Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)

Комп’ютерні науки
(повна назва кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА
до кваліфікаційної роботи

магістр
(освітній рівень)

на тему: **Порівняльний аналіз інформаційних систем виявлення вторгнень у роботу комп'ютерних систем**

Виконав: студент 6 курсу, групи СТм-61
спеціальності 126 «Інформаційні системи та технолгії»
(шифр і назва спеціальності)

(підпис) Ребуха А.М.
(прізвище та ініціали)

Керівник (підпис) Гром'як Р.С.
(прізвище та ініціали)

Нормоконтроль (підпис) Мацюк О.В.
(прізвище та ініціали)

Рецензент (підпис) Кареліна О.В.
(прізвище та ініціали)

м. Тернопіль – 2020

АНОТАЦІЯ

"Порівняльний аналіз інформаційних систем виявлення вторгнень у роботу комп'ютерних систем" // Ребуха Андрій Миколайович // Тернопільський національний технічний університет ім. І. Пулюя, факультет комп’ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СТм-61 // Тернопіль, 2020 // с. – , рис. – , табл. – , джерел – .

Ключові слова: ВТОРГНЕННЯ, ЗАГРОЗА, СИСТЕМА ВИЯВЛЕННЯ, ПРОТОКОЛ, СЕРВЕР, МЕРЕЖА.

У магістерській роботі виконано дослідження способів забезпечення необхідного рівня захищеності комп'ютерних систем на основі систем виявлення вторгнень з різним типами функціонування. Здійснено огляд принципів роботи систем виявлення вторгнень.

В дипломній роботі показано актуальність захисту комп'ютерних систем від проникнення в їх роботу та захист від таких вторгнень. Проаналізовано основні механізми роботи таких систем та розроблено рекомендації по їх використанню.

ANNOTATION

"Comparative analysis of intrusion detection systems into computer systems " // Diploma paper of Master degree level // Rebukha Anrii Mykolayovytch // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Computer Science Department // Ternopil, 2020 // p. – , Fig. – , Tables – , Refence. – .

Key words: INTRUSION, THREAT, DETECTION SYSTEM, PROTOCOL, SERVER, NETWORK.

The research of ways of providing the necessary level of protection of computer systems on the basis of systems of detection of intrusions with various types of functioning is executed in the master's thesis. An overview of the principles of operation of intrusion detection systems.

The thesis shows the relevance of protection of computer systems from intrusion into their work and protection against such intrusions. The main mechanisms of operation of such systems are analyzed and recommendations for their use are developed.

ЗМІСТ

Розділ 1 Принципи функціонування систем виявлення вторгнень 7
1.1 Система виявлення вторгнень 7
1.2 Системи виявлення вторгнень на основі сигнатур (SIDS) 10
1.3 Виявлення в режимі реального часу 12
1.3.1 Атаки відмови в обслуговуванні (DOS) 12
1.3.2 Атаки підслуховування 13
1.3.3 Атаки вторгнення або атака користувача до руту (U2R) 13
1.3.4 Атаки зловживання входом 14
1.3.5 Атаки на рівні програми 14
1.4 Функції IDS 14
1.4.1 Збір даних 14
1.4.2 Вибір функцій 14
1.4.3 Аналіз 15
1.4.4 Дія 15
1.5 Особливості життєвого циклу IDS 15
1.5.1 Оцінка та вибір 15
1.5.2 Розгортання 16
1.5.3 Експлуатація та використання 16
1.5.4 Технічне обслуговування 17
1.6 Методики роботи IDS 17
1.6.1 Визначення аномального вторгнення 17
1.6.2 Виявлення впливу на основі сигнатур 19
1.6.3 Цільовий моніторинг 19
1.7 Інструменти виявлення вторгнень 20
1.8 Потреби і виклики 21
1.9 IDS в різних сферах 22
1.10 IDS для хмарних обчислень 23
1.11 IDS в технологіях інтелектуального аналізу даних 24

1.12 Висновки до розділу 24
Розділ 2 Типи систем виявлення вторгнень та їх робота 25
2.1 Система виявлення вторгнень на основі сигнатур (SIDS) та аномалії (AIDS) . 28
2.2 Джерела даних про вторгнення 30
2.3 Методи впровадження AIDS 33
2.4 Методи, засновані на статистиці 33
2.5 Методи, засновані на знаннях 35
2.6 AIDS на основі техніки машинного навчання 36
2.7 Навчання без нагляду в системі виявлення вторгнень 43
2.8 Навчання під наглядом 44
2.9 Ансамблеві методи 45
2.10 Гібридні методи 45
Розділ 3 Показники ефективності для IDS 46
3.1 Набори даних для виявлення вторгнень 47
3.2 Порівняння загальнодоступних наборів даних IDS 51
3.3 Вибір функцій для IDS 53
3.4 Види комп’ютерних атак 54
3.5 Методи ухилення від IDS 56
3.6 Проблеми IDS 58
3.7 Проблема IDS щодо виявлення ухилення від вторгнення 59
Розділ 4 Охорона праці та безпека в надзвичайних ситуаціях 60
4.1 Вимоги до мікроклімату, освітленню, рівням шуму, іонізуючих та неіонізуючих електромагнітних полів та випромінювань моніторів 60
4.2 Забезпечення захисту працівників суб’єктів господарювання та населення від впливу іонізуючих випромінювань 64
Висновки 66
Перелік посилань 68

РОЗДІЛ 1
ПРИНЦИПИ ФУНКЦІОНУВАННЯ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Метою виявлення вторгнень є моніторинг мережевих ресурсів для виявлення аномальної поведінки та неправильного використання в мережі. Концепція виявлення вторгнень була запроваджена на початку 1980-х років після еволюції Інтернету з кінцевим спостереженням та моніторингом загрози [3]. Раптово зріс репутація та інтеграція в інфраструктуру безпеки. З тих пір кілька подій в технології IDS вдосконалили виявлення вторгнень до поточного стану. Джеймс Андерсон впровадив підхід, згідно з яким аудиторські сліди містять важливу інформацію, яка може бути корисною для відстеження зловживань та розуміння поведінки користувачів [3].

Потім виявилось, а дані аудиту та його важливість призвели до значних поліпшень в підсистемах захисту кожної операційної системи. Вперше було визначено систему IDS та систему виявлення вторгнень (HIDS). Приблизно в 1990-х роках генеруються доходи та збільшується ринок виявлення вторгнень. Real secure – це мережа виявлення вторгнень, розроблена ISS. Через рік Cisco визнала пріоритет для задачі виявлення вторгнень у мережу та придбала Wheel Group для досягнення рішень безпеки [3].

1.1 Система виявлення вторгнень

Кожна система виявлення вторгнень (Intrusion Detection System – IDS) фактично є охоронною сигналізацією. Для прикладу система блокування в будинку захищає будинок від крадіжки. Але якщо хтось порушує систему замків і намагається увійти в будинок, саме охоронна сигналізація виявляє, що замок зламаний, і попереджає власника, піднявши сигнал тривоги. Більше того, брандмауери дуже добре фільтрують вхідний трафік з Інтернету на предмет обходу брандмауера [4]. Наприклад, зовнішні користувачі можуть підключитися до Інтранету, набравши номер через модем, встановлений у приватній мережі організації; такий доступ не може бути виявлений брандмауером.

Система запобігання вторгненню (Intrusion Prevention System – IPS) – це мережева технологія безпеки / запобігання загрозам, яка перевіряє потоки мережевого трафіку для виявлення та запобігання експлуатації вразливості. Існує два типи системи запобігання: на основі мережі (NIPS) та на основі хоста (HIPS). Ці системи стежать за мережевим трафіком і автоматично вживають заходів для захисту мереж і систем. Проблемою IPS є помилкові спрацьовування та негативні, відповідно, наслідки. Під помилково позитивним визначається подія, яка видає сигнал тривоги в IDS, коли немає атаки. Під помилковим негативом визначається подія, яка не викликає тривоги, коли відбувається атака. Вбудована система виявлення та запобігання вторгнень може створити вузькі місця, такі як одна точка відмови, оновлення підписів та зашифрований трафік. Дії, що відбуваються в системі або мережі, вимірюються за допомогою IDS [4].

На рисунку 1.1 показано класифікацію систем виявлення вторгнень:

– для хоста (HIDS);
– для мережі (NIDS);
– для застосунку (AIDS).

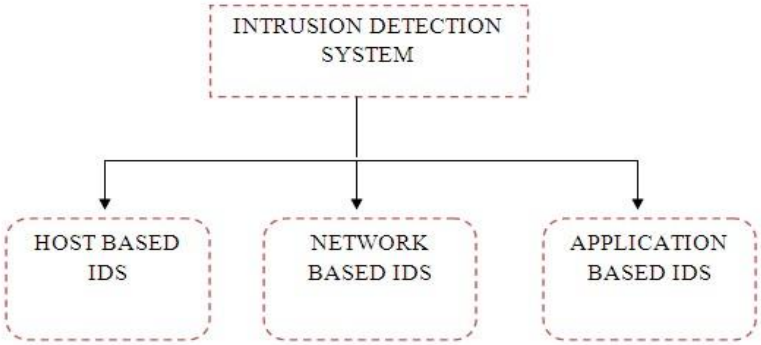

Рисунок 1.1 – Типи IDS

IDS, що базується на хості, розглядає ознаку вторгнення в локальну систему. Для аналізу вони використовують реєстрацію хост-системи та іншу інформацію. Обробник на основі хоста називається датчиком. Інші джерела, з яких датчик, що базується на хості, може отримувати дані, включають системні журнали та інші

журнали, що генеруються процесами операційної системи та вмістом об'єктів, що не відображаються у стандартних механізмах аудиту та реєстрації операційної системи.

Система, що базується на хості, сильно довіряє залежить від результатів програмного аудиту. Ця інформація дозволяє системі виявлення вторгнень виявляти тонкі зловживання, які не були б помітні на вищому рівні абстракції. Елементарний принцип в IDS, включаючи мережеву систему виявлення вторгнень (NIDS), походить від досліджень аномалії HIDS, заснованих на новаторській роботі Деннінга [5]. IDS на основі хоста надає набагато більш релевантну інформацію, ніж IDS на основі мережі. HIDS ефективно використовується для аналізу мережевих атак, наприклад, він іноді може точно сказати, що зробив зловмисник, які команди він використовував, які файли він відкрив, а не просто показати невизначене звинувачення, що є спроба виконати небезпечну команду.

Переваги систем виявлення вторгнень на основі хосту:

- Перевіряє успіх або невдачу атаки.
- Відстежує діяльність системи.
- Виявляє атаки, які мережевий IDS не вдається виявити.
- Виявлення та реагування майже в режимі реального часу.
- Не вимагає додаткового обладнання.
- Менша вартість входу.

Мережеві системи IDS збирають інформацію з самої мережі, а не з кожного окремого хоста. NIDS проводить аудит мережевих атак під час переміщення пакетів по мережі. Мережеві датчики оснащені підписами атак, які є правилами щодо того, що буде складати атаку, і більшість мережевих систем дозволяють досвідченим користувачам визначати власні підписи. Атаки на датчик базуються на підписі, і вони є результатом попередніх атак, і робота моніторів буде прозорою для користувачів, і це також важливо.

Прозорість моніторів зменшує ймовірність того, що супротивник зможе знайти його та звести нанівець його можливості [6]. Агенти мережевих вузлів IDS (NNIDS) розгортаються на кожному хості в мережі, яка підлягає захисту.

Переваги мережевих систем виявлення вторгнень:

- Нижча вартість.
- Простіше розгортати.
- Виявлення мережевих атак.
- Зберігання доказів.

Таким чином, вторгненням можна визначити будь-який несанкціонований вид діяльності, що спричиняє пошкодження інформаційної системи. Це означає, що будь-яка атака, яка може становити можливу загрозу конфіденційності, цілісності чи доступності інформації, буде розглядатися як вторгнення. Наприклад, діяльність, яка може призвести до того, що комп’ютерні служби не реагують на законних користувачів, вважається вторгненням. IDS – це програмна чи апаратна система, яка ідентифікує зловмисні дії на комп’ютерні системи з метою забезпечення безпеки системи [16]. Метою IDS є виявлення різних видів шкідливого мережевого трафіку та використання комп'ютера, які неможливо ідентифікувати за допомогою традиційного брандмауера. Це життєво важливо для досягнення високого захисту від дій, що загрожують доступності, цілісності або конфіденційності комп'ютерних систем. Системи IDS можна розділити на дві групи:

- система виявлення вторгнень на основі сигнатур (SIDS);
- система виявлення вторгнень на основі аномалій (AIDS).

1.2 Системи виявлення вторгнень на основі сигнатур (SIDS)

Системи виявлення вторгнень на основі сигнатур (SIDS) базуються на методах узгодження шаблонів для пошуку відомої атаки; вони також відомі як виявлення, засноване на знаннях або виявлення зловживання. У SIDS застосовуються відповідні методи для виявлення попереднього вторгнення. Іншими словами, коли підпис втручання збігається з підписом попереднього вторгнення, який уже існує в базі даних підписів, спрацьовує сигнал тривоги. Для SIDS журнали хоста перевіряються, щоб знайти послідовності команд або дій, які раніше були ідентифіковані як шкідливі

програми. SIDS також були позначені в літературі як виявлення, засноване на знаннях, або виявлення зловживання.

Рисунок 1.2 демонструє концептуальну роботу підходів МОРОГ. Основна ідея полягає у створенні бази даних підписів про вторгнення та порівнянні поточного набору дій з існуючими підписами та піднятті тривоги, якщо знайдено збіг. Наприклад, правило у формі «якщо: попередній -тоді: послідовний» може призвести до «якщо (IP-адреса джерела = IP-адреса призначення), то позначити як атаку».

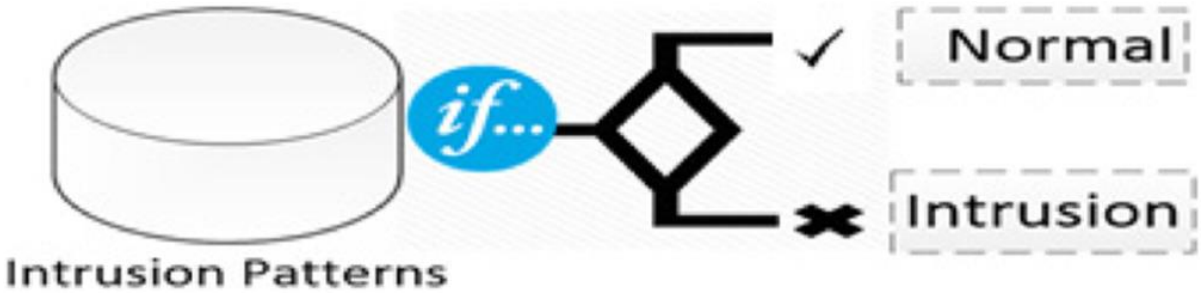

Рисунок 1.2 – Концептуальна робота підходів МОЗТ

SIDS зазвичай забезпечує чудову точність виявлення раніше відомих вторгнень. Однак SIDS зазнає труднощів у виявленні атак нульового дня з тієї причини, що в базі даних не існує відповідної сигнатури, доки сигнатура нової атаки не буде отримана.

Традиційні підходи до SIDS вивчають мережеві пакети та намагаються зіставити з базою даних підписів. Але ці методи не можуть ідентифікувати атаки, що охоплюють кілька пакетів. Оскільки сучасне шкідливе програмне забезпечення є більш складним, може знадобитися витягувати інформацію про підписи через кілька пакетів. Це вимагає від IDS відкликання вмісту попередніх пакетів. Що стосується створення сигнатури для SIDS, то, як правило, існує ряд методів, коли сигнатури створюються як машина станів, формальні шаблони мовних рядків або семантичні умови [16].

Зростаючий рівень атак з нульовим днем [11] робить техніки SIDS поступово менш ефективними, оскільки попередніх підписів для таких атак не існує. Поліморфні варіанти шкідливого програмного забезпечення та збільшення кількості цільових атак

можуть ще більше підірвати адекватність цієї традиційної парадигми. Потенційним рішенням цієї проблеми було б використання методів боротьби зі AIDS, які діють шляхом профілювання того, що є прийнятною поведінкою, а не тим, що є аномальним, як описано в наступному розділі.

1.3 Виявлення в режимі реального часу

IDS на основі додатків (APIDS) перевірятиме ефективну поведінку та події протоколу [7]. Система або агент розміщується між процесом і групою серверів, які контролюють та аналізують протокол додатків між пристроями. Умисні атаки – це злоякісні атаки, що здійснюються незадоволеними працівниками для заподіяння шкоди організації, а ненавмисні атаки завдають фінансової шкоди організації, видаляючи важливий файл даних. На рівні OSI відбувається багато різних атак, основін типи котрих показано на рис. Рисунок 1.3 –

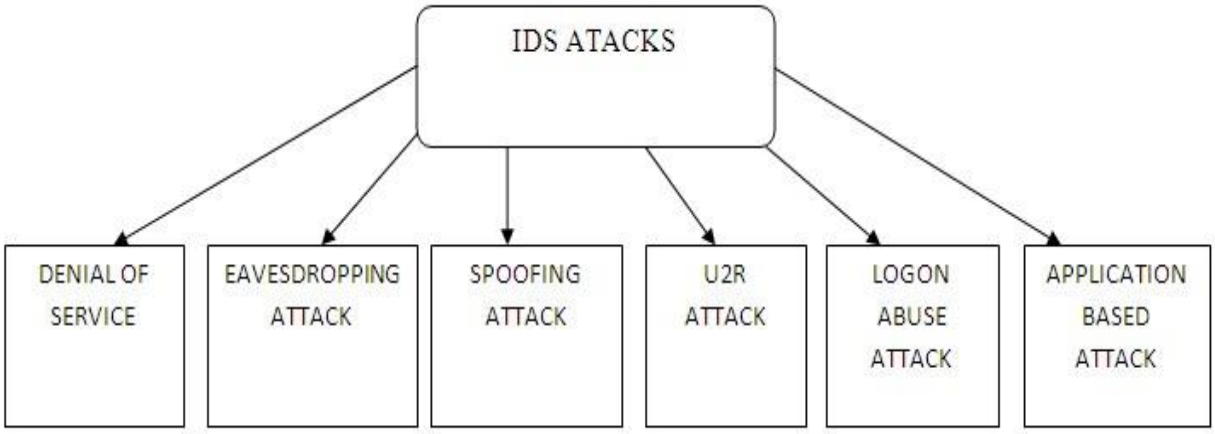

Рисунок 1.3 – Типи атак на систему

Опишемо коротко кожен з типів атак.

1.1.1 Атаки відмови в обслуговуванні (DOS)

Зловмисник намагається відмовити уповноваженим користувачам у просуванні запитуваної послуги. Розширений розподілений відмова в обслуговуванні

відбувається в розподіленому середовищі, яке зловмисник надсилає або заливає сервер численними з’єднаннями, які вимагають збити цільову систему[7]. Типи атак DOS:

SYN Атака.

Атака SYN також визначається як атака синхронізації. Тут зловмисник надсилає потік запиту SYN до місця призначення, щоб використовувати ресурси сервера і зробити систему невідповідною.

Пінг смерті.

У цьому зловмисник надсилає запит пінгу до цільової системи, який перевищує 65536 байт, що призводить до аварійного завершення роботи системи. Формальний розмір повинен бути 56 байт або 84 байти, якщо врахувати заголовок Інтернет-протоколу.

1.1.2 Атаки підслуховування

Це схема втручання зловмисника у спілкування. Цю атаку можна здійснити за допомогою телефонних ліній або електронної пошти..

Атаки підміни.

Зловмисник видає себе за іншого користувача для підробки даних та отримання переваг щодо незаконних дій у мережі. Підробка IP-повідомлень є загальним прикладом, коли система спілкується з довіреним користувачем і забезпечує доступ до зловмисника.

1.1.3 Атаки вторгнення або атака користувача до руту (U2R)

Зловмисник намагається отримати доступ до системи або маршруту через мережу. Атака переповнення буфера – типова атака вторгнення, яка виникає, коли веб-служба отримує більше даних, ніж було запрограмовано для обробки, що призводить до втрати даних.

1.1.4 Атаки зловживання входом

Атака зловживання входом призведе до нехтування механізмами автентифікації та контролю доступу та надасть користувачеві більше переваг [2].

1.1.5 Атаки на рівні програми

Зловмисник націлений на інвалідність шару нанесення. Наприклад, слабкість безпеки на веб-сервері або в несправних елементах управління на стороні сервера [2].

1.4 Функції IDS

IDS складається з чотирьох ключових функцій, а саме збору даних, вибору функцій, аналізу та дії, що наведено на рис.1.4.

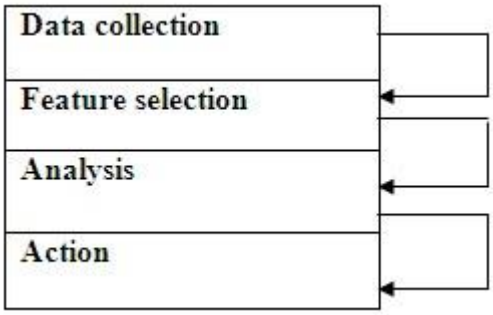

Рисунок 1.4 – Функціональність IDS

1.1.1 Збір даних

Цей модуль передає дані як вхідні дані до IDS. Дані записуються у файл, а потім аналізуються. Мережевий IDS збирає та змінює пакети даних, а в IDS, що базується на хості, збирає такі деталі, як використання диска та процеси системи.

1.1.2 Вибір функцій

Для вибору конкретної функції в мережі доступні великі дані, які зазвичай оцінюються на предмет втручання. Наприклад, адреса протоколу Інтернету (IP) вихідної та цільової системи, тип протоколу, довжина заголовка та розмір можуть бути прийняті як ключ для вторгнення [15].

1.1.3 Аналіз

Дані аналізуються, щоб знайти правильність. IDS, що базується на правилах, аналізує дані, де вхідний трафік перевіряється за попередньо визначеними підписом чи шаблоном [15]. Іншим методом є IDS, заснований на аномалії, де вивчається поведінка системи та застосовується математичний режим ls [15].

1.1.4 Дія

Він визначає атаку та реакцію системи. Він може або повідомити системного адміністратора усіма необхідними даними через піктограми електронної пошти / сигналізації, або може відігравати активну роль у системі, скинувши пакети, щоб він не зайшов у систему або не закрив порти [15].

1.5 Особливості життєвого циклу IDS

Постачальники часто випускають нові продукти IDS, які агресивно конкурують за свої частки ринку. Оцінка нових систем не є актуальним завданням, а інформація про розрахунок товару недосконала. Наймання та утримання робітників для управління безпекою та виявленню вторгнень є складними завданнями. Швидкі зміни в IT роблять проблемою для фірми впровадження довгострокової стратегії безпеки.

Розглянемо коротко етапи життєвого циклу системи виявлення вторгнень, зображеного на рисунку 1.4.

1.5.1 Оцінка та вибір

Якщо організація планує отримати IDS, вона повинна вивчити ресурси, доступні для експлуатації та обслуговування систем. Життєвий цикл продукту для економічних IDS прискорюється. Оцінка третьої сторони доступна, і їхні звіти, як правило, на поверхні. Цей процес ілюструє виявлення зловмисника та обсяг роботи, необхідної для підтримання системи в мережі з трафіком, а процес відбору визначає ідентифікацію характеру, підходів, точності, зручності та ефективності.

1.5.2 Розгортання

Етап розгортання включає роботу датчиків для максимального захисту критично важливих елементів шляхом налаштування IDS для відображення політики безпеки та встановлення прав доступу.

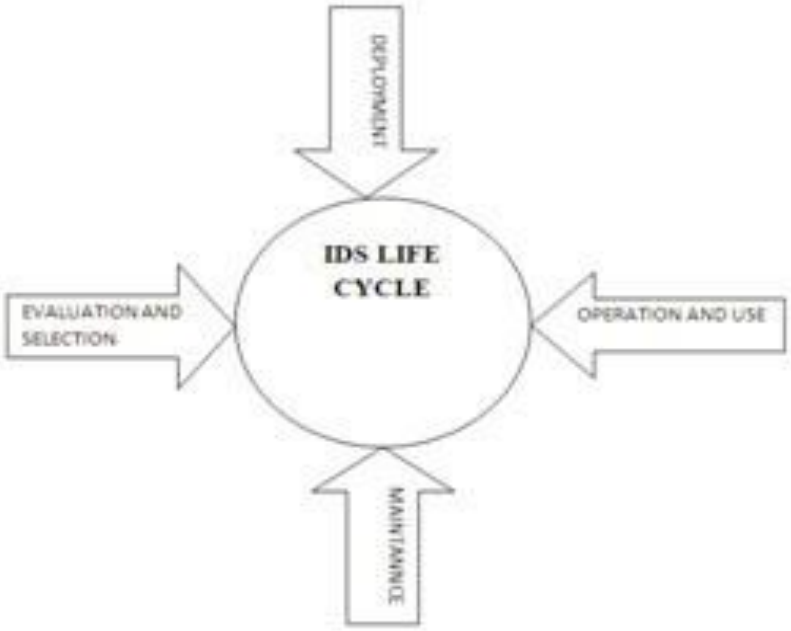

Рисунок 1.5 – Етапи життєвого циклу IDS

Користувачі повинні розробити правила поводження та пов'язати їх із іншими системами. Робоча група з виявлення вторгнень (IETF) розробляє загальний формат оповіщення, який використовує IDS для оповіщення з різних систем, і про них повідомляється на загальній консолі дисплея.

1.5.3 Експлуатація та використання

Організація адмініструє IDS для моніторингу хоста та реагування на звіт як попередження. Він встановлює ролі та відповідальність за аналіз та моніторинг результатів як ручних, так і автоматичних реакцій. Розумні зловмисники, які усвідомлюють, що IDS розгорнуто під час мережевої атаки, змушують її подавати помилкові повідомлення.

1.5.4 Технічне обслуговування

Технічне обслуговування включає встановлення підписів та оновлення IDS. Розміщення датчиків слід періодично переглядати, щоб переконатись, що система або мережа змінюються. Організація повинна залучати, навчати та утримувати кваліфікований технічний персонал для роботи та підтримки технологій IDS.

1.6 Методики роботи IDS

1.6.1 Визначення аномального вторгнення

Аномалія вказується як витікання, особливості або винятки – це шаблон даних, який працює ненормально. Техніка виявлення аномалій призначена для виявлення шаблонів, далеких від звичайних, а інші позначені як вторгнення [7]. Виявлення аномалій класифікуються на статичні та динамічні детектори.

Детектор статичної аномалії приймається як частина контрольованої системи, яка залишається постійною. Статична частина складається з двох частин, тобто системного коду та системних даних. Статичні частини системи можна представити у вигляді двійкового біта. Якщо має місце будь-яке відхилення від початкової форми, тоді помилка була вказана або грабіжник змінив частину системи.

У динамічному детекторі включено визначення поведінки системи. Поведінка системи визначається як порядок різних подій. Наприклад, записи аудиту, вироблені операційною системою, використовуються IDS для визначення подій, що представляють інтерес [7]. У цьому випадку поведінку можна спостерігати лише тоді, коли записи аудиту створюються ОС і події відбуваються в суворій послідовності [7]. Якщо невизначена поведінка розглядається як аномальна, тоді системні адміністратори можуть бути попереджені помилковими тривогами [8].

Виявлення аномалізму корисно для пошуку таких атак, як зловживання протоколом та сервісними портами, DoS на основі створених корисних навантажень, DoS на основі обсягу (DDoS), переповнення буфера та інші аномалії корисного навантаження додатків.

Методи, що використовуються для виявлення аномалій:

Кількість подій і лічильник подій вдосконалено та впроваджено у виявленні аномалій.

Статистичні моделі

Статистична модель показує результат як статистичну величину. Існує два типи статистичних моделей, вони є

a) Операційна модель (OM) Порогова метрика: дії, які відбуваються протягом певного періоду, регулюють тривогу. Це можна візуалізувати в блокуванні Win2k; користувач після n невдалих спроб входу в систему регулює будильник. Тут нижня межа дорівнює 0, а верхня межа дорівнює n.

b) Процес Маркова або маркерна модель: У цій моделі система перевіряється з фіксованим інтервалом часу. Поведінка виявляється як аномалія, якщо ймовірність стану низька.

Моделі пізнання

a) скінченний автомат: скінченний автомат (FSM) або скінченний автоматизатор – це модель поведінки, зафіксована в станах, переходах та діях. Держава визначає інформацію про минуле. Дія – це опис діяльності, яка повинна бути виконана в певний момент, і типами дій є вхідна дія, вихідна дія та дія переходу.

б) сценарії опису : мови сценаріїв характеризують напади на комп’ютери та мережі. Усі мови сценаріїв здатні досліджувати послідовності конкретних подій.

Когнітивні методи виявлення загроз.

Методи виявлення, засновані на пізнанні (їх також називають системами, що базуються на знаннях або на практиці), працюють над даними аудиту. Набір заздалегідь визначених правил для класів та атрибутів визначається із набору даних навчання.

a) Підсилене дерево рішень або підсилене дерево (BT): воно використовує алгоритм ADA Boost (адаптивне підсилення) для генерації багатьох класифікаторів дерев рішень, підготовлених за різною вибіркою, що реалізовано в IDS.

b) Підтримка векторної машини (SVM): SVM визначається як класифікатори, призначені для двійкової класифікації. SVM на основі дерева рішень – це техніка, яка

поєднує ці два методи для ефективного вирішення проблеми. За допомогою цього методу можна зменшити час навчання та тестування.

1.6.2 Виявлення впливу на основі сигнатур

Тут набір даних має кількість екземплярів, і всі дані повинні бути позначені як звичайні чи нав'язливі. Алгоритми машинного навчання використовуються для підготовки набору даних відповідно до їх мітки. Ця техніка автоматично зберігає підпис для виявлення зловмисника. Техніка виявлення зловживань створюється автоматично, і роботи є більш складними та точними, ніж виконані вручну. Залежно від надійності та серйозності підпису, який активується в системі, деякі відповіді на тривогу або сповіщення повинні бути надіслані відповідним органам.

Методи, що використовуються для виявлення зловживання:

a) Відповідність виразів: відповідність виразів є найпростішою та найпростішою формою виявлення зловживання. При цьому він шукає потік подій, таких як записи в журналі, для того, щоб відбувся точний шаблон.

b) Аналіз переходу стану: ця модель атакує стан або переходи в мережі. Кожна подія в мережі застосовується до кінцевих автоматів, що, нарешті, призводить до переходу. Атака відбудеться, коли машина досягне остаточного стану.

1.6.3 Цільовий моніторинг

Моніторинг цілей – це техніка, яка використовується для повідомлення про будь-які зміни чи модифікації в системі. Це зазвичай робиться за допомогою криптографічного алгоритму, який обчислює крипто-контрольну суму для кожного цільового файлу [5]. Якщо в крипто-контрольній сумі відбуваються будь-які зміни, вони повідомляються IDS. Контрольна сума Tripwire – це перевірка цілісності, яка перевіряє зміни чи модифікації у файлах.

1.7 Інструменти виявлення вторгнень

Продукт виявлення вторгнень, який сьогодні доступний, стосується цілого ряду організаційних цілей безпеки [2]. У цьому розділі розглядається інформація про засоби безпеки.

SNORT.

SNORT – це легке програмне забезпечення з відкритим кодом. SNORT використовує гнучку мову, засновану на правилах, для опису трафіку [9]. З IP-адреси; він записує пакет у зручній для читання формі. За допомогою аналізу протоколів, морського вилучення вмісту та різних попередніх процесорів Snort виявляє тисячі хробаків, спроби використання вразливості, сканування портів та інші підозрілі поведінки [6].

OSSEC-HIDS.

OSSEC (безпека з відкритим кодом) – це безкоштовне програмне забезпечення з відкритим кодом. Він працюватиме в основній операційній системі та використовує архітектуру на основі клієнта / сервера. OSSEC має можливість надсилати журнали ОС на сервер для аналізу та зберігання. Він використовується в потужній системі аналізу журналів, провайдерах, університетах та центрах обробки даних. Журнали автентифікації, брандмауери контролюються та аналізуються HIDS.

FRAGROUTE.

Його називають маршрутизатором фрагментації. Тут від зловмисника до фрагментатора передається IP-пакет, який потім фрагментується і трансформується в сторону.

HONEYD.

Honeyd – це інструмент, який створює віртуальні хости в мережі [6]. Послуги, що використовуються хостом, Honeyd дозволяє одному хосту запитувати декілька адрес у локальній мережі для моделювання мереж. Можна збити віртуальні машини або простежити їх маршрут [6]. Будь-який тип служби на віртуальній машині може бути змодельований за допомогою простого конфігураційного файлу [6].

KISMET.

Це рекомендація для WIDS (бездротової системи виявлення вторгнень). WIDS компрометує з корисним навантаженням пакетів та подіями WIDS. Він знайде точку доступу.

1.8 Потреби і виклики

Для впровадження пристрою IPS існує безліч проблем. IPS-пристрій розроблений для роботи в режимі вбудованого подання з єдиною точкою відмови. Деякі атаки, що переслідуються, не виявляються, якщо пасивний IDS виходить з ладу, а продуктивність мережі впливає на збій вбудованого пристрою. Один із компонентів мережі, пристрій NIPS (система запобігання вторгненню в мережу) повинен працювати як мережевий комутатор. Він повинен відповідати вимогам до продуктивності та надійності мережі для організації викликів. Отже, дуже мало споживачів готові пожертвувати мережевою продуктивністю та надійністю в цілях безпеки.

NIPS s зменшує трафік, і проблема NIPS скидає пакети, вони використовуються для здійснення потоку даних. Більшість висококласних постачальників IPS отримають цю проблему, використовуючи спеціальне обладнання із вдосконаленими FPGA та ASIC. Необхідно розробити продукт для функціонування як пристрій виявлення та запобігання вторгненню. Кожна організація потребує IDS, яка є як інструмент оборони. Організації стикаються з деякими проблемами при впровадженні системи виявлення вторгнень.

1. Технологія IDS не потребує втручання людини. Сьогодні технологія IDS пропонує певну автоматизацію, наприклад, сповіщення адміністратора на випадок виявлення шкідливої діяльності, відмова від шкідливого з'єднання протягом певного періоду часу, динамічна модифікація списку контролю доступу маршрутизатора з метою зупинки шкідливого з'єднання. Для кожної події, що трапляється, слід контролювати журнали IDS. Щоденний моніторинг журналів необхідний для аналізу діяльності, яка виявляється IDS протягом певного періоду.

2. Впровадження IDS залежить від успішності розгортання. Планування важливо на етапі проектування та впровадження. У більшості випадків бажано впровадити гібридне рішення мережевого та хост- IDS. Рішення можуть різнитися в різних організаціях. Мережі на основі IDS є безпосереднім вибором для багатьох організацій з – за своєї здатності контролювати кілька систем, а також той факт, що вона не вимагає програмного забезпечення для завантаження у виробничій системі в відміну від господарів на основі IDS.

Деякі організації надають гібридне рішення. Отже, доступні ресурси потрібні системі перед встановленням хост- сенсора.

3. Співвідношення менеджера датчиків має бути схваленим. Дуже важливо розробити базову політику перед початком впровадження IDS та уникати помилкових результатів. Датчик IDS може надсилати на датчик багато помилкових результатів, і коефіцієнт може бути неадекватним.

4. Технологія IDS все ще реактивна, а не активна, і ця технологія працює на підписах атак. Підписи визначаються як шаблон атак, який був визначений d раніше. Базу даних підписів потрібно оновлювати щоразу, коли виявляється інший тип атаки, і вони фіксуються в базі даних, і частота оновлення підписів різниться від постачальника до постачальника.

5. Через зіткнення доменів у комутованій мережі трафік вхідного та вихідного порту не видно з будь-якого іншого хост-порту. Але в мережі, що базується на концентраторі, вхід і вихід можна переглянути з будь-якого порту. Датчик NIDS повинен виявляти трафік у порт і з порту, а також зловмисний трафік в комутованому середовищі. Для досягнення такого роду вони використовують дзеркальне відображення або охоплення портів.

1.9 IDS в різних сферах

IDS використовується у численних областях, а ефективність у кожному випадку описується та визначає, як вони виконувались.

9.1 IDS у MANET

MANET [10] визначається як мобільна мережа adhoc. Це автономна мережа, яка природно складається з комбінацій мобільних вузлів без централізованого адміністрування. IDS використовується в MANET. Зазвичай повідомлення розщеплюються на певне число пакетів, і вони використовують апаратні пристрої, як провід і модем для передачі. Але в MANET вони підключені бездротовим способом. Сторожовий собака та оцінювач шляху – це два прийоми, додані до протоколу в Adhoc.

Сторожовий собака ідентифікує неправильні вузли, підслуховуючи передачу наступного стрибка. Тоді оцінювач шляхів допомагає знайти маршрути, які не містять цих вузлів. IDS використовуються в MANET під час передачі серії пакетів до місця призначення через мобільну мережу, щоб знайти зловмисника, якщо такий є.

1.10 IDS для хмарних обчислень

Хмарні обчислення ілюструються як хмарні обчислювальні технології на основі Інтернету, де віртуальні спільні сервери надають пристрої платформи інфраструктури програмного забезпечення та інші ресурси та розміщують клієнта як послугу на основі оплати за користування. Користувач хмарних доу не тримає жодної фізичної основи, замість цього він орендує посередника (третю сторону). Вони платять лише за використання ресурсу. Система виявлення вторгнень відіграє важливу роль у безпеці та стійкості активної системи захисту від ворожих атак зловмисників для будь-якого бізнесу та IT-організації. У хмарних обчисленнях програми надходять на віддалений сервер провайдера, і вони мають контроль над використанням даних. IDMEF (формат обміну повідомленнями про виявлення вторгнень) – це стандарт, який використовується в хмарі для комунікаційних цілей.

- Проблеми безпеки хмарних обчислень.
- Конфіденційність хмарних даних.
- Атаки на віддалений сервер.
- Аудит безпеки хмарних технологій.
- Відсутність взаємодії даних.

1.11 IDS в технологіях інтелектуального аналізу даних

Інтелектуальний аналіз даних – це процес вилучення прихованих знань із баз даних. IDS дуже важливі при аналізі даних. Виявлення вторгнень включає виявлення набору зловмисних дій, які порушують цілісність та доступність інформаційних ресурсів.

Виявлення вторгнень в інтелектуальному аналізі даних має два підрозділи, це виявлення зловживання та виявлення аномалій. При виявленні зловживання марковані дані будуються з використанням передбачувальної моделі. При виявленні аномалій між моделями існує відхилення. Для того, щоб спочатку використовувати дані, їх слід перетворити на дані, що пропонуються, і до них застосовуються моделі інтелектуального аналізу даних, і вони узагальнюються для отримання результату.

В цій області IDS постають перед такими викликами:

- Великий обсяг даних.
- Вища розмірність..
- Попередня обробка даних.

1.12 Висновки до розділу

Основною метою даного розділу є надати огляд необхідності та корисності системи виявлення вторгнень. Таким чином розділ дає повне дослідження про типи IDS, життєвий цикл, різні домени, типи атак та інструменти. IDS стають важливими для сьогоднішньої безпеки в корпоративному світі та для користувачів мережі. IPS визначає заходи запобігання безпеці. У життєвому циклі розроблені фази та проілюстровано етапи. Також показано, що існує немало проблем, які потрібно подолати. Методи виявлення аномалій та виявлення зловживань спеціально проілюстровані, і можуть бути використано багатьма методами. Подальша робота буде проведена щодо порівняльного аналізу деяких популярних алгоритмів аналізу даних, що застосовуються до IDS, та вдосконалення IDS на основі класифікації з використанням методів вибіркового зворотного зв'язку.

РОЗДІЛ 2
ТИПИ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ ТА ЇХ РОБОТА

Еволюція шкідливого програмного забезпечення (зловмисного програмного забезпечення) представляє критичну проблему для проектування систем виявлення вторгнень (IDS). Шкідливі атаки стали більш досконалими, і головним завданням є виявлення невідомих та затуманених шкідливих програм, оскільки автори шкідливого програмного забезпечення використовують різні методи ухилення для приховування інформації, щоб запобігти виявленню IDS. Крім того, спостерігається зростання таких загроз безпеці, як атаки нульового дня, призначені для користувачів Інтернету. Тому комп’ютерна безпека стала важливою, оскільки використання інформаційних технологій стало частиною нашого повсякденного життя. Як результат, різні країни, такі як Австралія та США, зазнали значного впливу нападів нульового дня. Згідно з звітом про загрози безпеки в Інтернеті за 2017 рік, у 2016 році було зареєстровано понад три мільярди атак з нульовим днем, а обсяг та інтенсивність атак з нульовим днем були значно більшими, ніж раніше [11]. Як підкреслюється в Статистиці про порушення даних у 2017 році, приблизно дев'ять мільярдів записів даних були втрачені або викрадені хакерами з 2013 року [12]. У звіті Symantec встановлено, що кількість випадків порушення безпеки зростає. Раніше кіберзлочинці в основному орієнтувались на клієнтів банків, грабували банківські рахунки або крали кредитні картки. Однак нове покоління шкідливих програм стало більш амбітним і націлене на самі банки, іноді намагаючись взяти мільйони доларів за одну атаку. З цієї причини виявлення атак з нульовим днем стало найвищим пріоритетом.

Гучні випадки кіберзлочинності продемонстрували легкість розповсюдження кіберзагроз у міжнародному масштабі, оскільки простий компроміс може порушити основні послуги та засоби бізнесу. У всьому світі існує велика кількість кіберзлочинців, мотивованих красти інформацію, незаконно отримувати доходи та знаходити нові цілі. Шкідливе програмне забезпечення навмисно створюється для компрометації комп’ютерних систем та використання будь-якої слабкості систем виявлення вторгнень. У 2017 році Австралійський центр кібербезпеки (ACSC)

критично вивчив різні рівні майстерності, що застосовуються зловмисниками [13]. Тому існує потреба у розробці ефективної системи IDS для виявлення нових, складних шкідливих програм. Метою IDS є якнайшвидше виявлення різних видів шкідливих програм, чого неможливо досягти за допомогою традиційного брандмауера. Зі збільшенням обсягу шкідливих програм на комп'ютері розвиток вдосконалених IDS став надзвичайно важливим.

В останні кілька десятиліть машинне навчання використовувалось для поліпшення виявлення вторгнень, і в даний час існує потреба в сучасній, ретельній систематиці та огляді цієї недавньої роботи. Існує велика кількість відповідних досліджень, що використовують або набір даних KDD-Cup 99, або DARPA 1999 для підтвердження розвитку IDS; однак немає чіткої відповіді на питання, які методи видобутку даних є більш ефективними. По-друге, час, необхідний для побудови IDS, не враховується при оцінці деяких методів IDS, незважаючи на те, що є критичним фактором для ефективності "онлайнових" IDS.

У цій роботі представлена сучасна таксономія, а також огляд значних дослідницьких робіт з IDS до теперішнього часу та класифікація запропонованих систем згідно з таксономією. Він надає структурований та всебічний огляд існуючих IDS, щоб дослідник міг швидко ознайомитися з ключовими аспектами виявлення аномалій. Цей документ також надає огляд методів інтелектуального аналізу даних , що застосовуються для проектування систем виявлення вторгнень. Описано методи, засновані на підписах та аномалії (тобто, SIDS та AIDS), а також декілька методів, що використовуються в кожному методі. Обговорюється складність різних методів боротьби зі AIDSом та методів їх оцінки, а потім набір пропозицій, що визначають найкращі методи залежно від характеру вторгнення. Також обговорюються виклики для поточних IDS. У цій роботі представлена дискусія щодо проблем набору даних IDS, які найбільше хвилюють наукове співтовариство в галузі систем виявлення вторгнень у мережі (NIDS) . У цій роботі пропонується структуроване та сучасне широкомасштабне дослідження системи виявлення вторгнень з точки зору методів та наборів даних; а також висвітлити проблеми методів, а потім зробити рекомендації.

Протягом останніх кількох років було опубліковано ряд опитувань щодо виявлення вторгнень. У таблиці 2.1 наведено методи IDS та набори даних, охоплені цим оглядом. Дослідження системи виявлення вторгнень та систематики, проведене в [14], класифікувало системи виявлення вторгнень на основі методів виявлення. Автори [15] обстежили методи виявлення, засновані на поведінці та профілях знань атак. Таксономія систем вторгнення від [16] представив класифікацію п’яти підкласів із поглибленим поглядом на їх характеристики:

– на основі статистики, на основі зразків,
– на основі правил,
– на основі виразів та евристики.

З іншого боку, наша робота зосереджена на принципі виявлення підписів, виявленні аномалій, систематиці та наборах даних.

Таблиця 2.1 – Порівняння цього огляд та подібних оглядів: (" +" – тема висвітлена, " -" тема не висвітлена)

Огляд	**Кількість цитувань станом на 01.06.2019**	**Методи системи виявлення вторгнень**						**Випуск набору даних**
		SIDS	**AIDS**				**Гібридні IDS**	
			Навчання під контролем	**Без нагляду**	**Навчання під наглядом**	**Ансамблеві методи**		
[17]	219	+	-	-	-	-	-	-
[18]	1039	+	+	-	-	-	-	-
[16]	505	+	+	+	-	-	+	-
[19]	108	+	+	+	+	+	+	-
[20]	338	+	+	+	-	+	+	+
[21]	181	-	+	+	-	-	-	+
Цей огляд		+	+	+	+	+	+	+

Існуючі оглядові статті зосереджуються на методах виявлення вторгнень або проблемі набору даних або типі комп'ютерної атаки та ухилення від IDS. Жодна стаття не аналізувала всебічно виявлення вторгнень, проблеми з наборами даних, методи ухилення та різні види атак. Крім того, розробка систем виявлення вторгнень була такою, що було запропоновано декілька різних систем, і тому існує потреба в

оновленні. Оновлений огляд таксономії дисципліни виявлення вторгнень представлений у цій роботі, ще більше вдосконалює таксономії, наведені в [16].

З огляду на обговорення попередніх опитувань, ця стаття зосереджується на наступному:

- Класифікація різних видів IDS за основними типами атак на основі методів вторгнення.
- Представлення класифікації метрик оцінки IDS аномалії мережі та обговорення важливості вибору ознак.
- Оцінка наявних наборів даних IDS, що обговорюють проблеми техніки ухилення.

2.1 Система виявлення вторгнень на основі сигнатур (SIDS) та аномалії (AIDS)

AIDS зацікавив багатьох науковців завдяки своїй здатності подолати обмеження SIDS. При AIDS створюється нормальна модель поведінки комп’ютерної системи з використанням методів машинного навчання, статистичних або заснованих на знаннях. Будь-яке значне відхилення між спостережуваною поведінкою та моделлю розглядається як аномалія, яку можна трактувати як вторгнення. Припущення для цієї групи методів полягає в тому, що зловмисна поведінка відрізняється від типової поведінки користувача. Поведінка ненормальних користувачів, що відрізняється від стандартної поведінки, класифікується як вторгнення. Розвиток AIDS складається з двох фаз: фази навчання та фази тестування.

На етапі навчання використовується звичайний профіль дорожнього руху для вивчення моделі нормальної поведінки, а потім на етапі тестування використовується новий набір даних для встановлення здатності системи узагальнювати до раніше невидимих вторгнень. AIDS можна класифікувати на ряд категорій на основі методу, що використовується для навчання, наприклад, на статистичній основі, на основі знань та на основі машинного навчання.

Головною перевагою AIDS є можливість ідентифікувати атаки нульового дня через те, що розпізнавання ненормальної активності користувачів не покладається на базу даних підписів. AIDS викликає сигнал небезпеки, коли досліджувана поведінка відрізняється від звичайної поведінки. Крім того, AIDS має різні переваги. По-перше, вони мають можливість виявляти внутрішні шкідливі дії. Якщо зловмисник починає робити транзакції в викраденому обліковому записі, які не ідентифіковані під час типової діяльності користувача, це створює сигнал тривоги. По-друге, кіберзлочинцю дуже важко розпізнати, що є нормальною поведінкою користувача, не видаючи попередження, оскільки система побудована з індивідуальних профілів.

У таблиці 2.2 представлені відмінності між виявленням на основі підпису та виявленням на основі аномалії. SIDS може ідентифікувати лише добре відомі вторгнення, тоді як AIDS може виявити напади нульового дня. Однак AIDS може призвести до високого показника хибнопозитивних результатів, оскільки аномалії можуть бути просто новою звичайною діяльністю, а не справжніми вторгненнями.

Таблиця 2.2 – Порівняння методологій виявлення вторгнень

	Переваги	**Недоліки**
SIDS	• Дуже ефективний при виявленні вторгнень з мінімальним числом помилкових тривог (FA). • Оперативно виявляє вторгнення. • Покращений для виявлення відомих атак. • Простий дизайн	• Потрібно часто оновлювати новий підпис. • SIDS призначений для виявлення атак на відомі підписи. Коли попереднє вторгнення було трохи змінено на новий варіант, система не зможе визначити це нове відхилення подібної атаки. • Не вдається виявити атаку нульового дня. • Не підходить для виявлення багатоетапних атак. • Мало розуміння розуміння нападів
AIDS	• Може використовуватися для виявлення нових атак. • Може використовуватися для створення підпису про вторгнення	• AIDS не може обробляти зашифровані пакети, тому атака може залишатися не виявленою та представляти загрозу. • Високі помилкові позитивні тривоги. • Важко створити нормальний профіль для дуже динамічної комп’ютерної системи. • Некласифіковані оповіщення. • Потрібне початкове навчання.

Оскільки таксономії для систем виявлення вторгнень на основі аномалій бракує, ми визначили п’ять підкласів на основі їх особливостей: на основі статистики,

на основі шаблону, на основі правил, на основі держави та на основі евристики, як показано в таблиці 2.3.

Таблиця 2.3 – Характеристики методології виявлення для систем виявлення вторгнень

Методика виявлення	**Характеристика**
На основі статистики: аналізує мережевий трафік, використовуючи складні статистичні алгоритми для обробки інформації.	• Потрібен великий обсяг статистичних знань. • Простий, але менш точний. • У реальному часі
На основі шаблону: визначає символи, форми та шаблони в даних.	• Простий у впровадженні • Функцію хешу можна використовувати для ідентифікації.
На основі правил: використовує "підпис" атаки для виявлення потенційної атаки на підозрілий мережевий трафік.	• Обчислювальні витрати систем, заснованих на правилах, можуть бути дуже високими, оскільки правила потребують узгодження зразків. • Дуже важко оцінити, які дії відбуватимуться і коли. • Потрібна велика кількість правил для визначення всіх можливих атак. • Низький показник хибнопозитивних даних • Високий рівень виявлення
Державний: вивчає потік подій для виявлення будь-якої можливої атаки.	• Імовірнісний, самотренінг • Низький показник хибнопозитивних результатів.
Заснована на евристиці: визначає будь-яку ненормальну діяльність, яка виходить за межі звичайної діяльності.	• Потрібні знання та досвід. • Експериментальне та еволюційне навчання

Попередні два розділи класифікували IDS на основі методів, що використовуються для виявлення вторгнень.

2.2 Джерела даних про вторгнення

IDS також можна класифікувати на основі джерел вхідних даних, що використовуються для виявлення ненормальної діяльності. Що стосується джерел даних, то, як правило, існує два типи технологій IDS, а саме IDS на основі хостів (HIDS) та IDS на основі мережі (NIDS). HIDS перевіряє дані, що походять від хост-системи та джерел аудиту, таких як операційна система, журнали віконного сервера,

журнали брандмауерів, аудит систем додатків або журнали баз даних. HIDS може виявляти внутрішні атаки, які не включають мережевий трафік.

NIDS відстежує мережевий трафік, що виділяється з мережі за допомогою захоплення пакетів, NetFlow та інших мережевих джерел даних. Мережеві IDS можна використовувати для моніторингу багатьох комп’ютерів, які приєднані до мережі. NIDS здатний контролювати зовнішні шкідливі дії, які можуть бути ініційовані із зовнішньої загрози на більш ранньому етапі, перш ніж загрози поширяться на іншу комп'ютерну систему. З іншого боку, NIDS мають обмежену можливість перевіряти всі дані в мережі з високою пропускною здатністю через обсяг даних, що проходять через сучасні високошвидкісні мережі зв'язку. NIDS, розгорнуті на ряді позицій у межах певної топології мережі, разом із HIDS та брандмауерами, можуть забезпечити конкретний, стійкий та багаторівневий захист як від зовнішніх, так і від внутрішніх атак.

У таблиці 2.4 наведено підсумок порівнянь між HIDS та NIDS.

Було запропоновано методологію HIDS із застосуванням розривних системних викликів із метою підвищення частоти виявлення, одночасно зменшуючи частоту помилкових тривог. Основна ідея полягає у використанні семантичної структури для системних викликів на рівні ядра, щоб зрозуміти аномальну поведінку програми.

Як показано в Таблиці 2.5 ряд систем AIDS також застосовується в мережевій системі виявлення вторгнень мережі (NIDS) та системі виявлення вторгнень хостів (HIDS) для підвищення ефективності виявлення за допомогою машинного навчання, заснованих на знаннях та статистичних схем.

Таблиця 2.4 – Порівняння типів технологій IDS на основі їх позиціонування в комп’ютерній системі

	Переваги	**Недоліки**	**Джерело даних**
HIDS	• HIDS може перевірити наскрізну поведінку зашифрованих комунікацій. • Не потрібно додаткового обладнання. • Виявляє вторгнення, перевіряючи файлову систему хостів, системні дзвінки або мережеві події. • Кожен пакет збирається повторно • Переглядає весь елемент, а не лише потоки	• Затримки у звітах про атаки • Споживає ресурси хосту • Потрібно встановити на кожному хості. • Він може контролювати атаки лише на машині, де він встановлений.	• Записи аудиту, файли журналів, інтерфейс прикладної програми (API), шаблони правил, системні дзвінки.
NIDS	• Виявляє атаки, перевіряючи мережеві пакети. • Не потрібно встановлювати на кожному хості. • Може перевірити різних хостів одночасно. • Можливість виявлення найширших діапазонів мережевих протоколів	• Завдання полягає у виявленні атак із зашифрованого трафіку. • Потрібне спеціальне обладнання. • Він підтримує лише ідентифікацію мережевих атак. • Складна для аналізу високошвидкісна мережа. • Найбільш серйозною загрозою є атака інсайдерів.	• Простий протокол управління мережею (SNMP) • Мережеві пакети (TCP / UDP / ICMP), • База інформації управління (MIB) • Записи маршрутизатора NetFlow

У таблиці 2.5 також наводяться приклади поточних підходів до виявлення вторгнень, де типи атак представлені в полі можливостей виявлення. Джерело даних включає системні дзвінки, інтерфейси прикладних програм, файли журналів, пакети даних, отримані в результаті добре відомих атак. Це джерело даних може бути корисним для класифікації поведінки вторгнень від ненормальних дій.

Таблиця 2.5 – Порівняння типів технологій IDS на прикладах з літератури. "P" вказує заздалегідь визначені атаки, а "Z" – атаки з нульовим днем

<table>
<tr><th colspan="3">Тип IDS</th><th>Можливість виявлення атак</th></tr>
<tr><td rowspan="4">Методи виявлення</td><td colspan="2">SIDS</td><td>P</td></tr>
<tr><td rowspan="3">AIDS</td><td>На основі статистики</td><td rowspan="3">Z</td></tr>
<tr><td>На основі знань</td></tr>
<tr><td>Машинне навчання</td></tr>
<tr><td colspan="2">AIDS + SIDS</td><td>P + Z</td></tr>
</table>

2.3 Методи впровадження AIDS

У цьому розділі представлений огляд підходів до AIDS, запропонованих останніми роками для підвищення точності виявлення та зменшення помилкових тривог.

Методи AIDS можна розділити на три основні групи: на основі статистики), на основі знань та на основі машинного навчання. Підхід, заснований на статистиці, передбачає збір та вивчення кожного запису даних у наборі елементів та побудову статистичної моделі нормальної поведінки користувачів. З іншого боку, заснована на знаннях система намагається ідентифікувати запитувані дії на основі існуючих системних даних, таких як специфікації протоколів та екземпляри мережевого трафіку, тоді як методи машинного навчання набувають складних можливостей узгодження шаблонів з навчальних даних. Ці три класи разом із прикладами їх підкласів показані на рис. 2.1.

2.4 Методи, засновані на статистиці

IDS, заснований на статистиці, створює модель розподілу для нормального профілю поведінки, потім виявляє низькоімовірні події та позначає їх як потенційні вторгнення. Статистичний AIDS по суті враховує такі статистичні показники, як медіана, середнє значення, режим та стандартне відхилення пакетів. Іншими словами, замість того, щоб перевіряти трафік даних, кожен пакет контролюється, що означає відбиток пальця потоку. Статистичний AIDS використовується для виявлення будь-

яких типів відмінностей у сучасній поведінці від нормальної поведінки. Статистичні IDS зазвичай використовують одну з наступних моделей.

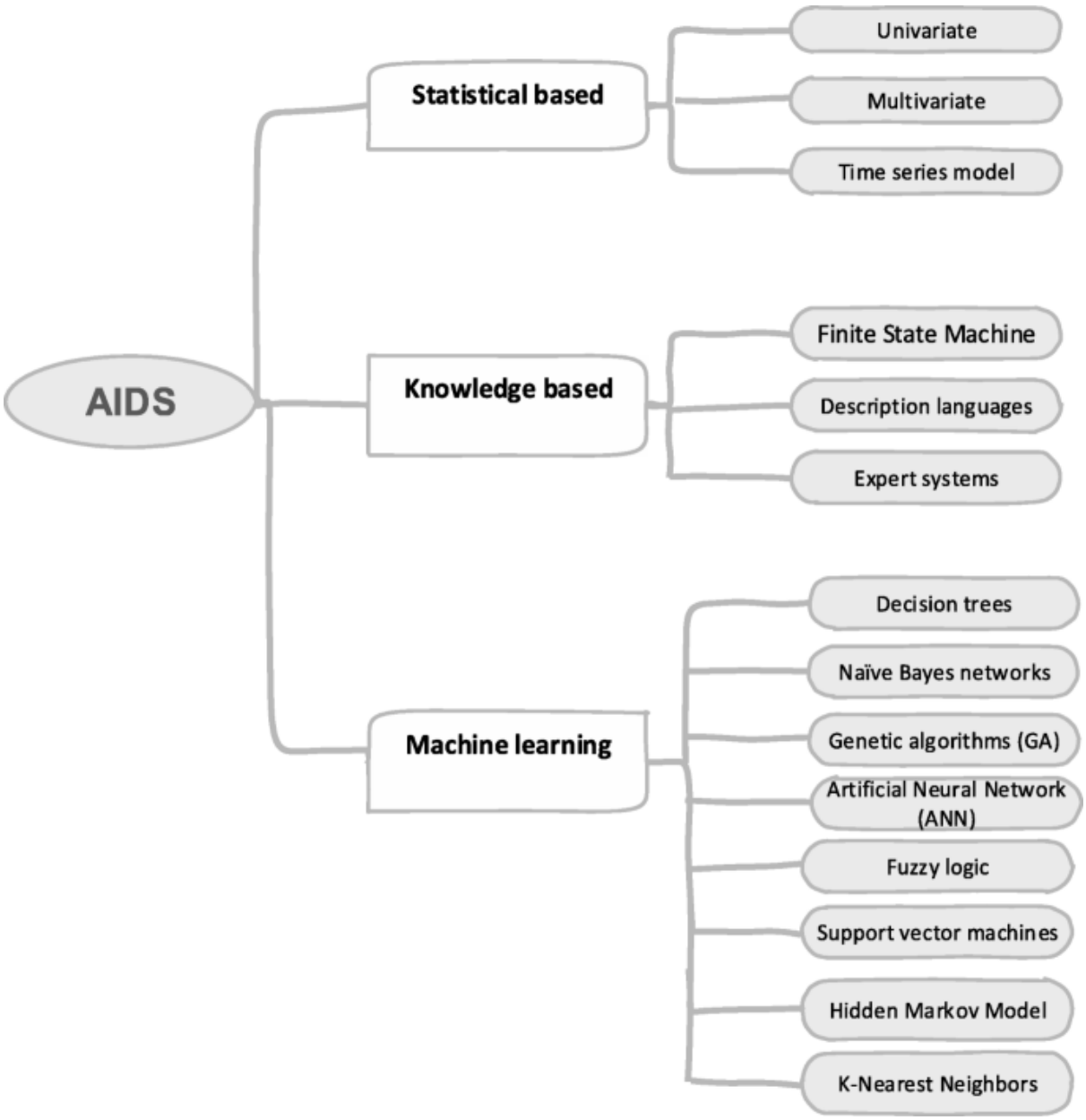

Рисунок 2.1 – Класифікація методів AIDS

Univariate: "Uni" означає "один", отже, це означає, що дані мають лише одну змінну. Цей прийом застосовується, коли статистичний нормальний профіль створюється лише для однієї міри поведінки в комп’ютерних системах. Однофакторні IDS шукають відхилення в кожній окремій метриці.

Багатовимірна: базується на взаємозв'язку двох або більше мір для того, щоб зрозуміти взаємозв'язки між змінними. Ця модель була б цінною, якщо експериментальні дані показують, що кращої класифікації можна досягти за допомогою комбінацій корельованих мір, а не аналізувати їх окремо. Є та ін. вивчити багатоваріантний метод контролю якості для виявлення вторгнень шляхом побудови довгострокового профілю звичайної діяльності. Основна проблема для багатовимірних статистичних ідентифікаторів полягає в тому, що важко оцінити розподіл для великих даних.

Модель часових рядів: часовий ряд – це серія спостережень, проведених протягом певного інтервалу часу. Нове спостереження є ненормальним, якщо його ймовірність виникнення на той момент занадто низька. Доцільність цієї техніки підтверджена за допомогою модельованих експериментів.

2.5 Методи, засновані на знаннях

Цю групу методів також називають методом експертної системи. Цей підхід вимагає створення бази знань, яка відображає законний профіль руху. Дії, що відрізняються від цього стандартного профілю, трактуються як вторгнення. На відміну від інших класів AIDS, стандартна модель профілю зазвичай створюється на основі людських знань, з точки зору набору правил, які намагаються визначити нормальну діяльність системи.

Головною перевагою методів, заснованих на знаннях, є здатність зменшувати помилково позитивні тривоги, оскільки система має знання про всі нормальні способи поведінки. Однак у динамічно мінливих обчислювальних середовищах цей тип IDS потребує регулярного оновлення знань щодо очікуваної нормальної поведінки, що є трудомістким завданням, оскільки збирати інформацію про всі нормальні способи поведінки дуже складно.

Кінцевий автомат (FSM): FSM – це обчислювальна модель, яка використовується для представлення та управління потоком виконання. Ця модель може бути застосована при виявленні вторгнень для створення моделі системи

виявлення вторгнень. Як правило, модель представлена у формі станів, переходів та видів діяльності. Стан перевіряє дані історії. FSM може представляти законну поведінку системи, і будь-яке відхилення від цього FSM розглядається як атака.

Мова опису: Мова опису визначає синтаксис правил, за допомогою яких можна вказати характеристики визначеної атаки. Правила можуть створюватися мовами опису, такими як N-граматика та UML.

Експертна система: Експертна система включає ряд правил, що визначають атаки. У експертній системі правила, як правило, визначаються вручну інженером, що працює у співпраці з експертом доменів.

Аналіз підписів: це найдавніша техніка, що застосовується в IDS. Він спирається на просту ідею узгодження рядків. При збігу рядків вхідний пакет перевіряється, слово за словом, з чітким підписом. Якщо підпис відповідає, піднімається попередження. Якщо ні, інформація в трафіку потім узгоджується з такою сигнатурою у базі даних сигнатур.

2.6 AIDS на основі техніки машинного навчання

Машинне навчання – це процес вилучення знань із великої кількості даних. Моделі машинного навчання складаються з набору правил, методів або складних «передавальних функцій», які можна застосувати для пошуку цікавих зразків даних або для розпізнавання або передбачення поведінки.

Методи машинного навчання широко застосовуються в галузі AIDS. Кілька алгоритмів та методів, таких як кластеризація, нейронні мережі, правила асоціацій, дерева рішень, генетичні алгоритми та методи найближчих сусідів, були застосовані для виявлення знань із наборів даних про вторгнення.

На основі методів машинного навчання, як показано на рис. 2.2, створені різні AIDS. Метою використання методів машинного навчання є створення IDS з підвищеною точністю та меншими вимогами до людських знань. За останні кілька років кількість AIDS, який використовував методи машинного навчання, збільшується.

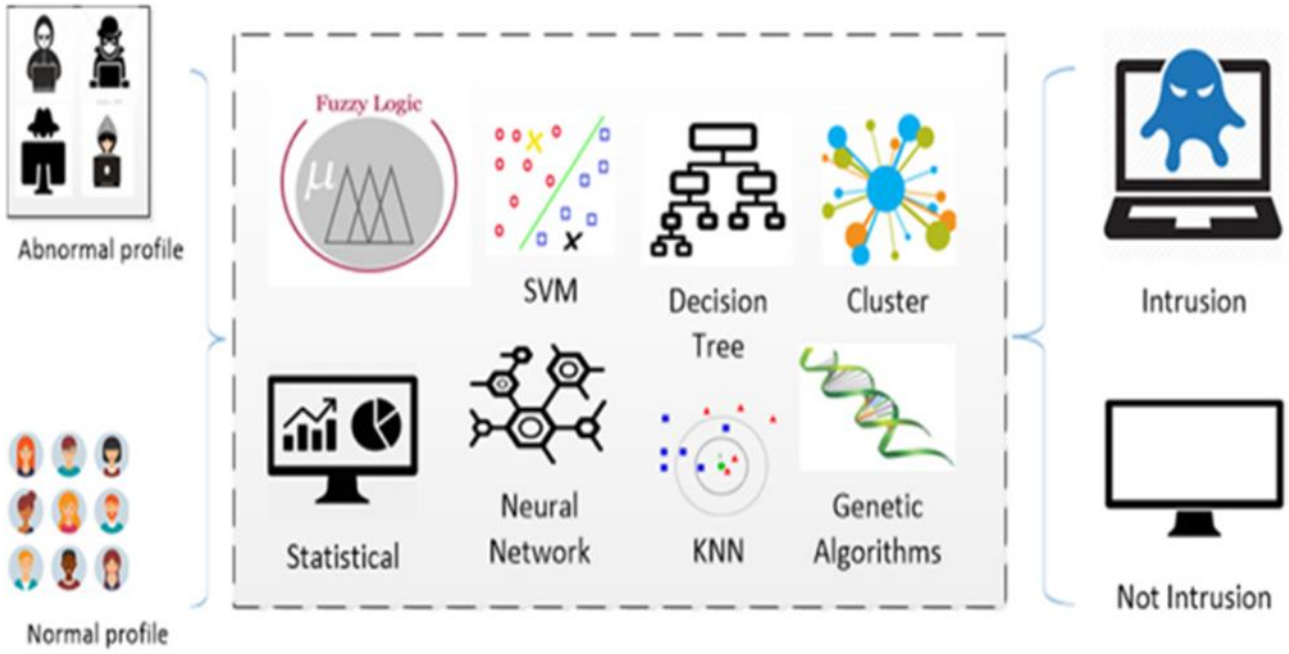

Рисунок 2.2 – Концептуальна робота підходів до AIDS на основі машинного навчання

Ключовим напрямком IDS, заснованого на дослідженнях машинного навчання, є виявлення закономірностей та побудова системи виявлення вторгнень на основі набору даних. Як правило, існує два види методів машинного навчання: під наглядом і без нагляду.

У цьому розділі представлені різні методи навчання під наглядом для IDS. Кожна техніка представлена детально, а також представлені посилання на важливі наукові публікації.

Методи IDS, що базуються на навчанні, виявляють вторгнення за допомогою промаркованих навчальних даних. Підхід під контролем навчання зазвичай складається з двох етапів, а саме навчання та тестування. На етапі навчання визначаються відповідні ознаки та класи, а потім алгоритм вивчає ці зразки даних. У контрольованому навчанні IDS кожен запис є парою, що містить мережеве або хостове джерело даних та пов'язане з цим вихідне значення (тобто мітку), а саме втручання або нормальне.

Далі можна застосувати вибір функцій для усунення непотрібних функцій. Використовуючи дані навчання для вибраних функцій, контрольована техніка навчання потім використовується для підготовки класифікатора для вивчення властивого зв'язку між вхідними даними та позначеним вихідним значенням. У літературі досліджено широкий спектр контрольованих методів навчання, кожен із яких має свої переваги та недоліки.

На етапі тестування навчена модель використовується для класифікації невідомих даних до вторгнень або нормального класу. Потім отриманий класифікатор стає моделлю, яка з урахуванням набору значень ознак передбачає клас, до якого можуть належати вхідні дані. На рисунку 2.3 показано загальний підхід до застосування методів класифікації. Ефективність класифікатора в спроможності передбачити правильний клас вимірюється за допомогою ряду показників, що обговорюється в розділі 4.

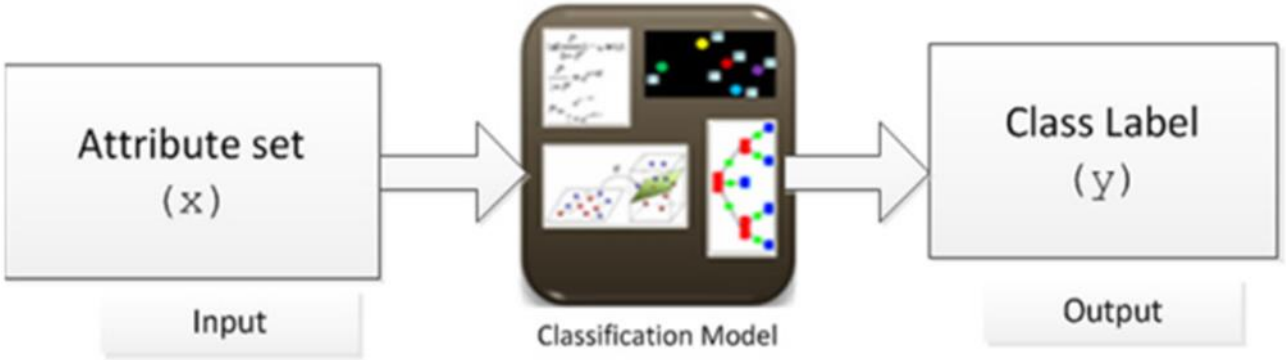

Рисунок 2.3 – Класифікація як завдання

Існує багато методів класифікації, таких як дерева рішень, системи, що базуються на правилах, нейронні мережі, векторні машини підтримки, Н. Байєс та метод найближчого сусіда. Кожна техніка використовує метод навчання для побудови класифікаційної моделі. Однак відповідний підхід до класифікації повинен не лише обробляти дані про навчання, але він також повинен точно визначати клас записів, яких він ще ніколи не бачив. Створення класифікаційних моделей з надійними узагальнювальними можливостями є важливим завданням алгоритму навчання.

Дерева рішень: Дерево рішень складається з трьох основних компонентів. Перший компонент – це вузол прийняття рішення, який використовується для ідентифікації атрибута тесту. Друга – це гілка, де кожна гілка представляє можливе рішення на основі значення тестового атрибута. Третій – це лист, який містить клас, до якого належить екземпляр.

Н. Байєс: Цей підхід заснований на застосуванні принципу Байєса з чіткими припущеннями про незалежність серед ознак. Метод відповідає на запитання типу "яка ймовірність того, що відбувається певний вид атаки, враховуючи спостережувану системну діяльність?" застосовуючи формули умовної ймовірності. Наївний Байєс покладається на особливості, які мають різну ймовірність виникнення в атаках та в нормальній поведінці. Модель класифікації Н.Байєса є однією з найбільш поширених моделей в IDS завдяки простоті використання та ефективності розрахунків, обидві взяті з її властивості умовного припущення про незалежність.

Однак система погано функціонує, якщо це припущення про незалежність не є дійсним, як було продемонстровано на наборі даних про виявлення вторгнень KDD'99, який має складні залежності атрибутів. Результати також показують, що модель Байєса знижує точність для великих наборів даних. Подальше дослідження показало, що більш досконала модель (HNB) може бути застосована до завдань IDS, що включають високу розмірність, надзвичайно взаємопов'язані атрибути та високошвидкісні мережі.

Генетичні алгоритми (GA): Генетичні алгоритми – це евристичний підхід до оптимізації, заснований на принципах еволюції. Кожне можливе рішення представлене у вигляді серії бітів (генів) або хромосоми, а якість розчинів з часом покращується завдяки застосуванню операторів відбору та відтворення, упереджених на користь монтерних рішень. Застосовуючи генетичний алгоритм до проблеми класифікації вторгнень, зазвичай існує два типи кодування хромосом: один – відповідно до кластеризації, щоб генерувати двійковий метод кодування хромосом; інший – вказання центру кластера (матриця прототипу кластеризації) за допомогою цілочисельної кодуючої хромосоми. Мюррей та ін., Використовували GA для вироблення простих правил мережевого трафіку. Кожне правило представлене

геномом, а первинна популяція геномів – це ряд випадкових правил. Кожен геном складається з різних генів, які відповідають таким характеристикам, як джерело IP, призначення IP, джерело порту, призначення порту та один тип протоколу.

Штучна нейронна мережа (ANN): ANN є одним із найбільш широко застосовуваних методів машинного навчання, і, як було показано, він успішно виявляє різні шкідливі програми. Найбільш частою технікою навчання, що застосовується для навчання під наглядом, є алгоритм зворотного розповсюдження (BP). Алгоритм BP оцінює градієнт помилки мережі щодо її ваг, що піддаються модифікації. Однак для IDS на базі ANN точність виявлення, особливо для менш частих атак, і точність виявлення все ще потребують вдосконалення.

Навчальний набір даних для менш частих атак невеликий у порівнянні з набором більш частих атак, і це ускладнює для ANN правильне вивчення властивостей цих атак. Як результат, точність виявлення нижча для менш частих атак. У сфері інформаційної безпеки величезна шкода може статися, якщо не виявити низькочастотні атаки.

Наприклад, якщо атаки User Root (U2R) ухиляються від виявлення, кіберзлочинець може отримати привілеї авторизації кореневого користувача і тим самим здійснювати шкідливі дії в комп'ютерних системах жертви. Крім того, менш поширені напади часто є винятком. ANN часто страждають від місцевих мінімумів, і, отже, навчання може зайняти багато часу. Сила ANN полягає в тому, що за допомогою одного або декількох прихованих шарів він здатний створювати сильно нелінійні моделі, які фіксують складні взаємозв'язки між вхідними атрибутами та мітками класифікації. З розвитком багатьох варіантів, таких як періодичні та згорткові NN, ANN є потужним інструментом у багатьох задачах класифікації, включаючи IDS.

Нечітка логіка: ця методика базується на ступенях невизначеності, а не на типовій істинній або хибній булевій логіці, на якій створені сучасні ПК. Отже, він представляє прямий спосіб дійти до остаточного висновку на основі неясних, неоднозначних, галасливих, неточних або відсутніх вхідних даних. З нечітким

доменом нечітка логіка дозволяє екземпляру належати, можливо частково, одночасно до декількох класів.

Тому нечітка логіка є хорошим класифікатором для проблем IDS, оскільки сама безпека включає нечіткість, а межа між нормальним та аномальним станами недостатньо чітко визначена. Крім того, проблема виявлення вторгнень містить різні числові особливості у зібраних даних та кілька похідних статистичних показників. Побудова IDS на основі числових даних з жорсткими порогами виробляє високі помилкові тривоги.

Діяльність, яка лише незначно відхиляється від моделі, не може бути розпізнана або незначна зміна нормальної активності може спричинити помилкові тривоги. За допомогою нечіткої логіки можна змоделювати цю незначну аномалію, щоб зберегти низькі показники хибних ставок. За допомогою нечіткої логіки частоту помилкових тривог при визначенні нав'язливих дій можна зменшити. Було окреслено групу нечітких правил для опису нормальної та ненормальної діяльності в комп’ютерній системі та механізм нечітких умовиводів для визначення вторгнень.

Підтримуючі векторні машини (SVM): SVM – це дискримінаційний класифікатор, який визначається розділовою гіперплощиною. SVM використовують функцію ядра для відображення навчальних даних у просторішій області, щоб вторгнення було лінійно класифіковано. SVM добре відомі своїми можливостями узагальнення і в основному є цінними, коли кількість атрибутів велика, а кількість точок даних невелика. Різні типи розділювальних гіперплощин можна досягти, застосувавши ядро, таке як лінійна, поліноміальна, Гауссова радіальна базова функція (RBF) або гіперболічний тангенс. У наборах даних IDS багато функцій надлишкові або менш впливові при поділі точок даних на правильні класи. Тому вибір особливостей слід враховувати під час навчання SVM. SVM також може бути використаний для класифікації в декілька класів.

Прихована модель Маркова (HMM): HMM – це статистична модель Маркова, в якій процес, що моделюється, вважається марківським процесом з невидимими даними. У цій техніці прихована модель Маркова тренується щодо відомих функцій шкідливого програмного забезпечення (наприклад, послідовності коду операцій), і

після завершення етапу навчання, навчена модель застосовується для оцінки вхідного трафіку. Потім оцінка протиставляється заздалегідь визначеному порогу, а оцінка, більша за порогову, вказує на шкідливе програмне забезпечення. Так само, якщо оцінка менша за порогову, трафік визначається як нормальний.

Класифікатор K-Найближчі сусіди (KNN): Методи k-найближчого сусіда (k-NN) є типовим непараметричним класифікатором, що застосовується в машинному навчанні. Ідея цих методів полягає у присвоєнні неміченої вибірки даних класу його k найближчих сусідів (де k – ціле число, що визначає кількість сусідів, які слід врахувати). Рисунок 2.4 ілюструє класифікатор K-Найближчих сусідів, де k = 5. Точка X – це екземпляр немаркованих даних, який потрібно класифікувати. Серед п’яти найближчих сусідів X є три подібні моделі з класу Вторгнення та два з класу Нормальний. Отримавши більшість голосів, можна віднести X до класу Вторгнення.

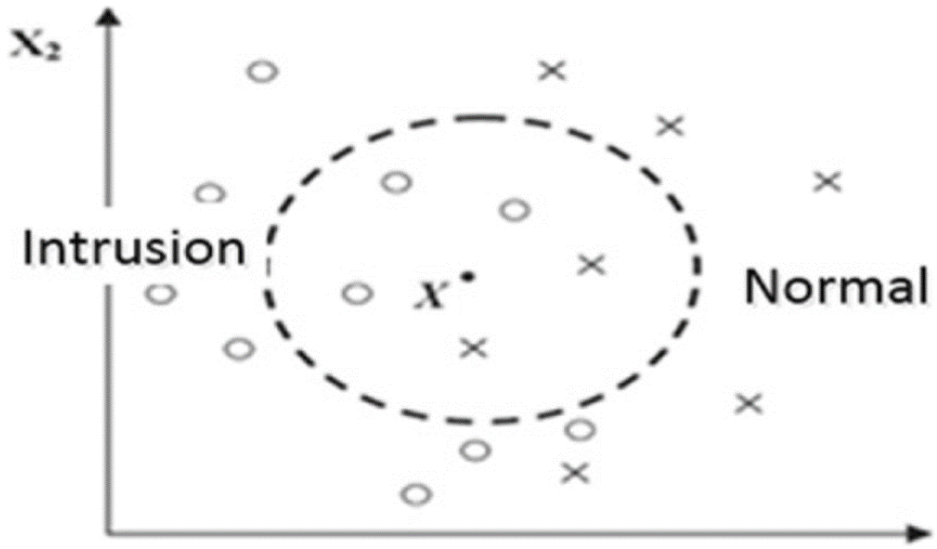

Рисунок 2.4 – Приклад класифікації за k-найближчим сусідом для k = 5

k-NN може бути належним чином застосований як еталон для всіх інших класифікаторів, оскільки він забезпечує хороші показники класифікації в більшості IDS.

2.7 Навчання без нагляду в системі виявлення вторгнень

Навчання без нагляду – це форма техніки машинного навчання, яка використовується для отримання цікавої інформації з наборів вхідних даних без міток класів. Точки вхідних даних зазвичай трактуються як набір випадкових величин. Потім для набору даних створюється модель спільної щільності. При контрольованому навчанні вихідні мітки даються і використовуються для навчання машини для отримання необхідних результатів для невидимої точки даних, тоді як при неконтрольованому навчанні мітки не даються, і натомість дані автоматично групуються в різні класи в процесі навчання . У контексті розробки IDS, некерованих засобів навчання, використання механізму ідентифікації вторгнень за допомогою немаркованих даних для підготовки моделі.

Як показано на рис. 2.5 , після того, як записи кластеризовані, усі випадки, що з'являються в невеликих кластерах, позначаються як вторгнення, оскільки звичайні випадки повинні створювати значні кластери порівняно з аномаліями. Крім того, зловмисні вторгнення та звичайні екземпляри неоднакові, тому вони не потрапляють в однаковий кластер.

K-означає: Методи K-означає – це одна з найбільш поширених технік кластерного аналізу, яка має на меті розділити "n" об'єктів даних на "k" кластери, в яких кожен об'єкт даних обраний у кластері з найближчим середнім значенням. Це метод кластеризації на основі відстані, і йому не потрібно обчислювати відстані між усіма комбінаціями записів. Він застосовує евклідову метрику як міру подібності. Кількість кластерів визначається користувачем заздалегідь.

Зазвичай кілька рішень перевіряються перед прийняттям найбільш прийнятного. Кластеризація k-середніх засобів є кращим підходом для класифікації даних із використанням некерованих методів виявлення вторгнень, коли доступні декілька типів наборів даних. Кластеризація може використовуватися в IDS для зменшення сигнатур вторгнень, створення високоякісного підпису або групового подібного вторгнення.

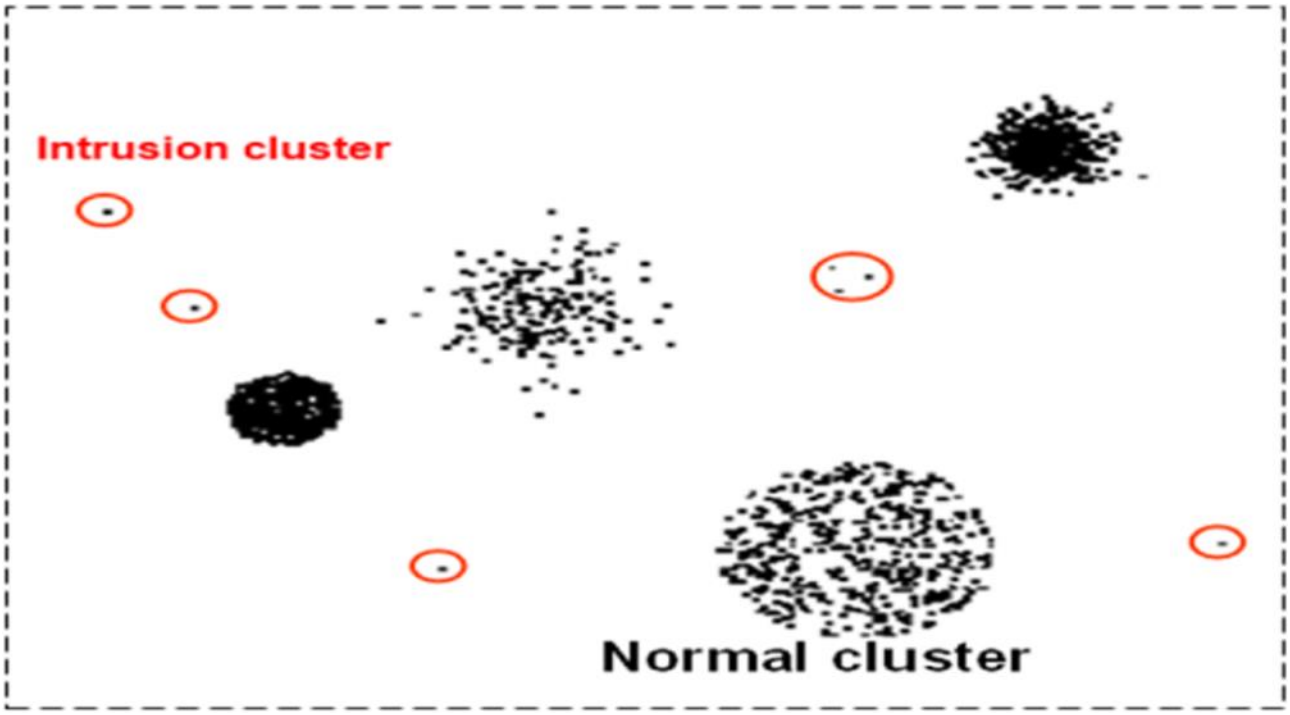

Рисунок 2.5 – Використання кластеризації для виявлення вторгнень

Ієрархічна кластеризація: це техніка кластеризації, метою якої є створення ієрархії кластерів. Підходи до ієрархічної кластеризації зазвичай класифікуються на дві категорії:

Агломеративні – методи кластеризації знизу вгору, коли кластери мають підкластери, які, в свою чергу, мають підкластери, а пари кластерів поєднуються, коли один рухається вгору по ієрархії.

Розділення – ієрархічні алгоритми кластеризації, де ітеративно виділяється кластер із найбільшим діаметром у просторі об’єктів та розділяється на двійкові підкластери з нижчим діапазоном.

2.8 Навчання під наглядом

Навчання під наглядом розподіляється між навчанням під наглядом (із повністю маркованими даними про навчання) та навчанням без нагляду (без будь-яких класифікованих даних про навчання). Дослідники показали, що навчання під напівконтролем може використовуватися разом із невеликим обсягом ефективності маркованого класифікатора даних для IDS з меншими витратами часу та витрат. Це є

цінним, оскільки для багатьох питань IDS марковані дані можуть бути рідкісними або випадковими. Експериментальні результати з використанням цього напівконтрольного виявлення вторгнень на наборі даних NSL-KDD показують, що немічені зразки, що належать до груп з низькою та високою розмитістю, вносять головний внесок у підвищення точності IDS, протиставлених традиційним.

2.9 Ансамблеві методи

Кілька алгоритмів машинного навчання можуть бути використані для отримання кращих результатів прогнозування, ніж будь-який із складових алгоритмів навчання. Запропоновано ряд різних ансамблевих методів, таких як посилення, завантаження та укладання.

Підсилення відноситься до сімейства алгоритмів, які здатні перетворити слабких учнів на сильних. Підсилення означає підготовку одного і того ж класифікатора на різних підмножинах одного і того ж набору даних. Стек поєднує різні класифікації за допомогою мета-класифікатора. Моделі базового рівня будуються на основі цілого навчального набору, потім мета-модель навчається на виходах моделі базового рівня як атрибути.

2.10 Гібридні методи

Традиційні IDS мають обмеження: їх неможливо легко змінити, неможливість ідентифікувати нові шкідливі атаки, низьку точність та високу кількість помилкових тривог. Там, де AIDS має такі обмеження, як високий показник помилково позитивних показників. Гібридна IDS базується на поєднанні AIDS та AIDS. Гібридна IDS долає недоліки AIDS та AIDS. Автори в [27] запропонували гібридні IDS, використовуючи Naive Bayes та дерево рішень, і досягли рівня виявлення 99,63% на наборі даних KDD'99.

РОЗДІЛ 3
ПОКАЗНИКИ ЕФЕКТИВНОСТІ ДЛЯ IDS

Існує багато метрик класифікації IDS, деякі з яких відомі під кількома назвами. У таблиці 3.1 наведена матриця плутанини для двокласного класифікатора, який може бути використаний для оцінки ефективності IDS. Кожен стовпець матриці представляє екземпляри у передбачуваному класі, тоді як кожен рядок представляє екземпляри у фактичному класі.

Таблиця 3.1 – Матриця плутанини для системи IDS

	Прогнозований клас		
Фактичний клас	Клас	Звичайний	Напад
	Звичайний	Справжній негатив (TN)	Хибнопозитивний (FP)
	Напад	Хибнонегативний (FN)	Справжній позитив (TP)

IDS зазвичай оцінюються на основі наступних стандартних показників ефективності

Правильний позитивний коефіцієнт (True Positive Rate – TPR): він обчислюється як співвідношення між кількістю правильно передбачених атак та загальною кількістю атак. Якщо виявляються всі вторгнення, тоді TPR дорівнює 1, що надзвичайно рідко для IDS. TPR також називають швидкістю виявлення (Detection Rate – DR) або чутливістю. TPR можна виразити математично як

$$TPR = TPTP + FN \tag{3.1}$$

Помилковий позитивний показник (FPR): він обчислюється як відношення між кількістю звичайних випадків, неправильно класифікованих як атака, та загальною кількістю звичайних випадків.

$$FPR = FPFP + TN \tag{3.2}$$

Помилковий негативний коефіцієнт (FNR): помилково негативний означає, що детектор не виявляє аномалію та класифікує її як нормальну. FNR можна виразити математично як:

$$FNR = FNFN + TP \tag{3.3}$$

Швидкість класифікації (CR) або точність: CR вимірює, наскільки точно IDS визначає нормальну або аномальну поведінку дорожнього руху. Це описується як відсоток усіх тих правильно передбачених екземплярів до всіх екземплярів:

$$\text{Точність} = TP + TNTP + TN + FP + FN \tag{3.4}$$

Крива робочої характеристики приймача (ROC): ROC має FPR на осі x та TPR на осі y. На кривій ROC TPR будується як функція FPR для різних точок відсічення. Кожна точка на кривій ROC представляє пару FPR і TPR, що відповідає певному порогу прийняття рішення. Оскільки поріг для класифікації змінюється, вибирається інша точка на ROC з різною швидкістю помилкової тривоги (FAR) та іншим TPR. Тест з ідеальною дискримінацією (без перекриття в двох розподілах) має криву ROC, яка проходить через лівий верхній кут (100% чутливість, 100% специфічність). Крива ROC зображена на рис. 3.1.

3.1 Набори даних для виявлення вторгнень

Набори даних оцінки відіграють життєво важливу роль у валідації будь-якого підходу IDS, дозволяючи нам оцінити здатність запропонованого методу виявляти нав'язливу поведінку. Набори даних, що використовуються для аналізу мережевих пакетів у комерційних продуктах, недоступні через проблеми конфіденційності.

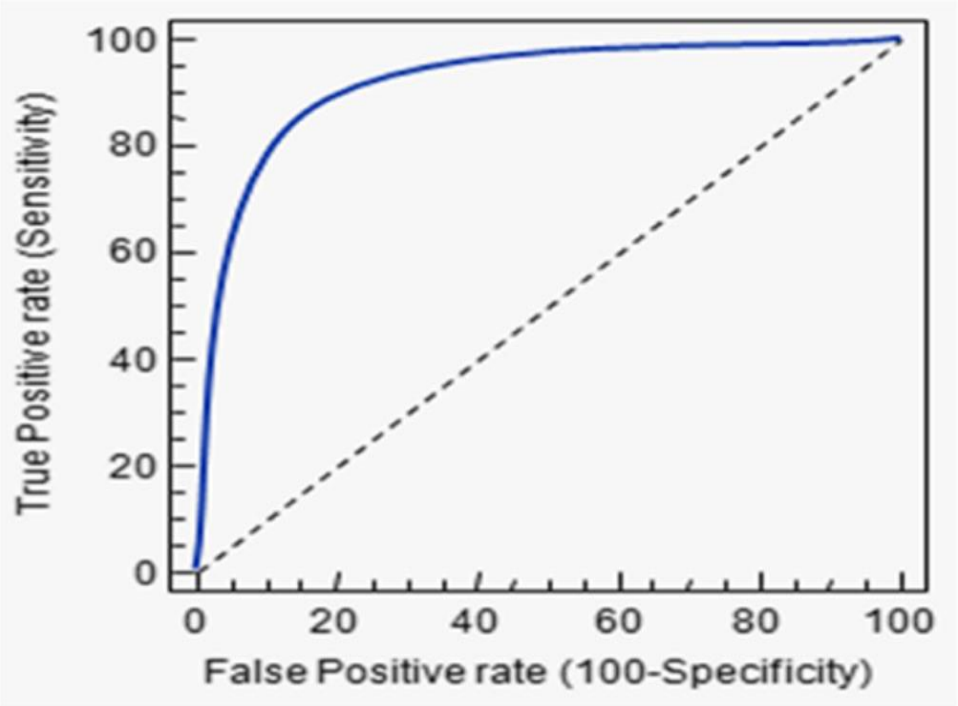

Рисунок 3.1 – Крива ROC

Однак існує кілька загальнодоступних наборів даних, таких як DARPA, KDD, NSL-KDD та ADFA-LD, і вони широко використовуються як еталони. Існуючі набори даних, які використовуються для побудови та порівняльної оцінки IDS, обговорюються в цьому розділі разом із їх особливостями та обмеженнями.

DARPA / KDD Cup99. Найбільш ранні зусилля для створення набору даних IDS було зроблено DARPA (Агентство перспективних дослідницьких досліджень оборони) в 1998 році, і вони створили набір даних KDD98 (Knowledge Discovery and Data Mining (KDD)). У 1998 році DARPA запровадив програму в лабораторіях MIT Lincoln Labs для забезпечення всебічного та реалістичного середовища порівняльного аналізу IDS. Незважаючи на те, що цей набір даних був важливим внеском у дослідження IDS, його точність та здатність враховувати реальні умови широко критикуються.

Ці набори даних були зібрані за допомогою декількох комп'ютерів, підключених до Інтернету, для моделювання невеликої бази ВПС США з обмеженим персоналом. Зібрано мережеві пакети та файли журналів хостів. Компанія Lincoln Labs побудувала експериментальний стенд, щоб отримати 2 місяці скидання пакетів

TCP для локальної мережі (LAN), моделюючи звичайну локальну мережу ВПС США. Вони змоделювали локальну мережу так, ніби це справжнє середовище ВПС, але переплели її кількома модельованими вторгненнями.

Зібрані мережеві пакети складали близько чотирьох гігабайт, що містили близько 4 900 000 записів. Тестові дані за 2 тижні мали близько 2 мільйонів записів про підключення, кожен з яких мав 41 функцію і був класифікований як нормальний або ненормальний.

Видобуті дані являють собою серію TCP-сесій, що починаються і закінчуються у чітко визначений час, між якими дані надходять до вихідної IP-адреси та до цільової IP-адреси, яка містить велику кількість атак, що моделюються у середовищі військової мережі. Набір даних DARPA 1998 р. був використаний як основа для виведення набору даних KDD Cup99, який був використаний у Третьому міжнародному конкурсі інструментів виявлення знань та обробки даних.

Ці набори даних застаріли, оскільки не містять записів останніх атак шкідливих програм. Наприклад, поведінка зловмисників відрізняється в різних топологіях мережі, операційних системах та наборах програмного забезпечення та злочинів. Тим не менш, KDD99 продовжує використовуватися як орієнтир у дослідницькому співтоваристві IDS і в даний час використовується дослідниками.

CAIDA. Цей набір даних містить трафік мережевого трафіку від атак DDoS (Distributed Denial-of-Service) і був зібраний у 2007 році. Цей тип атаки відмови в обслуговуванні намагається перервати звичайний трафік цільового комп'ютера або мережі, переповнюючи ціль потоком мережевих пакетів, не даючи регулярному трафіку дістатися до законного комп'ютера призначення. Одним недоліком набору даних CAIDA є те, що він не містить різноманітності атак. Крім того, зібрані дані не містять особливостей усієї мережі, що ускладнює розрізнення ненормальних та нормальних потоків руху.

NSL-KDD. NSL-KDD – це загальнодоступний набір даних, який був розроблений на основі попереднього набору даних KDD cup99. Статистичний аналіз, проведений на наборі даних cup99, порушив важливі проблеми, які сильно впливають на точність виявлення вторгнень, і призводить до оманливої оцінки AIDS.

Основною проблемою набору даних KDD є величезна кількість повторюваних пакетів. Приблизно 75%. Ця величезна кількість повторюваних екземплярів у навчальному наборі могла б вплинути на зміщення методів машинного навчання до нормальних екземплярів і тим самим запобігти їх вивченню нерегулярних екземплярів, які, як правило, більше шкодять комп’ютерній системі.

Набір даних поїзда NSL-KDD складається з 125973 записів, а тестовий набір містить 22544 записи. Розмір набору даних NSL-KDD достатній, щоб було практично використовувати весь набір даних NSL-KDD без необхідності вибіркової вибірки. Це дало послідовні та порівнянні результати різних дослідницьких робіт. Набір даних NSL_KDD складається з 22 атак навчальних вторгнень та 41 атрибута (тобто особливостей). У цьому наборі даних 21 атрибут відноситься до самого з'єднання, а 19 атрибутів описують природу з'єднань всередині одного хоста.

ISCX 2012. У цьому наборі даних проаналізовано реальні трафіки мережевого трафіку для виявлення нормальної поведінки комп’ютерів із реального трафіку протоколів HTTP, SMTP, SSH, IMAP, POP3 та FTP. Цей набір даних базується на реалістичному мережевому трафіку, який позначений і містить різноманітні сценарії атак.

ADFA-LD та ADFA-WD. Дослідники Австралійської академії оборонних сил створили два набори даних (ADFA-LD та ADFA-WD) як загальнодоступні набори даних, що представляють структуру та методологію сучасних атак. Набори даних містять записи як з операційних систем Linux, так і з Windows; вони створені на основі оцінки системного виклику HIDS. Ubuntu Linux версії 11.04 використовувався як основна операційна система для побудови ADFA-LD. Деякі випадки атак у ADFA-LD були отримані від нового шкідливого програмного забезпечення нульового дня, що робить цей набір даних придатним для висвітлення відмінностей між підходами SIDS та AIDS до виявлення вторгнень. Він включає три різні категорії даних, кожна група даних містить необроблені сліди системних викликів. Кожен набір навчальних даних був зібраний у хосту для звичайних дій, поведінка користувачів варіювалась від перегляду веб-сторінок до підготовки документів LATEX.

CICIDS 2017. Набір даних CICIDS2017 включає як доброякісну поведінку, так і деталі нових атак шкідливого програмного забезпечення: таких як Brute Force FTP, Brute Force SSH, DoS, Heartbleed, Web Attack, Infiltration, Botnet та DDoS . Цей набір даних позначається на основі мітки часу, IP-адреси джерела та призначення, портів джерела та призначення, протоколів та атак. Повна топологія мережі була налаштована для збору цього набору даних, який містить модем, брандмауер, комутатори, маршрутизатори та вузли з різними операційними системами (Microsoft Windows (наприклад, Windows 10, Windows 8, Windows 7 та Windows XP), macOS iOS від Apple і операційна система з відкритим кодом Linux). Цей набір даних містить 80 функцій мережевого потоку із захопленого мережевого трафіку.

3.2 Порівняння загальнодоступних наборів даних IDS

Оскільки в AIDS застосовуються методи машинного навчання, набори даних, що використовуються для методів машинного навчання, дуже важливі для оцінки цих методів для реалістичної оцінки. У таблиці 3.2 узагальнено популярні загальнодоступні масиви даних, а також деякі методи аналізу та результати для кожного набору даних за попередніми дослідженнями. У таблиці 3.3 узагальнено характеристики наборів даних.

Таблиця 3.2 – Порівняння результатів, досягнутих різними методами на загальнодоступних наборах даних IDS

Набір даних	**Результат**	**Спостереження**
DARPA 98	При виявленні Snort, 69% від загальної кількості створених попереджень вважаються помилковими тривогами.	SIDS застосовується без AIDS
	Системні дзвінки ANN-аналізу, 96% виявлення.	Для підготовки та тестування фреймворку було виконано класифікатор на основі штучної нейронної мережі (ANN).
	SVM на підмножині DARPA 98, 99,6% коефіцієнт виявлення.	SVM виділяє інформацію в різні класи за допомогою гіперплану або гіперплощин, оскільки він може мати справу з багатовимірною

Набір даних	Результат	Спостереження
		інформацією. SVM зазвичай демонструють хорошу продуктивність для задач бінарного класу.
KDDCUP 99	Багатовимірний статистичний аналіз аудиторських даних, рівень виявлення 90%	Багатофакторне використовується для зменшення частоти помилкових тривог.
	Найкращих результатів досяг алгоритм C4.5, який досягає істинної позитивної ставки 95%.	Дерева рішень, створені за C4.5, можуть бути використані для класифікації
	Класифікатор SMO 97% коефіцієнт виявлення.	Цей класифікатор на основі SVM з реалізацією SMO забезпечує високу точність виявлення. Однак точність повідомляється менше, ніж у (Chen et al., 2005), оскільки набір даних KDDCUP 99 є більш складним та вичерпним, ніж набір даних DARPA 98.
	Найкраща модель – це модель HNB, де для порівняння моделей використовується рівень довіри 95%.	Методи прихованого наївного Байєса (HNB) можуть бути застосовані до області IDS, яка страждає від розмірності, високо асоційованих атрибутів та високої швидкості мережі. Техніка HNB краща за методику, засновану на традиційному методі NB, з точки зору точності виявлення для IDS.
NSL-KDD	Алгоритм K-Найближчий сусід (k-NN), рівень виявлення 94%.	Алгоритм k-NN використовує всі позначені навчальні екземпляри як модель цільової функції. На етапі класифікації k-NN використовує стратегію пошуку на основі подібності для визначення локально оптимальної функції гіпотези.
	Nave Bayes, рівень виявлення становить 89%.	Байєсові класифікатори забезпечують помірну точність, оскільки основна увага приділяється класифікації класів для екземплярів, а не точних ймовірностей.
	C4.5 дав найкращий рівень виявлення 99%.	C4.5 вибирає функцію даних, яка найбільш ефективно ділить набір вибірки на підмножини, сприяючи підвищенню точності
	Класифікатор SMO, рівень виявлення становить 97%.	У роботі також використовується класифікатор на основі SVM і досягається рівень виявлення, подібний до (Chen et al., 2005).
	Кластеризація максимізації очікувань (EM), точність 78%	EM формує "м'яке" завдання кожного рядка для різних кластерів у відсотках до ймовірності кожного кластера. Точність у цьому методі низька, оскільки EM не дає матриці коваріації параметрів для стандартних помилок
ADFA-WD	Кріч та ін. використовували приховану модель Маркова (HMM), машину екстремального навчання (ELM) та SVM. Вони повідомили про точність 74,3% для HMM, 98,57% про точність для ELM та 99,64% про точність для SVM.	ADFA-WD – це набагато новий набір даних і містить нові атаки. Ось чому точність повідомлень була не такою хорошою, як для кожної техніки машинного навчання, порівняно з точністю із використанням застарілих даних KDD98. Як повідомляється, SVM забезпечує найвищу точність.

Набір даних	Результат	Спостереження
ADFA-LD	100% точність використання ELM із використанням оригінальної семантичної функції	Застосовуються нові семантичні ознаки. Тому ELM здатні легко та швидко використовувати нову семантичну функцію, включаючи кількість семантичних фраз.
CICIDS2017	Виявляється точність 94,5%, отримана лише за допомогою MLP, за допомогою MLP та класифікатора корисного навантаження разом із рівнем точності 95,2%.	Вибір функції здійснюється за допомогою алгоритму оцінки Фішера.
Бот-IoT	Найвища точність у моделі SVM. 98% коефіцієнт виявлення	Цей метод, заснований на SVM, забезпечив хорошу точність виявлення (Mitchell & Chen, 2015 ; Chen et al., 2005 ; Ferrari & Cribari-Neto, 2004)

Таблиця 3.3 – Порівняння наборів даних ("+" = True, "-" = False)

Набір даних	Реалістичний рух	Дані етикетки	Сліди IoT	Атаки з нульовим днем	Повний пакет захоплений	Рік
DARPA 98	+	+	-	-	+	1998 рік
KDDCUP 99	+	+	-	-	+	1999 рік
CAIDA	+	-	-	-	-	2007 рік
NSL-KDD	+	+	-	-	+	2009 рік
ISCX 2012	+	+	-	-	+	2012 рік
ADFA-WD	+	+	-	+	+	2014 рік
ADFA-LD	+	+	-	+	+	2014 рік
CICIDS2017	+	+	-	+	+	2017 рік
Бот-IoT	+	+	+	+	+	2018 рік

3.3 Вибір функцій для IDS

Вибір функцій корисний для зменшення обчислювальних труднощів, усунення надмірності даних, підвищення швидкості виявлення методів машинного навчання, спрощення даних та зменшення помилкових тривог. У цьому напрямі досліджень було застосовано деякі методи для розробки полегшених IDS.

Методи вибору об’єктів можна класифікувати за методами обгортки та фільтрування. Методи обгортки оцінюють підгрупи змінних для виявлення можливих взаємодій між змінними. Є два основні недоліки цих методів: накопичувальне

переобладнання, коли обсяг даних недостатній, і важливий час розрахунку, коли кількість змінних велика.

Методи фільтрування зазвичай застосовуються як етап попередньої обробки. Вибір функцій окремий від будь-яких технік машинного навчання. Як альтернативу, ознаки висуваються на основі їх балів у кількох статистичних тестах для їх кореляції зі змінною наслідку.

Як приклад впливу вибору ознак на продуктивність IDS, розглянемо результати в таблиці 3.4, які показують точність виявлення та час побудови режиму IDS класифікатора C4.5 з використанням повного набору даних з 41 функцією NSl- Набір даних KDD і з різними функціями.

Таблиця 3.4 – Детальна точність класифікатора дерева рішень C4.5 з різними наборами ознак

Техніка фільтрування	**Кількість функцій**	**Точність**	**Час**
Повний набір	41	99,55	2,76 сек
Збільшення інформації	13	99,64	0,84 сек
Коефіцієнт посилення	13	99,64	1,31 сек
Чі-квадрат	13	99,65	0,92 сек
Полегшення	13	99	0,93 сек

3.4 Види комп’ютерних атак

Кібератаки можна класифікувати на основі діяльності та цілей зловмисника. Кожен тип атаки можна класифікувати на один із наступних чотирьох класів:

1. Атаки відмови в обслуговуванні (DoS) мають на меті блокувати або обмежувати послуги, що надаються мережею, комп'ютером користувачам.

2. Метою зондуючих атак є отримання інформації про мережу або комп'ютерну систему.

3. Атаки User-to-Root (U2R) мають на меті непривілейований користувач отримати root-доступ або доступ адміністратора-користувача на певному комп'ютері або системі, на якій зловмисник мав доступ на рівні користувача.

4. Атаки віддаленого до локального (R2L) передбачають відправлення пакетів на машину-жертву. Кіберзлочинець вивчає діяльність користувача та отримує привілеї, які кінцевий користувач міг мати в комп'ютерній системі.

Таблиця 3.5 – Класи комп’ютерних атак

Види атаки	**Пояснення**
Переповнення буфера	Атакує межі буфера і перезаписує область пам'яті.
Черв'як	Відтворюється на локальному хості або через мережу.
Троянський	Програми виглядають привабливими та справжніми, але в них вбудований зловмисний код.
Відмова в обслуговуванні (DoS)	Подія безпеки, яка порушує роботу мережевих служб. Це починається з примусового скидання на цільових комп'ютерах. Користувачі більше не можуть підключитися до системи через недоступність послуги.
Сценарії загального інтерфейсу шлюзу (CGI)	Зловмисник використовує сценарії CGI для створення атаки, надсилаючи неправомірні дані на веб-сервер.
Затоплення дорожнього руху	Атакує обмежений розмір NIDS для обробки величезних транспортних навантажень та для розслідування можливих вторгнень. Якщо кіберзлочинець може спричинити затори в мережах, то NIDS буде зайнятий аналізом трафіку.
Фізичний напад	Прагне атакувати фізичні механізми комп’ютерної системи.
Атака паролем	Прагне зламати пароль протягом короткого часу, і це помічається послідовністю помилок входу.
Збір інформації	Збирає інформацію або знаходить слабкі місця в комп’ютерах або мережах за допомогою обнюхування чи пошуку.
Атака користувача до кореня (U2R)	Спочатку кіберзлочинець отримує доступ як звичайний користувач, а потім переходить на суперкористувача, що може призвести до використання декількох вразливостей системи.
Атака віддаленого до локального (R2L)	Кіберзлочинець надсилає пакети у віддалену систему, підключившись до мережі, не маючи облікового запису в системі.
Зонд	Визначення дійсних IP-адрес шляхом сканування мережі для збору пакетів даних хосту.

У цих широких категоріях існує безліч різних форм комп’ютерних атак. Короткий зміст цих атак з коротким поясненням, характеристиками та прикладами представлено в таблиці 3.5.

3.5 Методи ухилення від IDS

У цьому розділі розглядаються методи, які кіберзлочинці можуть використовувати, щоб уникнути виявлення за допомогою IDS, такі як фрагментація, затоплення, забруднення та шифрування. Ці методи становлять виклик для поточної системи IDS, оскільки вони обходять існуючі методи виявлення.

Роздробленість. Пакет ділиться на менші пакети. Потім фрагментовані пакети повторно збираються вузлом-одержувачем на рівні IP перед тим, як переслати їх на рівень програми. Щоб правильно вивчити фрагментований трафік, мережевий детектор повинен зібрати ці фрагменти так само, як це було в точці фрагментації. Для реструктуризації пакетів потрібно, щоб детектор утримував дані в пам'яті та збігав трафік із базою даних підписів. Методи, які використовуються зловмисниками, щоб уникнути виявлення, приховуючи атаки як законний трафік, – це перекриття фрагментів, перезапис та таймаути. Атама фрагментації замінює інформацію в складених фрагментованих пакетах новою інформацією, щоб створити шкідливий пакет.

На рис. 3.2 показано перезапис фрагмента. Пакетний фрагмент 3 генерується зловмисником. Детектор втручання в мережу повинен зберігати стан для всіх пакетів трафіку, який він виявляє.

Рисунок 3.2 – Фрагмент – перезаписати

Тривалість часу, протягом якого детектор може підтримувати стан трафіку, може бути меншою, ніж період, протягом якого хост призначення може підтримувати стан трафіку. Автори шкідливих програм намагаються скористатися будь-яким недоліком методу виявлення, доставляючи фрагменти атаки протягом тривалого часу.

Флуд. Зловмисник починає атаку, щоб завалити детектор, і це спричиняє несправність механізму управління. Коли детектор виходить з ладу, весь рух буде дозволено. Популярним методом створення ситуації флуду є підробка законного протоколу користувацьких датаграм (UDP) та протоколу керування повідомленнями Інтернету (ICMP). Флуд транспортних засобів використовується для маскування ненормальної діяльності кіберзлочинців. Тому IDS матиме надзвичайні труднощі у пошуку шкідливих пакетів у величезному обсязі трафіку.

Обфускація. Для ухилення від виявлення можна використовувати прийоми затухання, які є прийомами приховування нападу, ускладнюючи повідомлення для розуміння. Термінологія обфускації означає зміну програмного коду таким чином, щоб підтримувати його функціональну ідентичність з метою зменшення виявленості до будь-якого виду статичного аналізу або зворотного інженерного процесу, а також зробити його неясним і менш читабельним. Це затемнення шкідливого програмного забезпечення дозволяє йому уникнути поточного IDS.

SIDS покладається на відповідність підписів для виявлення шкідливого програмного забезпечення, де підписи створюються фахівцями-людьми шляхом перекладу шкідливого програмного забезпечення з машинного коду на символічну мову, таку як Unicode. Однак використання обфускації коду є дуже цінним для кіберзлочинців, щоб уникнути IDS.

Шифрування. Як правило, шифрування пропонує низку служб безпеки, таких як конфіденційність даних, цілісність та конфіденційність. Автори зловмисного програмного забезпечення використовують ці атрибути безпеки, щоб уникнути виявлення та приховування атак, які можуть бути націлені на комп’ютерну систему. Наприклад, атаки на зашифровані протоколи, такі як HTTPS, не можуть бути прочитані IDS. IDS не може зіставити зашифрований трафік із наявними підписами бази даних, якщо він не інтерпретує зашифрований трафік. Тому вивчення зашифрованого трафіку ускладнює детекторам виявлення атак. Наприклад, функції, засновані на вмісті пакетів, широко застосовуються для ідентифікації шкідливих програм із звичайного трафіку, які не можуть бути легко застосовані, якщо пакет зашифрований.

Ці виклики спонукають дослідників використовувати деякі функції статистичної мережі, які не покладаються на вміст пакетів. В результаті цього шкідливе програмне забезпечення потенційно можна ідентифікувати із звичайного трафіку.

3.6 Проблеми IDS

Хоча було проведено багато досліджень щодо IDS, залишається багато важливих питань. IDS повинні бути більш точними, з можливістю виявляти різноманітний вторгнення з меншою кількістю помилкових тривог та інших проблем.

Проблеми IDS для ICS. Промислові системи управління (ICS) зазвичай складаються з двох компонентів: обладнання контрольного контролю та збору даних (SCADA), яке отримує інформацію від датчиків, а потім управляє механічними машинами; та програмне забезпечення, яке дозволяє адміністраторам керувати машинами.

Кібератаки на ICS є великим викликом для IDS завдяки унікальній архітектурі ICS, оскільки зловмисники в даний час зосереджуються на ICS. Серед останніх атак на ICS виділяється атака Stuxnet, яка відома як перша зброя для кібервійни. Подібно до типової атаки, основною метою Stuxnet, ймовірно, була іранська атомна програма. Атаки, які можуть бути націлені на ICS, можуть фінансуватися державою, або їх можуть запускати конкуренти, внутрішні зловмисники зі зловмисною ціллю або навіть хактивісти.

Потенційні наслідки скомпрометованої ICS можуть бути руйнівними для громадського здоров'я та безпеки, національної безпеки та економіки. Порушені системи ICS призвели до значних каскадних відключень електроенергії, небезпечних викидів токсичних хімічних речовин та вибухів. Тому важливо використовувати надійні ICS для надійної, безпечної та гнучкої роботи.

Дуже важливо мати систему IDS для ICS, яка враховує унікальну архітектуру, роботу в режимі реального часу та динамічне середовище для захисту об'єктів від атак.

Оскільки Microsoft більше не створює виправлення безпеки для застарілих систем, вони можуть просто атакуватися новими видами програм-вимагачів та шкідливими програмами з нульовим днем.

Подібно, можливо, не вдасться виправити або оновити операційні системи ICS для застарілих програм.

Надійна система IDS може допомогти галузям та захистити їх від загрози кібератак. На жаль, сучасні методи виявлення вторгнень, запропоновані в літературі, зосереджені на програмному рівні. Необхідний життєво важливий підхід для виявлення нульових днів та складних атак на програмному рівні, а також на апаратному рівні без попередніх знань. Це можна зробити, інтегрувавши як апаратне, так і програмне забезпечення систем виявлення вторгнень та витягнувши корисні функції як HIDS, так і NIDS.

3.7 Проблема IDS щодо виявлення ухилення від вторгнення

Виявлення нападів, замаскованих методами ухилення, є проблемою як для СІДС, так і для AIDS. Здатність методів ухилення визначатиметься здатністю IDS повертати оригінальний підпис атак або створювати нові підписи для висвітлення модифікації атак. Надійність IDS до різних методів ухилення все ще потребує подальшого дослідження. Наприклад, SIDS у регулярних виразах може виявляти відхилення від простих мутацій, таких як маніпулювання пробілами, але вони все ще марні проти ряду методів шифрування.

РОЗДІЛ 4
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Вимоги до мікроклімату, освітленню, рівням шуму, іонізуючих та неіонізуючих електромагнітних полів та випромінювань моніторів

Вимоги до виробничих приміщень для експлуатації ЕОМ.

У цьому розділі наведена характеристика приміщень, де експлуатуються ЕОМ. Наведені їх параметри.

Об'ємно-планувальні рішення будівель та приміщень для роботи з ЕОМ мають відповідати вимогам ДСанПІН 3.3.2.007-98 [28]. Розміщення робочих місць з ЕОМ у підвальних приміщеннях, на цокольних поверхах заборонено. Площа на одне робоче місце становить не менше ніж 6,0 м^2, а об'єм - не менше ніж 20,0 м^3. Приміщення для роботи з ЕОМ повинні мати природне та штучне освітлення відповідно до СниП II-4-79.

Природне освітлення має здійснюватись через світлові прорізи, орієнтовані переважно на північ чи північний схід, і забезпечувати коефіцієнт природньої освітленості (КПО) не нижче, ніж 1,5%. Виробничі приміщення повинні обладнуватись шафами для зберігання документів, магнітних дисків, полицями, стелажами, тумбами тощо, з урахуванням вимог до площі приміщень. У приміщеннях з ЕОМ слід щоденно робити вологе прибирання. Приміщення з ЕОМ мають бути оснащені аптечками першої медичної допомоги.

При приміщеннях з ЕОМ мають бути обладнані побутові приміщення для відпочинку під час роботи, кімната психологічного розвантаження. В кімнаті психологічного розвантаження слід передбачити встановлення пристроїв для приготування й роздачі тонізуючих напоїв, а також місця для занять фізичною культурою [29].

Гігієнічні вимоги до параметрів виробничого середовища включають вимоги до параметрів мікроклімату, освітлення, шуму і вібрації, рівнів електромагнітного та іонізуючого випромінювання.

У виробничих приміщеннях на робочих місцях з ЕОМ мають забезпечуватись оптимальні значення параметрів мікроклімату: температури, відносної вологості й рухливості повітря (ГОСТ 12.1.005-88, СН 4088-86) (таблиця 4.1).

Таблиця 4.1 – Норми мікроклімату для приміщень з ВТД ЕОМ та ПЕМ*

Пора року	Категорія робіт	Температура повітря, °С, не більше	Відносна вологість повітря, %	Швидкість руху повітря, м/с
Холодна	легка- 1а	22-24	40-60	0,1
	легка- 16	21-23	40-60	0,1
Тепла	легка- 1а	23-25	40-60	0,1
	легка- 16	22-24	40-60	0,2

Рівні позитивних і негативних іонів у повітрі приміщень з ЕОМ мають відповідати санітарно-гігієнічним нормам (таблиця 4.2).

Таблиця 4.2 – Рівні іонізації повітря приміщень при роботі з ЕОМ

Рівні	Число іонів в 1 см повітря	
	п+	п -
Мінімально необхідні	400	600
Оптимальні	1500-3000	3000-5000
Максимально допустимі	50000	50000

Штучне освітлення в приміщеннях з робочими місцями, обладнаними ЕОМ має здійснюватись системою загального рівномірного освітлення. У виробничих та адміністративно-громадських приміщеннях, у разі переважної роботи з документами, допускається застосування системи комбінованого освітлення (крім системи загального освітлення додатково встановлюються світильники місцевого освітлення).

Значення освітленості на поверхні робочого столу в зоні розміщення документів має становити 300-500 лк. Якщо це неможливо забезпечити системою загального освітлення, допускається використовувати місцеве освітлення. При цьому світильники місцевого освітлення слід встановлювати таким чином, щоб не

створювати бликів на поверхні екрана, а освітленість екрана має не перевищувати 300 лк.

Як джерела світла для штучного освітлення мають застосовуватись переважно люмінесцентні лампи типу ЛБ. У разі влаштування відбитого освітлення у виробничих та адміністративно-громадських приміщеннях допускається застосування металогалогенних ламп потужністю 250 Вт. Допускається застосування ламп розжарювання у світильниках місцевого освітлення.

Рівні звукового тиску в октавних смугах частот, рівні звуку та еквівалентні рівні звуку на робочих місцях, обладнаних ЕОМ, мають відповідати вимогам СН 3223-85, ГОСТ 12.1.003-83, ГР 2411-81 (таблиця 4.3).

Таблиця 4.3 – Допустимі рівні звуку, еквівалентні рівні звуку і рівні звукового тиску в октавних смугах частот

Вид трудової діяльності	Рівні звукового тиску в дБ в октавних смугах із середньогеометричними частотами, Гц									
	31,5	63	125	250	500	1000	2000	4000	8000	Рівні звуку, еквівалентні рівні звуку, дБА
Програмісти ЕОМ	86	71	61	54	49	45	42	40	38	50
Оператори в залах обробки інформації на ЕОМ та оператори комп'ютерного набору	96	83	74	68	63	60	57	55	54	65
В приміщеннях для розташування шумних агрегатів ЕОМ	103	91	83	77	73	70	68	66	64	75

Значення напруженості електростатичного поля на робочих місцях з ЕОМ (як у зоні екрана дисплея, так і на поверхнях обладнання, клавіатури, друкувального пристрою) мають не перевищувати гранично допустимих за ГОСТ 12.1.045-84, СН 1757-77 (таблиця 4.4). Значення напруженості електромагнітних полів на робочих

місцях з ЕОМ мають відповідати нормативним значенням (ГДР N 3206-85, ГДР № 4131-86, СН N 5802-91, ГОСТ 12.1.006-84) (табл. 4.4).

Таблиця 4.4 – Допустимі параметри електромагнітних випромінювань і електростатичного поля

Види поля	Допустимі параметри поля		Допустима поверхнева щільність потоку енергії (інтенсивність потоку енергії), Вт/м^2
	за електричною складовою (Е), В/м	за магнітною складовою (Н), А/м	
Напруженість електромагнітного поля 60 кГц до 3 мГц	50	5	
3 мГц до 30 мГц	20	—	
30 мГц до 50 мГц	10	0,3	
50 мГц до 300 мГц	5	-	
300 мГц до 300 гГц	-	-	10
Електромагнітне поле оптичного діапазону в ультрафіолетовій частині спектру: УФ-С (220-280 мм)			0,001
УФ-В (280-320 мм)			0,01
УФ-А (320-400 мм)			10,0
у видимій частині спектру:			
400-760 мм			10,0
в інфрачервоній частині спектру:			
0,76-10,0 мкм			35,0-70,0
Напруженість електричного поля ЕОМ			20 кВ/м

Інтенсивність потоків інфрачервоного випромінювання має не перевищувати допустимих значень згідно СН 4088-86, ГОСТ 12.1.005-88.

Інтенсивність потоків ультрафіолетового випромінювання не повинна перевищувати допустимих значень, відповідно до СН 4557-88.

Іонізуючі випромінювання на відстані 0,05 м від екрана до корпусу відеотермінала при будь-яких положеннях регулювальних пристроїв не повинні перевищувати 7,74 х 10 в ст.-12 А/кг, що відповідає еквівалентній дозі 0,1 мбер/год (100 мкР/год) НРБУ № 58.

4.2 Забезпечення захисту працівників суб'єктів господарювання та населення від впливу іонізуючих випромінювань

Захист від іонізуючих випромінювань може здійснюватись шляхом використання наступних принципів:

– використання джерел з мінімальним випромінюванням шляхом переходу на менш активні джерела, зменшення кількості ізотопа;

– скорочення часу роботи з джерелом іонізуючого випромінювання;

– віддалення робочого місця від джерела іонізуючого випромінювання;

– екранування джерела іонізуючого випромінюванн.

Екрани можуть бути пересувні або стаціонарні, призначені для поглинання або послаблення іонізуючого випромінювання. Екранами можуть бути стінки контейнерів для перевезення радіоактивних ізотопів, стінки сейфів для їх зберігання

Альфа-частинки екрануються шаром повітря товщиною декілька сантиметрів, шаром скла товщиною декілька міліметрів. Однак, працюючи з альфа-активними ізотопами, необхідно також захищатись і від бета- або гамма-випромінювання.

З метою захисту від бета-випромінювання використовуються матеріали з малою атомною масою. Для цього використовують комбіновані екрани, у котрих з боку джерела розташовується матеріал з малою атомною масою товщиною, що дорівнює довжині пробігу бета-частинок, а за ним – з великою масою.

З метою захисту від рентгенівського та гамма-випромінювання застосовуються матеріали з великою атомною масою та з високою щільністю (свинець, вольфрам).

Для захисту від нейтронного випромінювання використовують матеріали, котрі містять водень (вода, парафін), а також бор, берилій, кадмій, графіт. Враховуючи те, що нейтронні потоки супроводжуються гамма-випромінюванням, слід використовувати комбінований захист у вигляді шаруватих екранів з важких та легких_матеріалів (свинець-поліетилен).

Дієвим захисним засобом є використання дистанційного керування, маніпуляторів, роботизованих комплексів.

В залежності від характеру виконуваних робіт вибирають засоби індивідуального захисту: халати та шапочки з бавовняної тканини захисні фартухи, гумові рукавиці, щитки, засоби захисту органів дихання (респіратор „Лепесток"), комбінезони, пневмокостюми, гумові чоботи.

Дієвим чинником забезпечення радіаційної безпеки є дозиметричний контроль за рівнями опромінення персоналу та за рівнем радіації в навколишньому середовищі.

Оцінка радіаційного стану здійснюється за допомогою приладів, принцип дії котрих базується на наступних методах:

– іонізаційний (вимірювання ступеня іонізації середовища);

– сцинтиляційний (вимірювання інтенсивності світлових спалахів, котрі виникають в речовинах, що люмінесціюють при проходженні через них іоні: «чих випромінювань);

– фотографічний (вимірювання оптичної щільності почорніння фотопластинки під дією випромінювання);

– калориметричні методи (вимірювання кількості тепла, що виділяється в поглинальній речовині).

ВИСНОВКИ

Кіберзлочинці орієнтуються на користувачів комп’ютерів, використовуючи складні методи, а також стратегії соціальної інженерії. Деякі кіберзлочинці стають дедалі витонченішими та мотивованішими. Кіберзлочинці продемонстрували свою здатність приховувати свою особистість, приховувати своє спілкування, віддаляти свою особу від нелегальної вигоди та використовувати інфраструктуру, стійку до компромісів. Тому для комп'ютерних систем стає все більш важливим захист за допомогою вдосконалених систем виявлення вторгнень, здатних виявляти сучасні шкідливі програми. Для проектування та побудови таких систем IDS необхідно мати повний огляд переваг та обмежень сучасних досліджень IDS.

У цій роботі ми детально представили огляд методологій, типів та технологій виявлення вторгнень з їх перевагами та обмеженнями. Розглядаються декілька методів машинного навчання, запропонованих для виявлення атак нульових днів. Однак такі підходи можуть мати проблему генерації та оновлення інформації про нові атаки та спричиняти високі помилкові тривоги або низьку точність. Ми узагальнили результати нещодавніх досліджень та дослідили сучасні моделі підвищення ефективності боротьби зі AIDS як рішення для подолання проблем IDS.

Крім того, були вивчені найпопулярніші загальнодоступні масиви даних, що використовуються для досліджень IDS, та обговорені їх методи збору даних, результати оцінки та обмеження. Оскільки звичайна діяльність часто змінюється і з часом може не залишатися ефективною, існує потреба у нових та більш повних наборах даних, що містять широкий спектр шкідливих програм. Необхідний новий набір шкідливих програм, оскільки більшість існуючих методів машинного навчання навчаються та оцінюються на основі знань, наданих старим набором даних, таким як DARPA / KDD99, які не включають новіші дії щодо шкідливого програмного забезпечення. Тому тестування проводиться з використанням цих наборів даних, зібраних лише у 1999 році, оскільки вони є загальнодоступними та відсутні інші альтернативні та прийнятні набори даних. Хоча ці набори даних широко прийняті як еталони, вони більше не представляють сучасних атак нульового дня. Хоча набір

даних ADFA містить багато нових атак, він недостатній. З цієї причини тестування на AIDS за допомогою цих наборів даних не дає реальної оцінки і може призвести до неточних тверджень щодо їх ефективності.

У цьому дослідженні також вивчаються чотири поширені методи ухилення, щоб визначити їх здатність уникати найостанніших IDS. Ефективна система IDS повинна мати можливість точно виявляти різні види атак, включаючи вторгнення, що включає методи ухилення. Розробка IDS, здатних подолати методи ухилення, залишається головним викликом для цієї галузі досліджень.

ПЕРЕЛІК ПОСИЛАНЬ

1. Paymen Kabiri and Alee A. Gorbouney. " Survey Examination on Intrusion Detection Systems and Response” – International Journal of Security in Computer Networks, Vol.1, No.2, PP.84–102, Sep. 2005.

2. Cristoper Low "Fundamentals of Wireless attacks and their detection" – GIAC Security Essentials Certification (GSEC) Practical Assignment 13, April, 2005.

3. Paule Iannella. The Evolution of IDSs – T.D.I., LLC. International Journal of Network Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, February 2015.

4. Hrystofer Lau. "Understanding Wireless attacks and their detection." GIAC Security Essentials Certification (GSEC) Practical Assignment 13 April 2005. PP. 1 – 3.

5. Endorf, Carl F., Eugene Schultz, and Jim Mellander. Intrusion detection & prevention. McGraw-Hill Osborne Media, 2004.

6. Rebecca Gurley Bace, “Intrusion Detection,” Macmillan Technical Publishing, 2000. P. 128.

7. Kavitha B., Karthikeyan S. Efficient Intrusion Detection with Reduced Dimension Using Data Mining Classification Methods and Their Performance Comparison. In: Das V.V. et al. (eds) Information Processing and Management. BAIP 2015, vol 70. Springer, Berlin, Heidelberg.

8. Anita K. Jones and Robert S. Sielken “Computer System Intrusion Detection A Survey “International Journal of Computer Theory and Engineering, Vol.2, No.6, December, 2010.

9. Top 125 Network Security Tools // [Електронний ресурс]. – Режим доступу: http://sectools.org/

10. Sakar Saran, Sonyu Ahrauual “A Survey on Enhanced Intrusion Detection System in Mobile Ad hoc Network MANET” // International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 7, September 2012. PP. 135–144.

11. Symantec, "Internet security threat report 2017," April, 7017 2017, vol. 22 // [Електронний ресурс]. – Режим доступу: https://www.symantec.com/ content/dam/symantec/docs/ reports/ istr-22-2017-en.pdf .

12. Breach_LeveL_Index. (2017, November). Data breach statistics // [Електронний ресурс]. – Режим доступу: http://breachlevelindex.com

13. Australian. (2017, November). Australian cyber security center threat report 2017. [Електронний ресурс]. – Режим доступу: https://www.acsc.gov.au/ publications/ACSC_Threat_Report_2017.pdf

14. S. Axelsson, Stefan. Intrusion detection systems: A survey and taxonomy. Vol. 99. Technical report, 2000.

15. H. Debar, M. Dacier, and A. Wespi, "A revised taxonomy for intrusion-detection systems," in Annales des télécommunications, 2000, vol. 55, no. 7–8, pp. 361–378.

16. Liao H-J, Lin C-HR, Lin Y-C, Tung K-Y (2013b) Intrusion detection system: a comprehensive review. J Netw Comput Appl 36(1): pp. 16–24.

17. T. F. Lunt, "Automated audit trail analysis and intrusion detection: a survey," in Proceedings of the 11th National Computer Security Conference, 1988, vol. 353: Baltimore, MD.

18. Axelsson, Stefan. Intrusion detection systems: A survey and taxonomy. Vol. 99. Technical report, 2000. [Електронний ресурс]. – Режим доступу: https://neuro.bstu.by/ai/To-dom/My_research/Paper-0-again/For-research/D-mining/Anomaly-D/Intrusion-detection/taxonomy.pdf

19. Agrawal, Shikha, and Jitendra Agrawal. "Survey on anomaly detection using data mining techniques." Procedia Computer Science 60 (2015): pp. 708-713.

20. Buczak, Anna L., and Erhan Guven. "A survey of data mining and machine learning methods for cyber security intrusion detection." IEEE Communications surveys & tutorials 18.2 (2015): pp. 1153-1176.

21. M. Ahmed, A. Naser Mahmood, and J. Hu, "A survey of network anomaly detection techniques," J Netw Comput Appl, vol. 60, pp. 19–31, 1// 2016.

22. Стефанів АМ Класифікація методів виявлення фішингу в інтерактивних мультимедійних виданнях/АМ Стефанів, НВ Загородна, РО Козак//Збірник тез доповідей VIII Міжнародної науково-технічної конференції молодих учених та студентів „Актуальні задачі сучасних технологій “, 27-28 листопада 2019 року.–Т.: ТНТУ, 2019.–Том 1.–С. 136–137.

23. Сачик Т.В. Захист персональної інформації в задачах аналізу та обробки великих даних : дипломна робота магістра за спеціальністю „125 — кібербезпека“/ Т.В. Сачик. — Тернопіль: ТНТУ, 2019. — 107 с.

24. Паперовський Б.О. Аналіз сучасних методів виявлення аномалій та можливих втручань в роботу комп'ютерної системи „125 — кібербезпека“/ Б.О. Паперовський. — Тернопіль: ТНТУ, 2018. — 7 с.

25. Загородна, Н. В. "Аналіз анти-бот стратегій, що грунтуються на інтерактивному підтвердженні участі людини." Матеріали III-ої міжнародної науково-технічної конференції" Захист інформації і безпека інформаційних систем".– Львів: 05-06.

26. Oleh Maksymets, Ruslan Kozak. Analysis Methods of Data Mining and Machine Learning in Attacks Detection on Computer Systems. V Inter University Conference of Students and Young Scientists “Engineer of XXI Century” // The University of Bielsko-Biała (ATH) in Bielsko-Biała. 2015/12, pp. 449-454.

27. D. M. Farid, N. Harbi, and M. Z. Rahman, "Combining naive bayes and decision tree for adaptive intrusion detection," arXiv preprint arXiv:1005.4496, 2010.

28. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин МОЗ України від 10.12.1998 № 7. // Офіційний сайт Верховної Ради України. – [Електронний ресурс]. – Режим доступу https://zakon.rada.gov.ua/rada/show/ v0007282-98

29. Вдосконалення охорони праці в ІТ-індустрії. // Харківський національний дорожний університет. [Електронний ресурс]. – Режим доступу: https://www.khadi.kharkov.ua/fileadmin/ P_vcheniy_secretar/ %D0%9E%D0% A5%D0%9E% D0%A0%D0%9E% D0%9D% D0%90_% D0%9F% D0%A0% D0%90%D0%A6% D0%86/R_IT-INDUSTRIA.pdf