}}\right) max\left(\frac{x_{\alpha b}}{y_{\alpha b}}, \frac{x_{\alpha e}}{y_{\alpha b}}, \frac{x_{\alpha b}}{y_{\alpha e}}, \frac{x_{\alpha e}}{y_{\alpha e}}\right) \right\} \qquad (3.6)$$

З огляду на трикутність функцій приналежності, можна (3.6) з врахуванням (3.5) переписати в наступному вигляді

$$z = x + y = \{x_b + y_b, x + y, x_e + y_e\}$$
$$z = x - y = \{x_b - y_b, x - y, x_e - y_e\}$$
$$z = x * y = \{x_b * y_b, x * y, x_e * y_e\}$$
$$z = x / y = \{x_b / y_b, x / y, x_e / y_e\}$$

Модель 1. При заданій безлічі вхідних параметрів $X = \{x_i\}$, $A = \{a_i\}$, $X \cap A = \varnothing$ і вихідний параметр *y*, причому, кожен параметр є нечітким і його значення описується функцією приналежності типу (3.3). В такому випадку кожен параметр повинен визначається трьома значеннями

$$x = \{x_{ib}, x_i, x_{ie}\}$$
$$a = \{a_{ib}, a_i, a_{ie}\}$$
$$y = \{y_b, y, y_e\}$$

У разі, коли відображення має наступний вигляд

$$y = \sum_i a_i x_i$$

та застосовуючи для вирішення системи співвідношення (3.6) та вирази (3.3-3.5) можна отримати нечітке значення для параметру *y*, яке визначається наступним виразом

$$f_d\left(y^k, y^{'}\right)$$

$y^{'}$ представлене нечітким трикутним числом, яке визначається наступним співвідношеннями

$$y^{'} = \left(\sum_i a_{ib} x_{ib}, \sum_i a_i x_i, \sum_i a_{ie} x_{ie} \right)$$

Модель 2. При заданій безлічі вхідних параметрів и вихідному параметри $\tilde{y}$, кожен з яких є нечітким і його значення визначено функцією приналежності, кожен параметр буде визначається наступними чотирма значеннями

$$x_i = \{x_{ib}, x_i, x_{ie}\},$$
$$a_i = \{a_{ib}, a_i, a_{ie}\},$$
$$y_i = \{y_{ib}, y_i, y_{ie}\}.$$

У випадку, коли вихідне відображення параметрів має вигляд

$$y = \frac{1}{\sum_i a_i} \sum_i a_i x_i$$

та застосовуючи для нього співвідношення (3.3-3.4) можна отримати нечітке значення параметра $\widetilde{y}$, яке визначається наступним виразом

$$f_d \left(y_i^k, y^{'} \right)$$

$y^{'}$ нечітке трикутне значення, яке визначається наступним чином

$$y^{'} = (z_2, z_3, z_1)$$

де $z_1 = \frac{1}{\sum_i a_{ib}} \sum_i a_{ie} x_{ie}$, $z_2 = \frac{1}{\sum_i a_{ie}} \sum_i a_{ib} x_{ib}$, $z_3 = \frac{1}{\sum_i a_i} \sum_i a_i x_i$

Модель 3. При заданій множині вхідних параметрів $\{fx_1, fx_2\}$, і вихідному параметрі *fy*, де кожен з параметрів є нечітким і його значення визначається функцією приналежності типу (3.3), кожен параметр буде визначатися трьома значеннями

$$fx_i = \{x_{ib}, x_i, x_{ie}\}, i = 1,2,$$
$$fy = \{y_b, y, y_e\}.$$

У випадку, коли вихідне відображення параметрів має наступний вигляд:

$$fy = \frac{fx_1 fx_1 + fx_1 fx_2 + fx_2 fx_2}{fx_1 + fx_2}$$

та застосовуючи для такого співвідношення вирази, можна отримати наступні нечіткі характеристики параметру, які визначається наступним чином:

$$f_d\left(y_i^k, y_i'\right).$$

це нечітке трикутне число, яке визначено наступним співвідношеннями

$$y' = \left(z_2, z_3, z_1\right)$$

де, $z_1 = x\left|1bx_{1b} + x_{1b}x_{2b} + x_{2b}x_{2b}\right. / x\left|1e + x_{2e}\right.$,

$$z_2 = x\left|1x_1 + x_1x_2 + x_2x_2\right. /\left(x_1 + x_2\right),$$

$$z_2 = x\left|1ex_{1e} + x_{1e}x_{2e} + x_{2e}x_{2e}\right. /\left(x_{1b} + x_{2b}\right).$$

3.2 Моделювання послідовностей вторгнень

Для оцінки сценаріїв вторгнень здійснюється моделювання послідовностей їх реалізації з використанням нечітких характеристик процесів їх функціонування.

Враховуючи, що атаки на систему представлені послідовністю певних дій, необхідно визначити інструментальні та програмні засоби, які дозволять описувати ці послідовності, а також використовувати нечіткі параметри при описі здійснення сценарію. В ході дослідження, для цього, було запропоновано використовувати нечіткі часові мережі Петрі, що дозволило описати характеристики атак з позиції їх нечіткого характеру протікання та здійснити оцінювання ймовірності їх реалізації.

При побудові ланцюгів атак було визначено, що кожні етапи при реалізації атаки взаємодіють за двох варіантів - паралельно і послідовно. В мережах Петрі дану взаємодію можна описати алгебраїчною лінійною сумою, якщо проводиться описання послідовних етапів, і складаною структурою якщо описуються паралельні шаги виконання атаки. При описі заданих варіантів взаємодій необхідно використовувати визначені специфічні операцій над нечіткими числами. Зважаючи на це, в ході дослідження, було описано для використання трьох типів операцій.

Перший тип операцій визначає отримання значення нечітких лінійних сум характеристик, які характерні при послідовній реалізації етапів виконання сценарію загрози

$$\tau_k = \sum \tau_{ij} =$$

де τ_{ij} – значення нечіткого числа,

α_{ij} – ліва границя числа,

β_{ij} – права границя числа

Другий варіант опису операцій сценаріїв дозволяє обчислювати вирази двох параметрів

$$\tau_k = \tau_1 * \tau_2 = \{\tau_1 * \tau_2, \tau_1\alpha_2 + \tau_2\alpha_1, \tau_1\beta_2 + \tau_2\beta_1\}.$$

Було визначено, що типовим завданням в моделюванні сценаріїв є множення тільки двох параметрів і інші випадки виходять за рамки даного дослідження.

Третій тип операцій визначає розподіл нечітких чисел:

$$\tau_k = \frac{\tau_1}{\tau_2} =$$

Визначивши заміну фрагментів $\tau_1\alpha_2 + \tau_2\alpha_1$ та $\tau_1\beta_2 + \tau_2\beta_1$ на α_{21} та β_{21} відповідно, попередні два вираження можна представити наступним чином

$$\tau_k = \tau_1 * \tau_2 = \{\tau_1 * \tau_2, \alpha_{21}, \beta_{21}\},$$

$$\tau_k = \frac{\tau_1}{\tau_2} = \left\{\frac{\tau_1}{\tau_2}, \alpha_{21} / \tau_2^2, \beta_{21} / \tau_2^2\right\}.$$

Використання усіх визначених типів операцій дозволяє описувати параметри виконання паралельних етапів реалізації загроз, де використовуються всі зазначені вище операції.

Мережа Петрі будується для визначення відповідних етапів атаки і представляється в графічному вигляді (рисунок 3.1). Звичайні часові мережі Петрі дозволяють, з використанням матриць спрацьовування переходів і диференціальних рівнянь обчислювати час переходу маркеру події по всій мережі і визначити ймовірність здійснення атаки.

Кожний стан S_i та відповідний перехід t_j визначають часові характеристики τ_ij, які характеризують час виконання відповідного етапу.

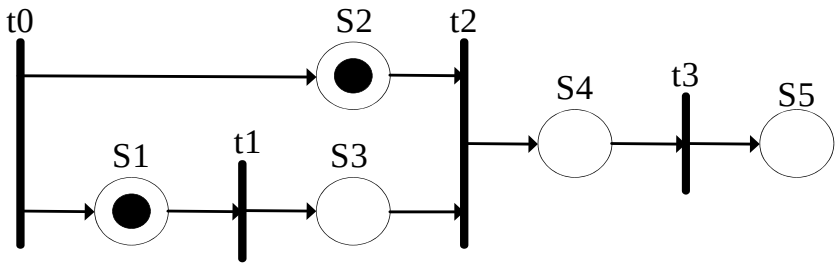

Рисунок 3.1 – Приклад моделі сценарію DoS атаки

Розглядаючи даний приклад зазначеної моделі атаки, підсумковий вираз для обчислення загального часу проходу маркеру по мережі наступний:

$$\tau_1 = \tau_{11} + \tau_{32}$$

$$\tau_2 = \frac{\tau_1^2 + \tau_1\tau_{22} + \tau_{22}^2}{\tau_1 + \tau_{22}}$$

$$\tau = \tau_2 + \tau_{43}$$

В ході складання виразу доцільно виконати його декомпозицію на окремі частини, які реалізують опис паралельного та послідовного взаємозв’язків між складовими елементами вторгнення.

Однак, використання класичних мереж Петрі накладає певні обмеження - параметри τ_ij задаються точними значеннями або усереднюються, що, в свою чергу, знижує загальну точність кінцевого результату моделі. До того ж, не завжди є можливість визначити точні параметри здійснення дій для опису в моделі, за умов невизначеності окремих етапів процесів атаки. Для вирішення таких складностей, в дослідженні було запропоновано використовувати наближенні значення та оцінки параметрів, які описують послідовність здійснення вторгнень.

$$\tau_{ij}(HSD) = \lfloor a_{ij}(HSD), b_{ij}(HSD) \rfloor,$$

де a_{ij}, b_{ij} – носій нечіткої множини відповідного параметру вторгнення

За таких умов опису, час повного переходу маркеру атаки по мережі можна описати наступною системою обчислень

$$\tau_1(HSD) = \tau_{11}(HSD) + \tau_{32}(HSD)$$

$$\tau_1(HSD) = \frac{\tau_1^2(HSD) + \tau_1(HSD)\tau_{22}(HSD) + \tau_{22}^2(HSD)}{\tau_1(HSD) + \tau_{22}(HSD)}$$

$$\tau(HSD) = \tau_2(HSD) + \tau_{43}(HSD)$$

де $\tau_{ij}(HSD)$ - одне із значень з носія $\lfloor a_{ij}(HSD), b_{ij}(HSD) \rfloor$

Засновуючись на вхідних даних для сценаріїв реалізації загрози безпеки, визначається система нечіткого логічного висновку. Функції приналежності параметрів, які використовуються в даному процесі, визначаються таким чином, щоб носії множин змінних розподілялися по діапазону цих параметрів за нормальним законом. В даному випадку проводиться генерація усіх можливих множин правил логічного висновку. Для організації навчання системи логічного висновку, використовуються результати імітаційного моделювання вторгнення, Також визначається множина точок дискретизації заданої функції приналежності, при реалізації нечіткого логічного висновку.

В результаті здійснення даних операцій проводиться розробка матриці вихідних параметрів, основні правила для нечіткої бази знань висновків, які відповідають визначеним вхідним змінним, а також інші характеристики нечіткого висновку.

Здійснивши обчислення множини значень результатів виконання моделі, реалізується процес дефазифікації, при якої використовуються бази знань. Процес дефазифікації заснований на використанні множини експертних оцінок

$$\tau_{HSD} = FDEF\left(\tau\left(HSD\right)\right),$$

де $FDEF$ – нечітка база знань параметрів, яка побудована з використанням множини експертних оцінок

Значення, яке при цьому отримується, використовується для обчислення умовної ймовірності реалізації сценарію вторгнення, яка залежіть від часу проходження маркеру

$$P\left(HSD\right)\left(t\right) = 1 - e^{\frac{-t}{\tau_{HSD}}},$$

де τ_{HSD} – дефаззіфіковане значення часу проходження по мережі,

t – час здійснення сценарію

В результаті виконання даного кроку, отримується значення ймовірності $PTS\left(TS\right)$ для моделі опису вторгнень, яке визначається описом відповідної атаки.

Сценарії загроз, які визначають ймовірність виникнення помилок, збоїв та відмов в мережі складно описувати послідовними та паралельними моделями атак. Складність полягає в тому, це не етапи здійснення певного процесу, а, статична характеристика стану чи результату іншої діяльності. Для уникнення даних труднощів, для даного типу сценаріїв загроз було запропоновано розробку моделей, в яких здійснюється опис даних типів

сценаріїв з використанням ймовірностей находження мережі або її компонентів у відповідному стані.

В процесі побудови моделей помилок та збоїв системи, було виявлено певні схожі структурні характеристики, що обумовило використання умовних ймовірностей здійснення процесів, які характеризують помилки і невідповідності в ході функціонування мережі. При реалізації моделей з урахуванням таких особливостей було визначено два основних параметри:

– параметр, який характеризує можливість. Використання даного параметру дозволяє визначити ймовірність виникнення помилки або збою, і визначається на діапазоні [0,1];

– параметр характеристики часу функціонування системи чи пристрою з урахуванням наявної помилки або збою.

Обчислення умовної ймовірності реалізації послідовностей сценарію при цьому описується наступним чином

$$P(TS) = 1 - e^{-\sigma t}.$$

де σ – коефіцієнт ймовірності помилки, збою або відмови

t – час здійснення сценарію

Основна ідея створення даного варіанту моделі полягає в тому, що визначається умовна ймовірність виконання сценарію, в залежності від ймовірності виникнення події, на протязі певного проміжку часу функціонування мережі або її складових.

Таблиця 3.1 – Залежність ймовірності здійснення сценарію

t	σ	$P(FGS)(t)$	σ	$P(FGS)(t)$
1	0,37	0,012	0,7	0,035
….	….	….	….	….
6	0,37	0,071	0,7	0,162

….	….	….	….	….
12	0,37	0,146	0,7	0,307
….	….	….	….	….
18	0,37	0,207	0,7	0,415
….	….	….	….	….
24	0,37	0,263	0,7	0,508

Наприклад, якщо представити реалізацію події «адміністратор мережі допустив помилку при налаштуванні фільтрації трафіку» між локальною мережею і зовнішньою мережею Інтернет, необхідно мати можливість визначення величини ймовірності того, що при заданому показнику ймовірності виникнення даної помилки σ рівній 0,7 і 0, 37, ця помилка вплине на роботу мережі на протязі доби

Очевидно, що збільшуючи час експлуатації мережевого обладнання або інших компонентів комп'ютерної мережі за умови наявності такої помилки, кінцева ймовірність реалізації даного сценарію загрози збільшується і функція ймовірності прагне дістатися одиниці. Максимальна оцінка можливості виникнення помилки, по суті, не дає максимальної ймовірності здійснення, що відповідає реальним умовам функціонування системи - навіть повна відсутність правил доступу на шлюзі не гарантує моментального здійснення сценарію.

Система оцінювання збоїв мережі ґрунтується на тому ж самому ймовірнісному підході визначення умовної ймовірності, проте має відмінності в семантичному трактуванні показника можливості виникнення збою. В процесі оцінювання помилок в мережі даний показник відображає експертну або випадкову оцінку внутрішніх характеристик мережі або її користувачів, то у випадку моделювання збоїв обладнання, даний параметр реалізує характеристику зовнішніх чинників, а не тільки стан мережі та її мережевого обладнання.

В якості зовнішніх факторів виступають природні катаклізми, фізичні вади та відмови (охолодження, живлення) та інші впливи на характеристики

функціонування мережі. Показник можливості, для даних характеристик, визначається оцінкою того, наскільки його виникнення може впливати на ймовірність реалізації сценарію, і, може описуватись за допомогою експертів, або на основі зовнішніх статистичних джерел інформації.

3.3 Моделі ініціаторів вторгнення

Як визначено в даному дослідженні, загрозою вважається ймовірність порушення безпеки в комп'ютерній мережі яка оцінюється системою виявлення вторгнень. Виходячи з цього, можна прийняти тезу, що загрозою є певне джерело небезпеки, яке здатне привести стан мережі до етапу здійснення сценаріїв загроз. Загрози визначають зовнішнє або внутрішнє втручання в функціонування системи або мережі, можуть носити випадковий або навмисний характер. За такого визначення, було побудовано структуру загроз безпеці інформаційної системи або комп'ютерної мережі (рисунок 3.2).

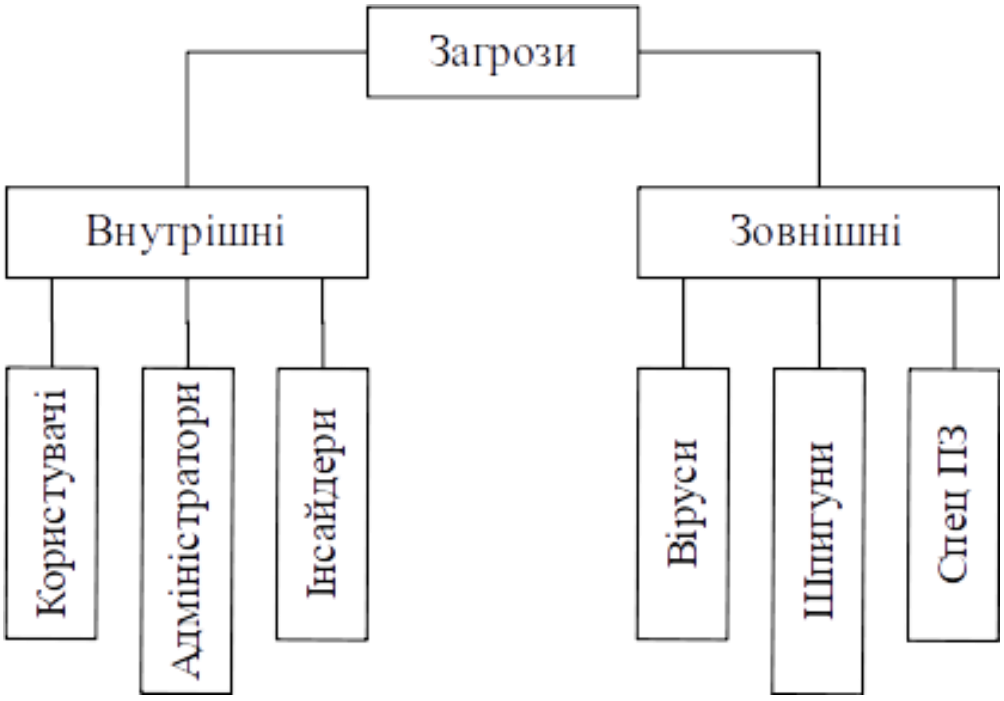

Рисунок 3.2 – Основні типи загроз

Дана структура демонструє класифікацію основних типів загроз в загальному вигляді. Багато з існуючих загроз класифіковані і представлені в спеціалізованих джерелах, доступних для кожного хто має намір їх вивчити.

Загрози обов'язково асоціюються зі сценаріями і інцидентами, джерелами для яких вони висувають, і розглядаються як структура джерело-наслідок. Однак даний підхід не завжди виправданий, тому як відсутність у системі моделювання сценарії такого визначення як джерело події знижує ймовірність оцінки самого факту виникнення загрози. Однак на виникнення таких загроз впливає множина різних факторів, які можуть зменшити або збільшити можливість їх виникнення. Ці фактори, в подальшому, впливають на систему як вразливість такої системи, так як вони здатні визначити слабкі місця в комп’ютерній мережі або системі.

Сукупність визначених факторів впливу складають множину елементів впливу на загрозу

$$PT(T_i) = \{\{Tf_1\}, \{Tf_2\}, \ldots, \{Tf_n\}\}$$

де $PT(T_i)$ – ймовірність виникнення загрози,

$\{Tf_n\}$ – підмножина факторів, що впливають на $PT(T_i)$

Кожний елемент такої множини факторів є певною підмножиною однотипних структур і це дозволяє, за певними властивостями, групувати фактори. Це, в свою чергу, дозволяє визначати загальнодоступну ієрархію загрози (рисунок 3.3) і спростити процес визначення параметру $PT(T_i)$.

Для оцінки ймовірності виникнення загрози в мережі, в рамках дослідження було запропоновано використання методу, який складається з наступних чотирьох етапів.

Перший етап передбачає визначення усіх факторів, які здатні здійснити вплив на ймовірність виникнення загрози. При цьому, створюється відповідна ієрархія і множина, де перелік факторів впливу систематизується і підлягає визначенню відповідної оцінки $f_i(z_i)$. Кожна кінцева вершина

ієрархії визначає оцінку фактора, інші вершини представляють згортку C_{vk} розташованих нижче значень.

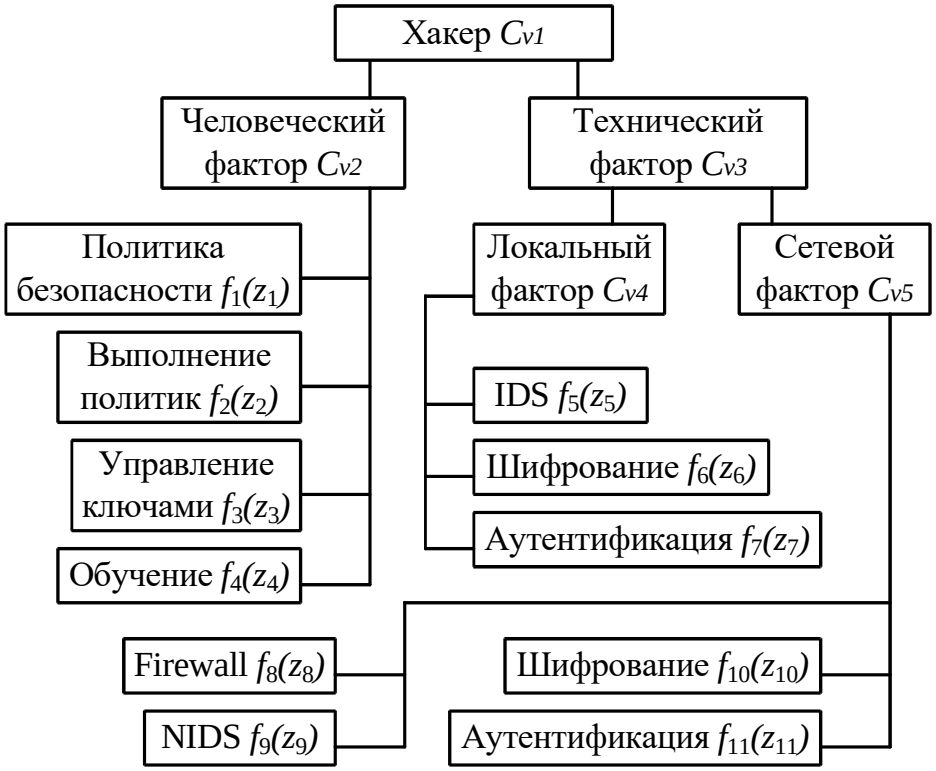

Рисунок 3.3 – Структура впливу на загрози

На другому етапі кожному фактору ставиться у відповідність експертна оцінка. Оцінку необхідно уніфікувати, тобто вона повинна бути приведена до єдиної системи з використанням коефіцієнта задоволеності кожного експерту:

$$f_i = 1 - e^{-\alpha t}$$

де α – коефіцієнт задоволеності експерта,

t – час функціонування даного об'єкту

Коефіцієнт α визначає ступінь задоволеності експерта станом мережі, кваліфікацією і навичками персоналу тощо. Час t визначає тривалість роботи

об'єкта (пристрій, система, актуальність інформації і т. Д.), який оцінюється з позиції вторгнення.

На даному етапі здійснюється ранжування джерел загроз, що дозволяє, в свою чергу, встановити ступень важливості одних чинників в порівнянні з іншими, або визначити сукупний вплив групи факторів

$$Firewall \ _C \ Аутентифікація \ _C \ Шифрування \ _C \ NIDS,$$

$$Firewall + Шифрування \ _I \ Firewall + NIDS,$$

де $_C$ – відношення переваги між факторами,

$_I$ – відношення переваги між факторами.

На основі даних переваг будується навчальна множина

Таблиця 3.2 – Порядок факторів впливу в залежності від переваг

Фактор Набір оцінок	*Firewall*	*Аутентифікація*	*Шифрування*	*NIDS*
A	0,81	0,82	0,91	0,91
B	0,86	0,81	0,92	0,92
C	0,7	0,81	0,61	0,43
D	0,73	0,83	0,45	0,62
E	0,56	0,82	0,47	0,67
F	0,51	0,81	0,62	0,41

За умов використання адитивних мір для множини, параметр з більшою оцінкою визначається з більшим пріоритетом. Однак, як можна побачити з таблиці 3.2 видно, що набір А має більшу перевагу, незважаючи на менш оцінене значення першого критерію.

Третій етап передбачає визначення нечітких мір для кожної кінцевої вершини ієрархії. При цьому використовуються отримані раніше оцінки і

значення взаємодії компонентів загроз та переваг між ними. В результаті виходить множина нечітких мір

$$v = [x_1, x_2, \ldots, x_n], n = 2^k$$

де x_n – значення нечіткої міри

k – кількість факторів, підпорядкованих вершині

Отримані значення підлягають оберненню Мебіуса, приведення нечіткого інтегралу до зручної форми арифметичних залежностей між факторами

$$m^v(A) = \sum_{BA} (-1)^{|A|} v(B)$$

де B та A первинна і кінцева безліч значень відповідно

На четвертому етапі виконується процес згортання оцінок факторів з використанням нечіткого інтеграла Шоке на основі коефіцієнтів m^v, замість нечіткої міри

$C_{vi}(T_i) = p_1 f_1 + p_2 f_2 + \ldots + p_j f_j$, для агрегації факторів

$C_{vk}(T_i) = p_{k1} C_1 + \ldots + p_{ki} C_i$, для агрегації складених вершин

де f_j – експертна оцінка фактору,

p_j – коефіцієнт на основі m^v,

T_i – розглянута загроза.

В результаті здійснення цих процесів, визначається ймовірність $P(T)$, яка використовується для оцінювання можливості виникнення інцидентів безпеки в мережі.

3.4 Висновки до розділу

Основними досягненнями в дослідженні, викладеними в даному розділі є наступні:

1. розроблено підхід до створення групових сигнатур вторгнень на основі нечітких мереж Петрі, що дозволяє описувати послідовність здійснення вторгнення в невизначеному форматі;

2. розроблено моделі для опису подій в системі, які супроводжуються вторгненням чи є його наслідками;

3. розроблено моделі, які дозволяють описувати загрози інформаційної безпеки, які виступають ініціаторами вторгнення.

Усі ці моделі дозволяють створювати нечіткі сигнатурні моделі вторгнень, а також аналізувати причини виникнення вторгнення на основі використання нечітких баз знань.

4 МОДЕЛЬ ОЦІНКИ ЗАХИЩЕНОСТІ КОМП'ЮТЕРНИХ МЕРЕЖ

На основі розроблених в ході дослідження нечітких моделей та інших елементів було розроблено структуру системи виявлення вторгнень, робота якої заснована на використанні нечіткої логіки.

При цьому, система передбачає три основні модулі, які реалізують зазначені моделі:

– модуль формування нечітких сигнатур вторгнень;

– модуль збору та аналізу інформації про трафік;

– модуль, який реалізує реакції системи при виявлення вторгнень.

Модуль формування нечітких сигнатур здійснює процес аналізу відомих атак та сигнатур, що дозволяє виявляти загальні ознаки атак, загроз та класифікуваню їх до груп сімейств вторгнень, або формування нового сімейства.

Модуль збору та аналізу здійснює спостерігання за трафіком на всіх рівнях мережевої моделі TCP, тобто аналізує кадри, пакети, сегменти та дані мережевих застосувань.

Модуль реалізації реакцій автоматизує основні процеси, які здійснюють активні дії системи виявлення вторгнень в разі визначення шкідливої діяльності сегменті або в мережі в цілому.

4.1 Визначення ступеню близькості сигнатур вторгнень

Модуль формування сигнатур використовує три базових, які функціонують в тандемі взаємодії:

– графічний інтерфейс аналітика;

– бібліотека для створення сигнатур;

– скрипти, які здійснюють класифікацію сигнатур.

Графічний інтерфейс надає можливості доступу до баз даних та знань сигнатур та до бібліотек створення сигнатур. Завантаження сигнатур здійснюється зі спеціалізованого серверу, або серверів партнерів, наприклад mitre.org, що, в свою чергу, дозволяє організувати власне централізоване сховище сигнатур, та проводити локальне резервування в самої системі виявлення вторгнень.

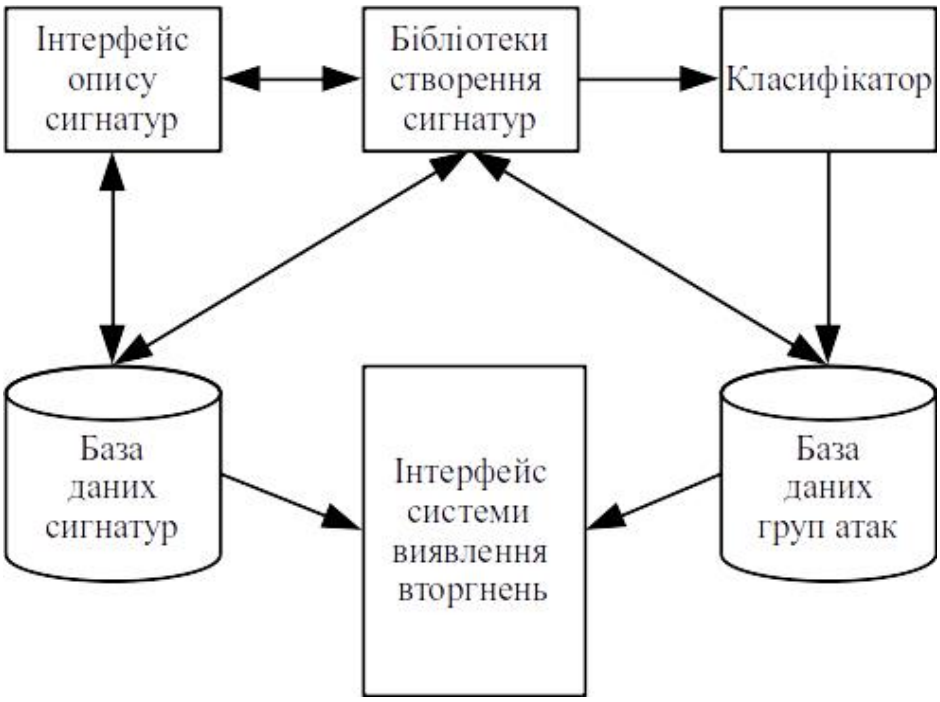

Рисунок 4.1 – Модуль управління сигнатурами

Для інженера-аналітика організовано прямий доступ до усіх наявних баз даних та знань сигнатур, що надає для нього можливість керування локальною базою даних з використанням розроблених API, що, в свою чергу, дозволяє створювати нові сигнатури, які аналітик дослідив в ході роботи та змінювати існуючи. При внесенні будь-яких змін в локальну базу даних, проводиться автоматична синхронізація з централізованою базою даних.

В блок класифікації завантажені усі алгоритми навчання без вчителя, які використовуються для виявлення близьких за структурою або схожих

сигнатур вторгнень. В результаті процесу класифікації визначаються групи або родини атак, які здійснюють свої дії в системі за однаковими або схожими сценаріями. Такий процес дозволяє виявляти атаки, які ще невідомі, або були підвернуті рефакторінгу їх програмної реалізації.

Модель формування родових сигнатур представлена з використанням множини характерних параметрів, композиція яких надає можливості, в подальшому, організовувати сигнатурний опис атак. Функціонування моделі дозволяє відокремлювати причину атаки (ініціатора), етапи реалізації атаки та вразливість, яка використовується при здійсненні атаки, а також методи класифікації, які використовуються для створення родових сигнатур.

$$B_{FS} = \{\{PT(T_i)\},\{S_a\},\{A_C\}\},$$
$$PT(T_i) = \{\{Tf_1\},\{Tf_2\},\ldots,\{Tf_n\}\},$$
$$S_a = \{S_{i1}, S_{i2},\ldots, S\},$$
$$A_C = \{a_1, a_2,\ldots, a_k,\}$$

В моделі параметр $PT(T_i)$ характеризує множину ініціаторів, які призводять до початку атаки, а Tf_n – це множина факторів, які чинять вплив на виникнення загрози. Множина S_a – це набір сигнатур атаки на мережеву структуру, де S_{i1} описує множину етапів вторгнення, яка надає можливості формувати сигнатури атаки і в подальшому групові сигнатури.

Множина A_C представлена набором комп’ютерних алгоритмів класифікації, які доступні для використання в процесі створення поодиноких та групових сигнатур вторгнення.

Усі елементи та модулі дозволяють використовувати наявну інформацію для створення характерних ознак вторгнення із записом в базу даних. Також можливо використовувати базу знань для статичного опису критеріїв впливу вторгнення на комп'ютерну мережу.

4.2 Процес оцінки мережевого трафіку

Оцінка мережевого трафіку базується на використанні моделей, які описують виникнення загроз та сигнатурному аналізі трафіку для виявлення атак. Враховуючи, що атаки, можуть суттєво відрізнятись одна від одної, в даному модулі використовується три блоки:

– блок аналізу канальних кадрів;

– блок аналізу мережевих пакетів;

– блок аналізу змісту файлів.

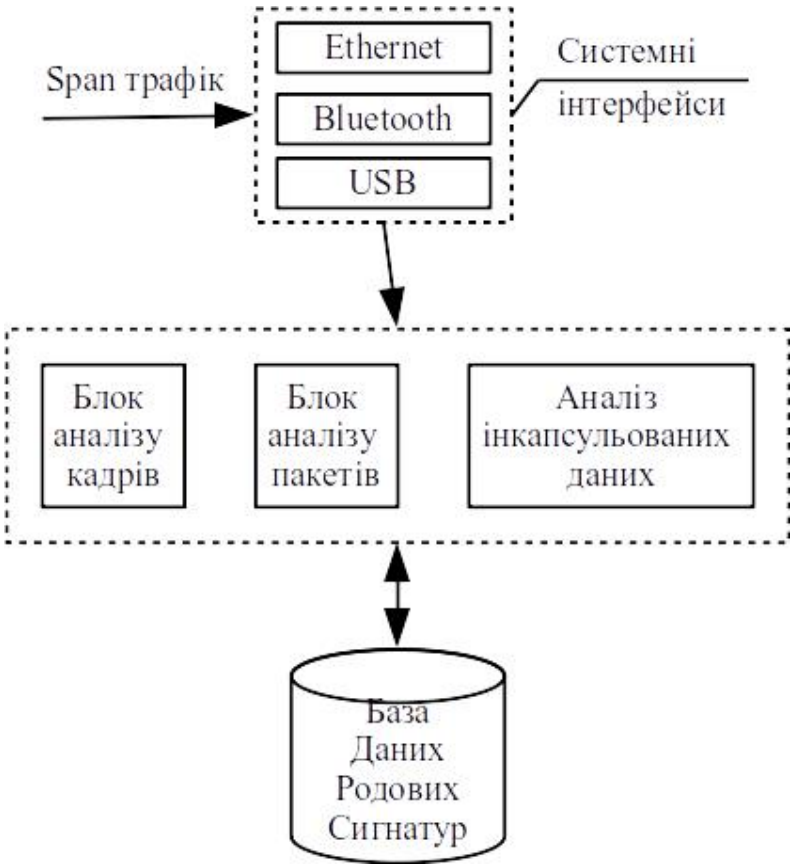

Рисунок 4.2 – Підсистема аналізу мережевого трафіку

За рахунок використання дзеркальованих інтерфейсів, система приймає мережевий трафік даних з усіх інтерфейсів, які визначені адміністраторами для аналізу. При неможливості використовувати дзеркальні інтерфейси,

встановлюється спеціальний сніфер в режимі inline. При цьому оцінці буде піддаватись абсолютно увесь мережевий трафік, що може призвести до навантаженню модулю оцінки.

Перехоплений мережевий трафік надходить до підсистеми аналізу, яка при умові взаємодії з локальними системними базами сигнатур вторгнень реалізує інтелектуальний контроль відповідного рівня моделі мережевої взаємодії.

Аналіз канальних кадрів здійснює контроль даних в рамках плоскої адресації, тобто між комутаторами, зокрема аналіз заголовків кадрів.

Аналіз пакетів реалізує контроль трафіку з позиції адресації та маршрутизації в мережі, зокрема, аналіз адрес джерела та призначення, та опцій заголовку, які в стандартних пакетах не використовуються.

Додатковий аналіз файлів виконується у випадках, коли мережевий трафік визначається системою підозрілим, або мережеві пристрої, які приймають участь сеансі зв'язку визначені як ті, що підозрюються в компрометації, але аналітика інших аспектів трафіку для цих пристроїв нічого не виявила. Для цього в системі використовується модуль, який виконує спеціалізований аналіз даних файлових структур, з наступними параметрами для пошуку підозрілих характеристик:

– походження файлу. Визначення джерела відправки даного файлу (хост в системі, мережева адреса та ін.);

– розширення файлу. Дозволяє визначити відповідність до застосування, яке використовує даний файл в рамках сеансу. Це надає можливості проводити аналіз, відповідності заголовків даного файлу до даного застосування (типові признаки файлу, сигнатури для застосувань та ін.).

Якщо шаблон файлу не відповідає цифровому зліпку застосування, файл негайно переводиться в ізольовану середу, з подальшим машинним аналізом або аналізується людиною.

Також передбачено проведення аналізу сесій на транспортному рівні та рівні застосувань, для запобігання таких вторгнень, які пов’язані із певними маніпуляціями з опціями протоколів або застосувань, які дозволяють зловмисникам налаштовувати тіньовий трафік всередині легальних транзакцій. В разі надходженні фрагментів трафіку до одного з зазначених модулів аналізу, здійснюється перетворення отриманих даних у формат, який відповідає вхідним вимогам машинного алгоритму класифікації та обробки послідовностей атаки.

В загальному вигляді модель аналізу представлена на рисунку 4.3.

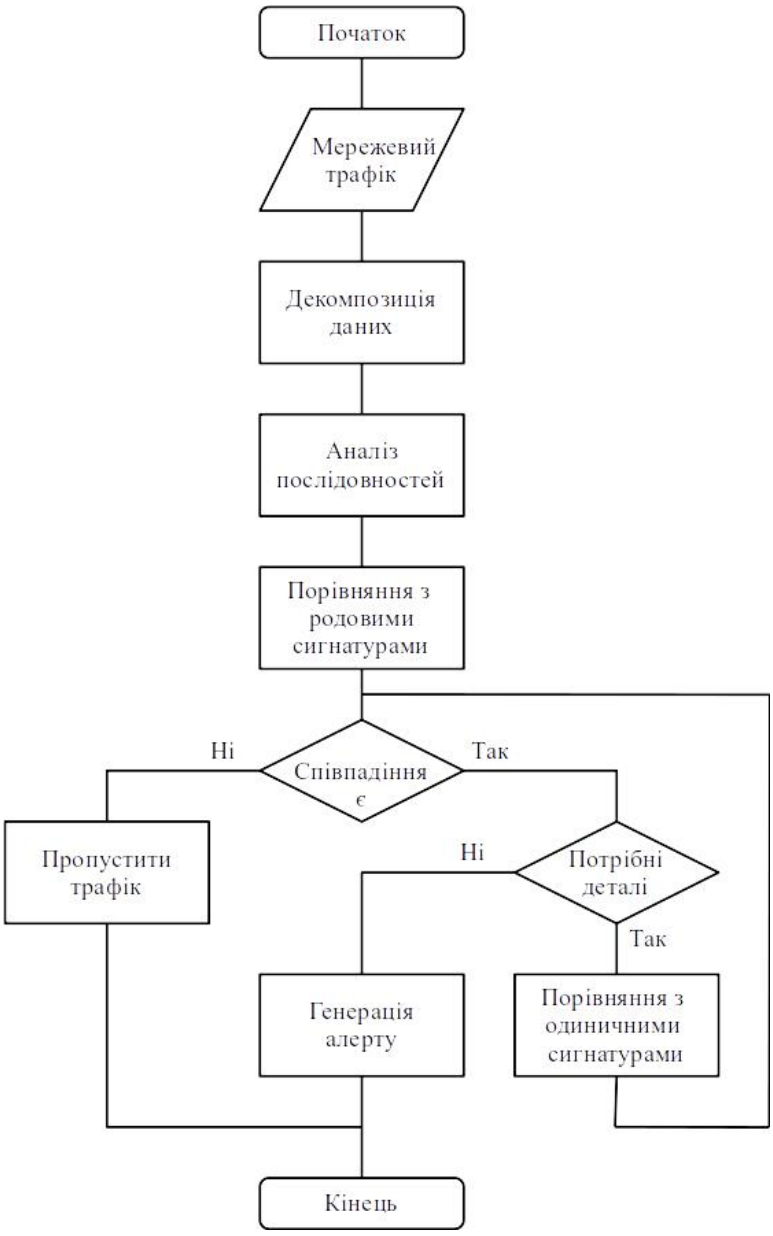

Рисунок 4.3 – Модель аналізу трафіку

В загальному вигляді модель аналізу відповідає операції спів ставлення з образком. Трафік, який надходить на інтерфейси системи виявлення вторгнень підлягає декомпозиції, тобто розбивається на протокольні одиниці. Кожна протокольна одиниця підлягає порівнянню з відповідним до неї шаблоном атак та вторгнень з ціллю виявлення характерних послідовностей, які можуть бути потенційно небезпечними.

Якщо співпадіння знайдене, приймається рішення про необхідність додаткового аналізу послідовностей. Якщо ймовірність того, що отриманий трафік підпадає під категорію небезпечного, система генерує відповідні повідомлення про тривогу. Якщо ймовірність невелика, система здійснює додаткові аналітичні дії з ціллю підвищити достовірність результату співставлення.

По завершенні процесу аналізу, здійснюється запис у журнал подій системи виявлення вторгнень, який здійснює синхронізацію з іншими захисними системами мережі, наприклад системами моніторингу мережі, Syslog сервером журналювання, або комплексною системою моніторингу та аналізу інцидентів та ризиків безпеки.

4.3 Оцінка реакцій на вторгнення

В дослідженні було прийнято, що необхідно використовувати активний моніторинг стану безпеки мережі, тому, розроблена система повинна мати можливість реалізувати базові дії, які направленні на здійснення дій, у відповідності до втручання у роботу мережі, або її окремих кінцевих станцій та серверів. При цьому, було визначено основні типи реакцій на виникнення вторгнення:

– інформування. В даному випадку генерується повідомлення відповідальним особам, яка містить основну інформацію про можливе вторгнення;

– скид сесії. Використання примусового скиду встановленої сесії між об'єктами мережі, яка прийнята, як потенційно або остаточно небезпечна для функціонування мережі;

– скид окремих протокольних одиниць. В даному випадку здійснюється примусовий скид окремих виявлених небезпечних кадрів, пакетів або сегментів;

– ізоляція інформації. Здійснення перенаправлення трафіку до спеціальної віртуальної середи, де буде проводитись більш детальний аналіз виявленої загрози;

– передача даних до SIEM. Здійснення перенаправлення підозрілого тарфіку до системи аналізу та розслідування небезпечних інцидентів, для проведення мануальних дій спеціалістами з безпеки.

Для забезпечення виконання реакції на вторгнення, проводиться спеціальне налаштування системи з урахуванням можливої тяжкості інциденту. Керування даними функціями виконуються аналітиками та адміністраторами для адекватного маркування та сортування такого трафіку.

4.4 Загальна структура системи виявлення вторгнень

На основі зазначених вище моделей було запропоновано систему виявлення вторгнень, яка реалізує вказані моделі та алгоритми (Рисунок 4.4).

Крім зазначених раніше модулів, використовуються субсистеми для сповіщення адміністраторів і інженерів мережі або системи про визначення вторгнень. Передбачено автоматичне формування звітів безпеки про виникнення вторгнень, а також підсистема прийняття рішень про прості дії щодо запобігання вторгненню, наприклад інформування шлюзу безпеки про адреси-джерела вторгнень для їх фільтрації на межі мережі.

Як і більшість систем виявлення вторгнень, запропонована система передбачає оф-лайн роботу і використання дзеркальованих портів для аналізу

копій трафіку. Проте, використання розроблених моделей суттєво знижує об’єм трафіку, який система може не встигнути обробити.

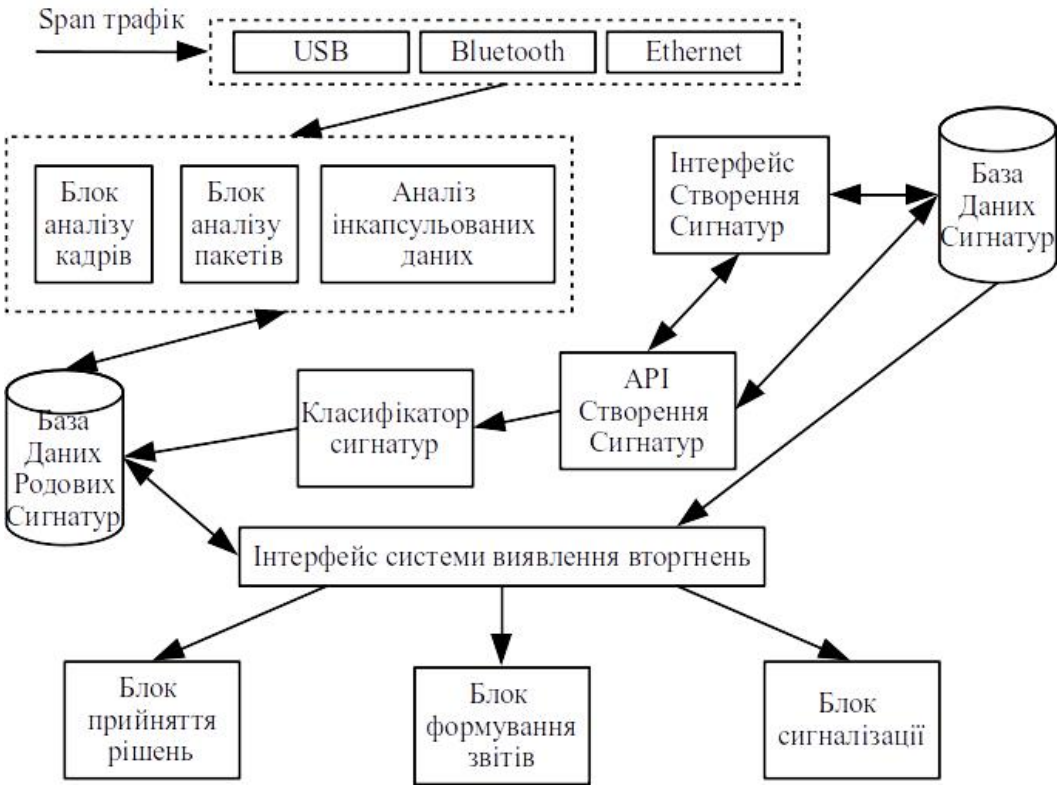

Рисунок 4.4 — Загальна архітектура системи виявлення вторгнень

Таким чином, запропонована система за рівних умов інтенсивності трафіку, знижує обчислювальне навантаження на апаратне забезпечення системи виявлення вторгнень, що дозволяє точніше та швидше виявляти навмисні та ненавмисні дії в комп’ютерній мережі.

4.5 Висновки до розділу

В даному розділі було представлено нечіткі моделі, які використовуються в системі виявлення вторгнень. Основні функції, які виконуються в системі – перехоплення, класифікація та аналітика мережевого внутрішнього та зовнішнього трафіку.

Основними перевагами за рахунок використання даної системи виявлення вторгнень із будуванням представлених моделей можна вважати наступні:

– впровадження інтелектуальних алгоритмів машинного навчання та класифікації мережевого трафіку дозволяє, за рахунок автоматизації, скоротити до 50% часу аналітиків, що, в свою чергу, надає можливості персоналу більше зосередитись на вирішенні інцидентів, які потребують безпосереднього втручання спеціалістів;

– використання методів класифікації по родовим ознакам стосовно втручань в мережу, дозволяє суттєво скоротити кількість наявних сигнатур, які необхідно використовувати при виявленні вторгнень, що дозволяє скоротити використання обчислювальних ресурсів системи;

– клієнт-серверна архітектура розробленої системи дозволяє більш ефективно здійснювати керування сигнатурами вторгнень, організовувати їх корекцію, створювати нові та модифікувати існуючи. Це дозволяє разом із створенням власних сигнатур, використовувати та класифікувати сигнатури сторонніх компаній.

Разом з тим, розроблені моделі, також, мають певні сфери застосування, де їх використання вимагає оптимізації та подальшого розвитку:

– розроблені моделі не пристосовані для здійснення поведінкового аналізу мережевих подій, а також для виявлення аномалій в мережевому трафіку;

– створення та модифікація сигнатур, на даний момент, потребує залучення кваліфікованих навчених співробітників.

Проте, не зважаючи на зазначені недоліки, розроблена система виявлення вторгнень, при умові використанні запропонованих моделей, була підвергнута тестовим випробовуванням в мережі, яка використовується в реальних умовах, та показала суттєву перевагу в порівнянні з класичними системами виявлення вторгнень (рисунок 4.5)

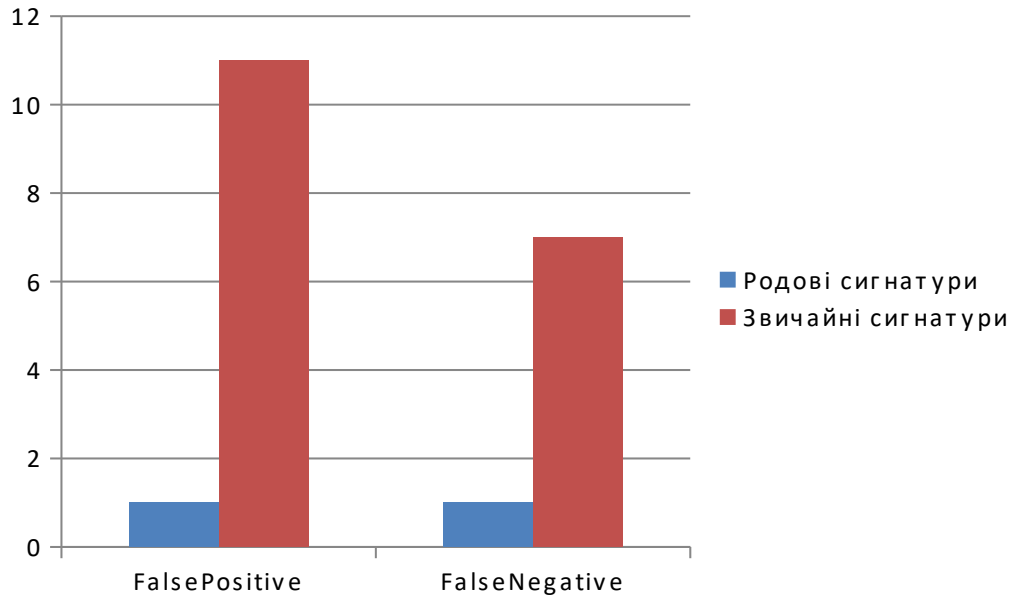

Рисунок 4.5 – Результати використання моделей виявлення вторгнень

При оцінюванні адекватності моделей виявлення вторгнень з використанням розробленої системи було проведено ряд тестових іспитів на проникнення, які імітували реальне вторгнення в систему, та було залучено спеціалістів, які здійснювали дані процеси втручання в систему.

Для порівняння були важливими два наступних параметри:

– False Positive. Параметр, який вказує на наявність вторгнень, які не були виявлені системою. Даний параметр вказує на ризики реального вторгнення в систему;

– False Negative. Параметр який вказує на виявлення вторгнення, якого реально не було. Даний параметр характеризує помилкові виявлення, які призводять до часових втрат аналітиків.

Отримані результати тестування свідчать про те, що доля помилково позитивних рішень про вторгнення від розроблених моделей становить 9,1% від результатів використання класичних сигнатур, а доля помилково негативних становить 14,3% від результатів використання класичних сигнатур.

В загалі, при проведені оцінки систем виявлення вторгнень було визначено, що використання розроблених моделей дозволяє виявляти до 99,2 % вторгнень, які імітувалися в мережевій структурі, в порівнянні з 90,6 % при використанні точних сигнатур.

В загалі, використання даної системи дозволить підвищити захищеність комп'ютерних мереж тому що точність виявлення на 7% в порівнянні з автоматизованими системами виявлення (відкритими), на 18% в порівнянні з моніторингом безпеки експертами.

ВИСНОВКИ

В останній час методи виявлення вторгнень розвивалася дуже стрімко, у зв’язку із залученням методів та систем штучного інтелекту в процес створення загроз інформаційної безпеки. Це обумовило наступні вимоги - по-перше, системи виявлення повинні більш ефективно, здійснювати навчання для виявлення широкого діапазону атак з мінімальною кількістю помилкових тривог. По-друге, засоби виявлення вторгнень необхідно розвивати з урахуванням стрімкого зростання розміру, швидкості і інтенсивності трафіку сучасних мереж. Також, необхідно мати методи аналізу, які дозволяють здійснювати ідентифікацію атак, спрямованих проти мереж в цілому.

Як було виявлено в ході дослідження, сучасні системи виявлення вторгнень, в основному, базуються на методах порівняння із шаблонами. Оскільки такі моделі виявлення моделюють тільки відомі атаки, розробникам доводиться регулярно оновлювати свій набір сигнатур. Такий підхід недостатньо ефективний при намаганнях виявлення невідомих нових атак.

Необхідно, щоб системи виявлення вторгнень мали можливість здійснювати аналіз потоків подій, які генеруються високошвидкісними мережами і серверами.

Із залученням високошвидкісних систем передачі даних, значно зростає об’єм мережевого трафіку. Пов'язані з мережами комп'ютери, за рахунок високих обчислювальних можливостей, здійснюють обробку все більшого об’єму даних і генерують все більш об'ємні журнали подій, тривог та помилок. Це призводить до проблеми, яку колись змушені були вирішувати системні адміністратори, що стикалися з величезними обсягами інформації. Було досліджено два варіанти аналізу такої кількості інформації в реальному

часі: поділ потоку подій або використання периферійних мережевих датчиків.

Встановлення датчиків в ключових місцях мережі надає можливості адміністраторам та інженерам виявляти вторгнення мережі в цілому, а не її сегментів. Іншими словами, мережа, яка використовує агентів, може надати інтегровану оцінку та повну картину стану мережевого захисту. Вторгнення, які маскуються під штатні дії в рамках одного серверу, можуть виявитися суттєво небезпечними в масштабах всієї мережі.

Розроблені моделі для систем виявлення вторгнень надають первинні засоби до створення новітніх IDS нового покоління, які здатні ідентифікувати атаки на мережеву структуру не тільки після атаки, але і на самому початку атаки або навіть до її початку, що дозволяє суттєво знизити кількість інцидентів безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1) J.P. Anderson, Computer Security Threat Monitoring and Surveillance, James P. Anderson Co., Fort Washington, Pa. 1980

2) D.E. Denning, «An Intrusion Detection Model», IEEE Trans. Software Eng., vol. 13, no. 2, Feb. 1987

3) M. Roesch, «Snort-Lightweight Intrusion Detection for Networks», Proc. Usenix Lisa ?99 Conf., Usenix Assoc., Berkeley, Calif., 1999

4) D. Curry, H. Debar, «Intrusion Detection Message Exchange Format: Extensible Markup Language (XML) Document Type Definition», Dec. 2001

5) R. Bace, P. Mell, «Special Publication on Intrusion Detection Systems», Tech. Report SP 800-31, National Institute of Standards and Technology, Gaithersburg, Md., Nov. 2001po

6) U. Lindqvist, P.A. Porras, «Detecting Computer and Network Misuse with the Production-Based Expert System Toolset», IEEE Symp. Security and Privacy, IEEE CS Press, Los Alamitos, Calif., 1999

7) V. Paxson, «Bro: A System for Detecting Network Intruders in Real-Time», Proc. Seventh Usenix Security Symp., Usenix Assoc., Berkeley, Calif., 1998

8) K. Ilgun, R.A. Kemmerer, P.A. Porras, «State Transition Analysis: A Rule-Based Intrusion Detection System», IEEE Trans. Software Eng. vol. 21, no. 3, Mar. 1995, 6. V. Paxson, «Bro: A System for Detecting Network Intruders in Real-Time», Proc. Seventh Usenix Security Symp., Usenix Assoc., Berkeley, Calif., 1998

9) Tarakanov A. O. Immunocomputing for intelligent intrusion detection // IEEE Computational Intelligence Magazine, Май 2008 г., с. 23–30. p

10) Котов В. Д. Система обнаружения вторжений на основе технологий искусственных иммунных систем // Интеллектуальные системы управления. М: Машиностроение, 2010. 544 с. С. 525–535.

11) Portnoy L., Eskin E., Stolfo S. J. Intrusion detection with unlabeled data using clustering // Proc. of ACM Workshop on Data Mining Applied to Security, 2001. P. 5–8.

12) Callegari C., Vaton S., Pagano M. A new statistical approach to network anomaly detection // Proc. of Performance Evaluation of Computer and Telecommunication Systems (SPECTS). 2008. P. 441–447.