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)
Кібербезпеки
(повна назва кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломної роботи

магістр
(освітній рівень)

на тему: **Огляд загроз для захищеності програмних систем та засобів захисту від зовнішнього проникнення в хмарних сервісах**

Виконав: студент 6 курсу, групи СБм-61
спеціальності 125 «Кібербезпека»
(шифр і назва спеціальності)

(підпис) Яворський Р.І.
(прізвище та ініціали)

Керівник (підпис) Александер М.Б..
(прізвище та ініціали)

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

Рецензент (підпис) (прізвище та ініціали)

м. Тернопіль – 2019

РЕФЕРАТ

"Огляд загроз для захищеності програмних систем та засобів захисту від зовнішнього проникнення в хмарних сервісах". // Яворський Руслан Іванович // Тернопільський національний технічний університет ім. І.Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2019 // с. – , рис. – , табл. – , ілюстр. – , джерел – .

Ключові слова: ЗАГРОЗА, НЕЙРОННА МЕРЕЖА, КЛАСИФІКАЦІЯ, СТАТИСТИЧЕНІ МЕТОДИ, СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ.

У магістерській роботі виконано дослідження способів забезпечення необхідного рівня захищеності хмарних сервісів, які доступні через мережеві з'єднання. Виконано огляд і класифікація матеріалу стосовно способів впливу шкідливого програмного забезпечення на мережеві хмарні сервіси та вироблено рекомендації стосовно використання систем виявлення вторгнень на основі різних принципів.

В дипломній роботі показано актуальність оцінювання рівня захищеності хмарних сервісів. Пропонується спосіб відбору характеристик та методів роботи систем виявлення вторгнень на основі нейромереж та статистичних методів.

ANNOTATION

"Review of threats for software systems security and security facilities against external penetration in cloud services" // Diploma paper of Master degree level // Yavorskii Ruslan Ivanovych // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Cybersecurity Department // Ternopil, 2019 // p. – , Fig. – , Tables – , Refence. – .

Key words: THREAT, NEURAL NETWORK, CLASSIFICATION, STATISTICAL METHODS, INTRUSION DETECTION SYSTEM.

The master's thesis investigates how to provide the required security level of cloud services that are accessible through network connections. The material was reviewed and classified regarding the ways in which malware could affect the network cloud services, and recommendations were made regarding the use of intrusion detection systems based on various principles.

The diploma thesis shows the relevance of assessing the security level of cloud services. A method of selecting the characteristics and methods of operation of neural network based intrusion detection systems and statistical methods are proposed.

ЗМІСТ

ВСТУП .....
РОЗДІЛ 1. ВИЯВЛЕННЯ МЕРЕЖЕВИХ АНОМАЛІЙ: МЕТОДИ, СИСТЕМИ ТА ІНСТРУМЕНТИ .....
1.1 Проблеми безпеки при використанні хмарних технологій віртуалізації ресурсів та послуг .....
1.2 Попередні огляди щодо виявлення мережевої аномалії .....
1.3 Проблема виявлення аномалій .....
1.4 Класифікація атак на віртуальні сервіси .....
РОЗІДЛ 2. АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ АНОМАЛІЙ У ВІРТУАЛЬНИХ СИСТЕМАХ .....
2.1 Загальна архітектура NIDS .....
2.2 Аспекти виявлення мережевої аномалії .....
РОЗІДЛ 3. МЕТОДИ ТА СИСТЕМИ ДЛЯ ВИЗНАЧЕННЯ АНОМАЛЬНОЇ МЕРЕЖІ .....
3.1 Статистичні методи та системи .....
3.2 Методи та системи на основі класифікації .....
3.3 Методи та системи на основі кластеризації .....
3.4 Програмні обчислювальні методи та системи .....
3.5 Методи та системи на основі знань .....
РОЗІДЛ 4. СПЕЦІАЛЬНА ЧАСТИНА. КЛАСИФІКАЦІЯ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ .....
4.1 Класифікація за розташуванням .....
4.2 Класифікація за функціональністю .....
4.3 Класифікація на основі принципів поширення .....
4.4 Класифікація на основі механізмів виявлення з сигнатурами .....
4.5 Класифікація на основі механізмів виявлення з нейронними мережами.....

4.6 Класифікація на основі способу виявлення .....
РОЗДІЛ 5. ОБГРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ .....
5.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР .....
5.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи .....
5.3 Розрахунок матеріальних витрат .....
5.4 Розрахунок витрат на електроенергію .....
5.5 Розрахунок суми амортизаційних відрахувань .....
5.6 Обчислення накладних витрат .....
5.7 Складання кошторису витрат та визначення собівартості НДР .....
5.8 Розрахунок ціни проекту .....
5.9 Визначення економічної ефективності і терміну окупності капітальних вкладень .....
РОЗДІЛ 6. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ .....
6.1 Охорона праці .....
6.2 Кольорове оформлення виробничих приміщень як фактор підвищення продуктивності праці .....
6.3 Концепція безпеки життєдіяльності .....
РОЗІДЛ 7. ЕКОЛОГІЯ .....
7.1 Отримання енергії за рахунок альтернативних джерел .....
7.2 Індексний метод в екології .....
ВИСНОВКИ .....
ПЕРЕЛІК ПОСИЛАНЬ .....
ДОДАТКИ

ВСТУП

Актуальність теми. Віртуалізація дає ряд переваг, ніж традиційні системи. Віртуалізація дозволяє одночасно запускати кілька операційних систем. Більше того, віртуалізація пропонує покращені, оптимізовані та дешеві послуги для клієнтів завдяки підтримці наданні своїх послуг, як абстрактної хмари у. Екземпляри серверів і сервісів в цьому випадку називаються віртуальними машинами (VM). Кожна VM має власну операційну систему та прикладні програми. Ініціюється VM для кожного користувача. Таким чином практично кожен користувач має доступ до віртуального комп'ютера. Монітор VM або гіпервізор – це модуль, що управляє VM та координує одночасну роботу операційних систем на одній фізичній машині.

Ризики щодо безпеки можуть змінюватися залежно від типу використовуваного гіпервізора. Підтримуваний гіпервізор розміщений в операційній системі. Ця віртуалізована інфраструктура піддається більшій загрозі, ніж звичайна традиційна операційна система. Віртуальні машини розміщуються на фізичному хості, і вони можуть комунікувати одна з одною. Ця комунікація дозволяє здійснювати атаки зловмисників. Тому тема роботи є актуальною з точки зору захисту віртуальних сервісів від вторгнень шкідливого програмного забезпечення.

Мета дослідження: розгляд теоретичних та практичних засад технології виявлення інфікованих комп'ютерів, формалізацію створення методик виявлення атак на віртуальні сервіси.

Об'єкт дослідження – процес виявлення шкідливого програмного забезпечення.

Предметом дослідження способи виявлення вторгнень на основі різноманітних підходів і принципів.

Для дослідження цілі дипломної роботи поставлені наступні **задачі**:

- розглянути основні загрози систем, що надають віртуальні сервіси;

– розглянути методи виявлення атак на хмарні мережеві сервіси;

– виконати аналіз інструментів виявлення вторгнень;

– запропонувати рішення для покращення достовірності спрацювання системи виявлення вторгнень.

Наукова новизна отриманих результатів.

Наукова новизна полягає у вирішенні задачі систематизації відомостей про засоби виявлення та запобігання атак на хмарні мережеві сервіси зараженими обчислювальними вузлами. При цьому було отримано такі результати:

– на основі класифікації загроз запропоновано використовувати системи виявлення вторгнень на основі нейронних мереж;

– виокремлено переваги та недоліки систем виявлення вторгнень на основі різних принципів;

– вироблено рекомендації стосовно використання систем виявлення вторгнень.

Практичне значення отриманих результатів.

Всі розроблені методи можуть бути доведені до практичного впровадження у складі системи захисту від зловмисного вторгнення. Така система дозволить мінімізувати ризики захищеності систем на основі віртуальних сервісів.

Публікації. Основні положення роботи доповідались, розглядались та обговорювались на науковій конференції Тернопільського національного технічного університету. Результати дипломної роботи опубліковані у тезах студентської наукової конференції, яка проводились у ТНТУ.

Структура роботи. Робота складається з розрахунково-пояснювальної записки. Розрахунково-пояснювальна записка складається з вступу, 7 частин, висновків, переліку посилань та додатків. Обсяг роботи: розрахунково-пояснювальна записка – ____ арк. формату А4.

РОЗДІЛ 1
ВИЯВЛЕННЯ МЕРЕЖЕВИХ АНОМАЛІЙ: МЕТОДИ, СИСТЕМИ ТА ІНСТРУМЕНТИ

1.1 Проблеми безпеки при використанні хмарних технологій віртуалізації ресурсів та послуг

Віртуалізація обчислювальних ресурсів та послуг дає ряд переваг, ніж традиційні системи. Віртуалізація дозволяє одночасно запускати кілька операційних систем. Крім того, віртуалізація пропонує покращені, оптимізовані та дешеві послуги для клієнтів завдяки підтримці хмари у наданні його послуг. Віртуалізація дозволяє отримати множину екземплярів віртуальних машин в одній фізичній машині; ці екземпляри називаються віртуальними машинами. VM має власну операційну систему та додатки. VM ініціюється для кожного користувача, який практично забезпечує повну операційну машину для користувача. Монітор VM (VMM) або гіпервізор - це модуль, що управляє VM та дозволи різні операційні системи працювати одночасно на одній фізичній машині. Побоювання щодо безпеки можуть змінитися відповідно до типу використовуваного гіпервізора. Розподілений гіпервізор розміщений в операційній системі. Ця віртуалізована інфраструктура наражається на більшу кількість загроз, ніж гіпервізор з голих металів; VM розміщуються у фізичній машині, і вони можуть спілкуватися один з одним. Ця комунікація дозволяє здійснювати напади зловмисника. Однак комунікація між VM не є предметом дослідження.

Віртуалізація піддає користувачів та інфраструктуру хмари вразливостям для безпеки. Питання безпеки, пов'язані з віртуалізацією, обговорюються нижче.

Образи VM використовується для створення екземплярів VM. Користувач може створити власний образ або використовувати образ із сховища. Обмін VM-образами у сховищі може перетворитися на серйозну загрозу, якщо воно буде

використано зловмисно; Зловмисник може досліджувати код образу, щоб шукати вразливості, або він може завантажувати образи, що містять зловмисне програмне забезпечення. VM, інстанційована за допомогою зараженого образу, стане джерелом впровадження зловмисного програмного забезпечення в хмару. VM може використовуватися для моніторингу діяльності та даних інших користувачів, що призводять до порушення конфіденційності. Крім того, якщо образ не очищено, він може розповсюдити конфіденційну інформацію користувача.

Ізоляція VM. Віртуальні машини, що працюють на одному і тому ж обладнанні, потрібно ізолювати одна від одної. Хоча існує логічна ізоляція, доступ до одних і тих же ресурсів може призвести до порушення даних та перехресних атак. Ізоляція VM потрібна не тільки на пристроях зберігання даних, але й на пам'яті та обчислювальному обладнанні.

VM втеча. Втеча VM - це ситуація, коли зловмисник виводить з-під контролю VMM. Ця ситуація може забезпечити зловмиснику доступ до інших VM і може пошкодити VMM. Крім того, може бути забезпечений доступ до обладнання для обчислення та зберігання даних хост-машини. Модель послуги IaaS піддається небезпеці, що, в свою чергу, може впливати на інші віртуальні сервіси.

Міграція VM. Міграція VM - це переміщення VM на іншу фізичну машину без відключення VM. Міграція VM здійснюється з різних причин, таких як балансування навантаження, стійкість до відмов та обслуговування. Під час процесу міграції вміст VM піддається впливу мережі, що може спричинити занепокоєння щодо безпеки даних. Крім даних, код VM стає вразливим для зловмисників під час міграції. Додатково міграційний модуль може скомпрометувати зловмисника для переміщення VM на компрометований сервер або під керуванням компрометованого VMM. Міграція VM є вирішальною і повинна виконуватись захищено.

Відкат VM. Віртуалізація дозволяє повертати VM до деякого попереднього стану. Однак, відкат викликає занепокоєння щодо безпеки. Наприклад, відкат може ввімкнути облікові дані безпеки, які раніше були відключені. Крім того, відкат може відтворити VM до вразливого стану, яка раніше була виправлена. Крім того, відкат може повернути VM до попередніх політик безпеки та помилок конфігурації.

Проблеми гіпервізора. Компрометований VMM може надати контроль зловмисникові до віртуальних машин. Метадані VM можуть також бути доступні зловмиснику, якщо зловмисник бере контроль над VMM. Гіпервізор забезпечує велике ромаїття атак через більше точок входу та складності взаємозв'язку. Крім того , у VMM є багато повідомлених помилок, які дозволяють зловмиснику взяти під контроль VMM або обійти обмеження безпеки.

Поширення VM. Поширення VM – це ситуація, коли кількість VM збільшується, і більшість вже створених VM знаходяться в режимі очікування. Поширення VM призводить до того, що ресурси приймаючої машини будуть витрачатися у великих масштабах.

Образи VM вимагають високої безпеки та жорсткості, оскільки вони задають початковий стан VM. Крім того, образи VM використовуються різними та неспорідненими користувачами. Тому безпека образів є основою для безпеки всієї хмари. Контроль доступу здійснюється при реєстрації та виході із сховища. Для публікації, пошуку та модифікації образів VM потрібні належні дозволи. Фільтри застосовуються до образів при публікації та пошуку для виявлення та видалення небажаної інформації. Фільтри видаляють залишкову приватну інформацію, шкідливі програми та піратське програмне забезпечення на образі. Система відстеження використовується для відстеження образу як за діями, так і за виводом. Служби технічного обслуговування запускають періодично інструменти виявлення зловмисних програм для образів у сховищі та виявляють уразливості та виправлення.

Віртуальна машина повинна бути захищена від атак не тільки в сховищі, а й під час виконання. У хмарному середовищі VM переміщуються між різними фізичними місцями та хмарними установками з різних причин, таких як балансування навантаження, фізична несправність машини, економія енергії та оновлення програмного забезпечення. Один із методів дозволяє мігрувати VM лише у тому випадку, якщо платформа призначення захищена до визначеного користувачем рівня. Використовується рівень довіри довіри (TAL), який визначає рівень довіри цільової платформи. TAL обчислюється за допомогою облікових даних апаратного Trusted Platform Module (TPM) та облікових даних Trust Token, запропонованих авторизованими вузлами. Токен довіри визначає рівень довіри програм. Користувач визначає TAL (найменший, низький, високий, середній і нормальний) в процесі запуску VM. Переміщення VM дозволено, якщо TAL цільової платформи знаходиться в діапазоні заданих вимог користувача. Цей процес також може бути використаний для вимірювання TAL розміщеної платформи на момент запуску VM. Запропонована методика дозволяє користувачеві перевіряти TAL платформи призначення після міграції VM, щоб переконатися, що його вимоги виконані.

Гіпервізор або VMM - це програмне забезпечення, яке управляє і контролює віртуалізацією в хмарі. Порушений гіпервізор може знищити всю систему.

Щоб захистити витік приватної інформації через відкат, автори в роботі [5] запропонували SPARC. SPARC - це захищений механізм, що дозволяє користувачам виключати додатки, які обробляють приватну інформацію, із пункту перевірки. Отже, час конфіденційної інформації скорочується. Автори запропонували також стратегію під назвою Checkpoint-збереження контрольної точки (PPC) для виключення конфіденційної інформації з пунктів пропуску. КПП відслідковує приватну інформацію шляхом аналізу потоку інформації та під час огляду знімає конфіденційну інформацію.

Мета цього дослідження - висвітлити проблеми безпеки, пов’язані з віртуалізацією хмарних обчислень, та представити деякі поточні рішення. Крім

того, робота сприяє розумінню вразливості віртуалізованих хмарних обчислень. Однак є проблеми із безпекою, які все ще потрібно вирішити або вимагати проведення додаткових досліджень. Більше того, завершений механізм безпеки у віртуалізованому середовищі ще не існує. Оскільки технологія віртуалізації стає все актуальнішою, багатьом таким небезпечним загрозам ще потрібно протидіяти.

З урахуванням прогресу в галузі Інтернет-технологій та сукупного зростання кількості мережевих атак, виявлення вторгнення в мережу стало важливою проблемою дослідження. Незважаючи на значний прогрес і великий обсяг роботи, є ще багато можливостей для розвитку подібних досліджень в виявленні і зриву мережевих атак.

На думку [1], спроба вторгнення або загроза - це навмисна і несанкціонована спроба (i) отримати доступ до інформації, (ii) маніпулювати інформацією або (iii) зробити систему ненадійною або непридатною. Наприклад, (a) атака відмови в обслуговуванні (DoS) намагається голодувати множину своїх ресурсів, необхідних для правильної роботи під час обробки; (b) черви та віруси експлуатують інших господарів через мережу; та (c) Компроміси отримують привілейований доступ до хоста, використовуючи переваги відомих уразливостей.

Термін виявлення вторгнень на основі аномалії позначає проблему пошуку виняткових зразків мережевого трафіку, які не відповідають очікуваній нормальній поведінці. Ці невідповідні зразки часто називають аномаліями, випередженнями, винятками, відхиленнями, сюрпризами, особливостями або суперечливими спостереженнями в різних областях застосування. З них, аномалія і викиди є двома з найбільш часто використовуваних термінів в контексті аномалії - на основі виявлення вторгнень в мережі.

Виявлення аномалій має широке застосування в таких сферах, як виявлення шахрайства для кредитних карток, виявлення вторгнень для кібербезпеки та військовий нагляд за діями противника. Наприклад, аномальна схема трафіку в

комп'ютерній мережі може означати, що зламаний комп’ютер посилає конфіденційні дані несанкціонованому хосту.

В останні десятиліття машинне навчання почало відігравати значну роль у виявленні аномалії. Дослідники розробили велику кількість методів виявлення вторгнень на основі аномалії. Багато методик працюють у конкретних областях, хоча інші є більш загальними.

Незважаючи на те, що в літературі є кілька оглядів щодо виявлення мережевої аномалії, такі огляди обговорюють набагато менше методів виявлення, ніж ми. В авторів обговорюють виявлення аномалій в цілому і покриє область виявлення вторгнення тільки на короткий час. Жодне з оглядів не включає загальні інструменти, що використовуються під час виконання різних етапів виявлення мережевої аномалії. Вони також не обговорюють підходів, що поєднують кілька індивідуальних методів для досягнення кращих показників. У цій роботі ми представляємо структуроване та всебічне огляди щодо виявлення вторгнень на основі аномалії з точки зору загального огляду, методів, систем, інструментів та наборів даних з обговоренням проблем та рекомендацій. Наша презентація деталізована з достатньою кількістю порівнянь, де це необхідно, і призначена для читачів, які бажають розпочати дослідження в цій галузі.

1.2 Попередні огляди щодо виявлення мережевої аномалії

Мережеве виявлення аномалії - це широка область досліджень, яка вже може похвалитися низкою оглядів, оглядових статей, а також книг. Проведено широке огляди методик виявлення аномалій, розроблених у машинному навчанні та статистиці. У [2] представити широкий огляд методів виявлення аномалії для числових, а також символічних даних. Автори у [3] представляють огляди методів виявлення аномалії, що використовуються спеціально для виявлення кібер-вторгнень.

Добрий обсяг досліджень щодо виявлення зовнішньої статистики у кількох книгах, а також у статтях огляди. Вичерпні обстеження виявлення аномалії в кількох областях були представлені в [4]. Автори у [5] повідомляти про основні методи та проблеми, виявлені в аналізі трафіку IP, з акцентом на виявлення додатків.

Про деякі роботи повідомлялося в контексті бездротових мереж. BC та ін. представити опис методів виявлення вторгнень для мобільних спеціальних мереж (MANET) та бездротових сенсорних мереж (WSN). Вони також представляють кілька важливих дослідницьких питань та викликів у контексті побудови IDS шляхом інтеграції аспектів мобільності.

У [6] запроваджують два різних підходи до створення IDS для MANET, а саме, на базі ланцюга Маркова. Вони також пропонують адаптивну схему для динамічного підбору нормальних профілів та відповідних порогів. BC та ін. побудувати вектор функцій на основі декількох параметрів, таких як тривалість дзвінка, період бездіяльності дзвінка та призначення виклику для ідентифікації дзвінки користувачів. Вони використовують методи класифікації для виявлення аномалій.

У [7] представляють огляд застосувань методів обчислювальної розвідки до проблеми виявлення вторгнень. Вони включають різні методи, такі як штучні нейронні мережі, нечіткі системи, еволюційні обчислення, штучна імунна система, інтелект рою та м'які обчислення.

У [8] пропонується Intrusion Detection System – IDS (ситсема виявлення вторгнень) рівня додатків на основі навчання послідовності для виявлення аномалій. Автори демонструють, що їх IDS є ефективнішим порівняно з підходами, що використовують моделі Маркова та алгоритми k-засобів. Описані в цьому розділі огляди охоплює більшість цитованих підходів та систем, про які повідомляється в літературі до цих пір.

1.3 Проблема виявлення аномалій

Для забезпечення відповідного рішення у виявленні мережевої аномалії нам потрібна концепція нормальності. Ідея нормального зазвичай вводиться формальною моделлю, яка виражає відносини між основними змінними, що беруть участь у системній динаміці. Отже, подія чи об'єкт визначаються як аномальні, якщо ступінь його відхилення щодо профілю чи поведінки системи, визначений моделлю нормальності, досить високий.

Наприклад, візьмемо систему виявлення аномалії S, яка використовує підхід на основі контролю характеристик. Це можна розглядати як пару S = (M, D), де M - модель нормальної поведінки системи, а D - міра близькості, що дозволяє обчислити, враховуючи запис про активність, ступінь відхилення щодо моделі M. Таким чином, кожна система має в основному два модулі: (i) модуль моделювання та (ii) модуль виявлення. Отримана модель згодом використовується модулем виявлення для оцінки нових подій або об'єктів або трафіку як аномальних або віджилих. Саме вимірювання відхилення дозволяє класифікувати події чи предмети як аномальні чи пережиті. Зокрема, модуль моделювання повинен бути адаптивним, щоб справлятися з динамічними сценаріями.

1.4 Класифікація атак на віртуальні сервіси

Вторгнення - це сукупність дій, спрямованих на загрозу безпеки комп'ютерних та мережевих компонентів з точки зору конфіденційності, цілісності та доступності. Це може зробити внутрішній чи зовнішній агент, щоб отримати несанкціонований вхід та контроль механізму безпеки. Для захисту інфраструктури мережевих систем системи виявлення вторгнень (IDS) забезпечують налагоджені механізми, які збирають та аналізують інформацію з різних областей всередині хоста або мережі для виявлення можливих порушень безпеки.

Функції виявлення вторгнень включають (i) моніторинг та аналіз діяльності користувачів, системи та мережі, (ii) налаштування систем для генерації звітів про можливі вразливості, (iii) оцінку цілісності системи та файлів (iv) розпізнавання моделей типових атак (v) аналіз ненормальної активності та (vi) відстеження порушень політики користувачів. IDS використовує оцінку вразливості для оцінки безпеки хоста або мережі. Виявлення вторгнення працює за припущенням, що вторгнення помітно відрізняються від звичайних системних дій і, таким чином, виявляються.

Андерсон у [9] класифікує зловмисників на два типи: зовнішній та внутрішній. Зовнішні зловмисники - це несанкціоновані користувачі машин, на які вони атакують, тоді як внутрішні зловмисники мають дозвіл на доступ до системи, але не мають привілеїв для кореневого або надрукувального режиму. Маскарадний внутрішній зловмисник реєструється, як інші користувачі, які мають законний доступ до конфіденційних даних, тоді як підпільний внутрішній зловмисник, найнебезпечніший, має право вимкнути аудиторський контроль для себе.

У комп'ютерних системах існують різні класи вторгнень чи атак. Їх короткий огляд подається в таблиці 1.1.

1.4 Класифікація систем виявлення вторгнень та систем виявлення вторгнень

Мережеве виявлення вторгнень вивчається майже 20 років. Як правило, поведінка зловмисника помітно відрізняється від поведінки законного користувача і тому може бути виявлена. Ідентифікатори також можуть бути класифіковані на основі їх розгортання в режимі реального часу.

Таблиця 1.1 – Класи комп'ютерних загроз: характеристика та приклади

Назва атаки	Характеристика
Вірус	(i) Самовідтворювальна програма, яка заражає систему без будь-яких знань чи дозволу користувача. (ii) Збільшує рівень зараженості мережевої файлової системи, якщо система має доступ до іншого комп’ютера.
Черв'як	(i) Самовідтворювальна програма, яка розповсюджується через мережеві сервіси в комп'ютерних системах без втручання користувача. (ii) Може завдати великої шкоди мережі, споживаючи пропускну здатність мережі.
Троян	(i) шкідливу програму, яка не може повторитись, але може спричинити серйозні проблеми із безпекою в комп'ютерній системі. (ii) Виявляється корисною програмою, але насправді має секретний код, який може створити резервну систему для системи, що дозволяє їй робити що завгодно в системі легко, і її можна назвати як хакерський контроль над системою без користувача дозвіл.
Відмова в обслуговуванні (DoS)	(i) Спроби заблокувати доступ до системних або мережевих ресурсів. (ii) Втрата послуги - це неможливість роботи певної мережі або послуги хоста, наприклад електронної пошти. (iii) Це реалізується шляхом примушування цільових комп'ютерів (ів) до скидання, або споживання ресурсів. (iv) Запропоновані користувачі не можуть більше спілкуватися належним чином через недоступність сервісу або через перешкоджені носії зв'язку.
Атака мережі	(i) Будь-який процес, який застосовується для зловмисної спроби порушити безпеку мережі, починаючи з рівня зв'язку даних до рівня програми різними способами, такими як маніпулювання мережевими протоколами. (ii) Незаконне використання облікових записів та привілеїв користувачів, виконання дій для видалення мережевих ресурсів та пропускної здатності, виконання дій, що не дозволяють законним авторизованим користувачам отримувати доступ до мережевих служб та ресурсів.

Продовження таблиці 1.1

Фізична атака	Спроба пошкодити фізичні компоненти мереж чи комп'ютерів.
Атака на пароль	Прагне отримати пароль за короткий проміжок часу, і зазвичай це позначається низкою відмов входу.
Атака Збір інформації	Збирає інформацію або знаходить відомі вразливості за допомогою сканування або зондування комп'ютерів або мереж.
Атака на користувач root (U2R) атака	(i) Він може використовувати вразливості, щоб отримати привілеї суперпользователя системи, починаючи як звичайний користувач у системі. (ii) Уразливості включають нюхаючі паролі, атаку словника або соціальну інженерію.
Віддалені до локального хоста (R2L) атаки	(i) Можливість передавати пакети у віддалену систему через мережу, не маючи жодного облікового запису в цій системі, отримувати доступ або як користувач, або як корінь до системи, та робити шкідливі операції. (ii) Здійснює атаку проти публічних служб (таких як HTTP та FTP) або під час підключення захищених служб (таких як POP та IMAP).
Зонд	(i) Сканує мережі, щоб виявити дійсні IP-адреси та зібрати інформацію про хост (наприклад, які послуги вони пропонують, використовувану операційну систему). (ii) Надає інформацію зловмиснику зі списком потенційних уразливих ситуацій, які згодом можуть бути використані для запуску атаки на вибрані системи та служби.

1) IDS на основі хоста (HIDS): HIDS контролює та аналізує внутрішні ресурси обчислювальної системи, а не її зовнішні інтерфейси. HIDS може виявити внутрішню діяльність, таку, яка програма отримує доступ до яких ресурсів і намагається отримати нелегітимний доступ. Прикладом є текстовий процесор, який раптово і незрозуміло починає змінювати базу даних паролів системи. Аналогічно, HIDS може дивитись на стан системи та її збережену інформацію, чи є вона в оперативній пам’яті, або у файловій системі, або у файлах журналів чи деінде. Можна вважати HIDS як агентом, який відстежує, чи все, чи хтось внутрішній чи зовнішній обходив політику безпеки, яку намагається застосовувати операційна система.

2) IDS мережі на основі (COA): NIDS займається виявлення вторгнень в мережі передачі даних. Вторгнення зазвичай трапляються у вигляді аномальних зразків, хоча певні методи послідовно моделюють дані та виявляють аномальні послідовності. Основною причиною цих аномалій є напади, розпочаті сторонніми

зловмисниками, які хочуть отримати несанкціонований доступ до мережі для крадіжки інформації або порушення її.

У типових умовах мережа підключається до решти світу через Інтернет. NIDS зчитує всі вхідні пакети або потоки, намагаючись знайти підозрілі зразки. Наприклад, якщо протягом короткого часу спостерігається велика кількість запитів на підключення TCP до дуже великої кількості різних портів, можна припустити, що хтось здійснює "сканування портів" на деяких комп’ютерах у мережі. Різні види сканування портів та інструменти для їх запуску детально обговорюються в. Сканування портів, як правило, намагається виявити вхідні коди оболонок так само, як це робить звичайна система виявлення вторгнень. Крім перевірки вхідного трафіку, NIDS також надає цінну інформацію про вторгнення у вихідний або місцевий трафік. Деякі атаки можуть навіть проводитися зсередини відстежуваної мережі або мережевого сегмента, а отже, взагалі не розглядаються як вхідний трафік. Дані, доступні для систем виявлення вторгнень, можуть бути на різних рівнях деталізації, наприклад, сліди рівня пакетів та записи IPFIX. Дані, як правило, є високомірними, із сукупністю категоричних та безперервних атрибутів.

Виявлення вторгнень на основі неправильного використання зазвичай шукає відомі нав'язливі схеми, але виявлення вторгнень на основі аномалії намагається визначити незвичні структури. Методи виявлення вторгнень можна класифікувати на три типи за механізмом виявлення. Це включає (i) неправильне використання, (ii) на основі аномалії та (iii) гібрид, як описано в таблиці III. Сьогодні дослідники зосереджуються в основному на виявленні вторгнень у мережу, що базується на аномаліях, оскільки це дозволяє виявити відомі, а також невідомі напади.

Є кілька причин, які роблять виявлення вторгнення необхідною частиною всієї оборонної системи. По-перше, багато традиційних систем і додатків були розроблені без урахування безпеки. Такі системи та програми були спрямовані на роботу в умовах, коли безпека ніколи не була головним питанням. Однак ті самі

системи та програми, коли вони розгорнуті в поточному сценарії мережі, стають головними головними болями в галузі безпеки. Наприклад, система може бути абсолютно безпечною, коли вона ізольована, але стає вразливою, коли вона є підключено до Інтернету. Виявлення вторгнень дає спосіб ідентифікувати та таким чином реагувати на атаки проти цих систем.

По-друге, через обмеження практики інформаційної безпеки та інженерії програмного забезпечення комп'ютерні системи та програми можуть мати недоліки в дизайні або помилки, які можуть бути використані зловмисником для нападу на системи чи програми. Як результат, деякі профілактичні механізми (наприклад, брандмауер) можуть виявитися не настільки ефективними, як очікувалося.

РОЗІДЛ 2
АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ АНОМАЛІЙ У ВІРТУАЛЬНИХ СИСТЕМАХ

Виявлення аномалії намагається знайти шаблони даних, які не відповідають очікуваній нормальній поведінці. Важливість виявлення аномалії пов'язана з тим, що аномалії в даних перекладаються на значну (і часто критичну) діючу інформацію в широкому спектрі областей додатків. Наприклад, аномальна схема трафіку в комп'ютерній мережі може означати, що зламаний комп'ютер надсилає конфіденційні дані несанкціонованому хосту. Однак аномалії в мережі можуть бути викликані декількома різними причинами.

Є дві широкі категорії мережевих аномалій: (а), пов'язаних з продуктивністю аномалій і (б) аномалії, пов'язані з безпекою. Різними прикладами аномалій, пов'язаних з продуктивністю, є: штормові трансляції, перехідні перевантаження, вузол з голосом, пейджинг по всій мережі та збій файлового сервера. Аномалії мережі, пов'язані з безпекою, можуть бути наслідком зловмисної діяльності зловмисників, які навмисно затоплюють мережу непотрібним трафіком, щоб захопити пропускну здатність, щоб законні користувачі не змогли отримувати послуги. Аномалії, пов'язані з безпекою, бувають трьох типів: (і) точка, (іі) контекстуальна та (ііі) колективна аномалії. Ця схема класифікації описана в таблиці IV. Однак наше огляди стосується лише мережевих аномалій, пов’язаних із безпекою.

В даний час мережеве виявлення вторгнень на основі аномалії є основним напрямком досліджень та розробок у сфері виявлення вторгнень. Стають доступними різні системи з мережевими можливостями виявлення вторгнень на основі аномалії, і вивчається багато нових схем. Однак тема ще далеко не дозріла, і ключові питання залишаються вирішеними до того, як широкомасштабне розгортання платформ проти NIDS стане практичним.

2.1 Загальна архітектура NIDS

Багато НІС розроблено дослідниками та практиками. Однак розробка ефективної архітектури боротьби зі NIDSом досі досліджується. Загальна архітектура NIDSy показана на рисунку 2.1.

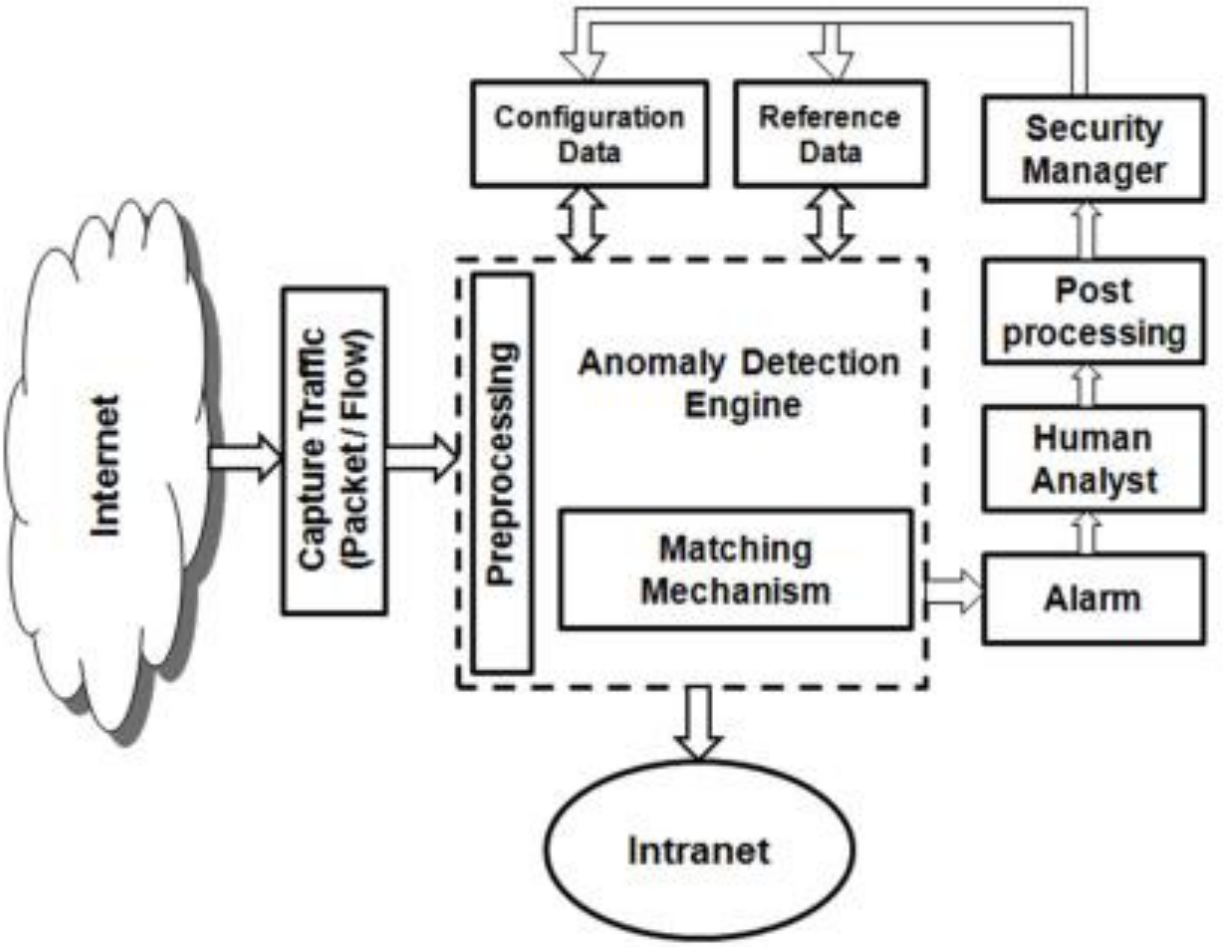

Рисунок 2.1 – Кроки щодо оновлення даних про конфігурацію в NIDS-і

Основні компоненти загальної моделі NIDSy обговорюються нижче.

1) Двигун виявлення аномалій: це серце будь-якої мережі виявлення вторгнень в мережу. Він намагається виявити виникнення будь-якого вторгнення в Інтернеті чи офлайн. Однак перед тим, як надіслати будь-який мережевий трафік до двигуна виявлення, він потребує попередньої обробки. Якщо напади відомі, їх

можна виявити, використовуючи підхід виявлення зловживань. З іншого боку, невідомі напади можна виявити за допомогою підходу, заснованого на аномалії, на основі відповідного механізму відповідності.

Механізм узгодження: це тягне за собою пошук певного шаблону чи профілю в мережевому трафіку, який можна побудувати за допомогою постійного моніторингу поведінки мережі, включаючи відомі подвиги та вразливості. Нижче наведено кілька важливих вимог при розробці ефективного механізму узгодження.

- Узгодження визначає, є чи новий екземпляр belongsto відомого класу, що визначається високим розмірним профілем чи ні. Відповідність може бути неточною.

- Відповідність повинна бути швидкою.

- Ефективна організація профілів може сприяти більш швидкому пошуку під час узгодження.

2) Довідкові дані: Довідкові дані зберігають інформацію про відомі підписи про вторгнення або профілі нормальної поведінки. Довідкові дані потрібно зберігати ефективно. Можливими типами довідкових даних, що використовуються в загальній архітектурі NIDS, є: профіль, підпис та правило. Що стосується NIDSy, це переважно профілі. Елементи обробки оновлюють профілі, коли з’являються нові знання про спостережувану поведінку. Ці оновлення виконуються через регулярні проміжки часу, орієнтовані на партію.

3) Дані конфігурації: це відповідає проміжним результатам, наприклад, частково створеним підписам проникнення. Простір, необхідний для зберігання такої інформації, може бути досить великим. Вивід проміжних даних повинен бути інтегрований з існуючими знаннями для створення послідовних, результатів уточнених.

4) Сигналізація: Цей компонент архітектури відповідає за генерацію тривоги на основі індикації, отриманої від двигуна виявлення.

Аналітик-людина: аналітик відповідає за аналіз, інтерпретацію та вжиття необхідних заходів на основі інформації тривоги, що надається механізмом виявлення. Аналітик також вживає необхідних заходів для діагностики інформації про тривогу як активності після обробки, щоб підтримувати посилання або оновлення профілю за допомогою менеджера захисту.

Таблиця 2.1 – Характеристика та типи систем виявлення вторгнень

Техніка	Характеристика
Неправильно використаний	(i) Виявлення засноване на наборі правил або підписів для відомих атак. (ii) Може виявити всі відомі шаблони атаки на основі довідкових даних. (iii) Як написати підпис, який охоплює всі можливі варіанти відповідного нападу, є складним завданням.
Аномалія	(i) Основне припущення: всі нав'язливі дії обов'язково аномальні. (ii) Такий метод будує нормальний профіль активності та перевіряє, чи стан системи відрізняється від встановленого профілю статистично значущою кількістю для повідомлення про спроби вторгнення. (iii) Аномальні дії, які не є нав'язливими, можуть бути відзначені як нав'язливі. Це помилкові позитиви. (iv) Потрібно вибирати порогові рівні, щоб жодна з перерахованих вище проблем не була необґрунтовано збільшена, а вибір функцій для моніторингу не оптимізований. (v) Обчислювально дорогі через накладні витрати та, можливо, оновлення кількох системних матриць профілю.
Гібридний	(i) використовує переваги як неправильного використання, так і методів виявлення на основі аномалії. (ii) Спроби виявити відомі, а також невідомі напади.

Таблиця 2.2 – Типи, характеристики та приклади аномалій

Типи	Характеристика	Приклад
Точкова аномалія	Екземпляр окремих даних, які були визнані аномальними щодо решти даних.	Ізольований екземпляр мережевого трафіку від звичайних випадків у певний час.
Контекстуальна аномалія	(i) Екземпляр даних, який виявився аномальним у конкретному контексті. (ii) Контекст викликається структурою в наборі даних. (iii) Для визначення контексту використовуються два набори атрибутів: (а) контекстуальні та (б) поведінкові атрибути.	Інтервал часу між покупками в шахрайстві з кредитною карткою
Колективна аномалія	(i) Збір відповідних випадків даних, виявлених аномально щодо всього набору даних. (ii) Колекція подій є аномалією, але окремі події не є аномаліями, коли вони відбуваються окремо в послідовності.	Послідовність, наступна: ... http-web, buffer-overflow, http-web, http-web, ftp, httpweb , ssh , http-web, ssh , buffer-overflow ...

5) Післяобробка: Це важливий модуль в NIDS для післяобробки сформованих сигналів тривоги для діагностики фактичних атак.

6) Захоплення трафіку: Захоплення трафіку є важливим модулем у NIDS. Неочищені дані про трафік фіксуються як на рівні пакетів, так і на потоці. Трафік рівня пакетів може бути зафіксований за допомогою загального інструменту, наприклад, Wireshark, а потім попередньо оброблений перед відправкою в двигун виявлення. Дані про рівень потоку у високошвидкісних мережах складаються з інформації, зведеної з одного або декількох пакетів. Деякі поширені інструменти для зйомки мережевого трафіку рівня потоку включають Nfdump, NfSen та Cisco Netflow V.9.

7) Менеджер безпеки: Збережені підписи вторгнень оновлюються Менеджером безпеки (SM) як і коли стають відомі нові вторгнення. Аналіз нових вторгнень є надзвичайно складним завданням.

2.2 Аспекти виявлення мережевої аномалії

У цьому розділі ми представляємо деякі важливі аспекти виявлення вторгнень на основі аномалії. Проблема виявлення вторгнення в мережу – це проблема класифікації або кластеризації, сформульована з таких компонентів: (i) типи вхідних даних, (ii) відповідність мір близькості, (iii) маркування даних, (iv) класифікація методів на основі використання (v) ідентифікація відповідних ознак та (vi) аномалії звітування. Кожну з цих тем ми обговорюємо коротко.

1) Типи вхідних даних: Основним аспектом будь-якої техніки виявлення вторгнень на основі аномалії є характер вхідних даних, що використовуються для аналізу. Введення – це, як правило, сукупність екземплярів даних (їх також називають об'єктами, записами, точками, векторами, шаблонами, подіями, справами, зразками, спостереженнями, сутностями). Кожен екземпляр даних може бути описаний за допомогою набору атрибутів двійкового, категоріального або числового типу. Кожен екземпляр даних може складатися лише з одного атрибута (одноваріантного) або з декількох атрибутів (багатоваріантних). У випадку випадків багатовимірних даних усі атрибути можуть бути одного типу або можуть бути сумішшю типів даних. Характер атрибутів визначає застосовність методів виявлення аномалії.

2) Відповідність мір близькості: заходи щодо близькості (подібності чи несхожості) необхідні для вирішення багатьох проблем розпізнавання шаблонів у класифікації та кластеризації. Відстань – це кількісна ступінь того, наскільки далеко розташовані два об'єкти. Міри відстані, що задовольняють метричним властивостям, просто називаються метричними, тоді як інші неметричні відстані

вимірювання іноді називають розбіжністю. Вибір міри близькості залежить від типу вимірювання або представлення об'єктів.

Як правило, заходи близькості – це функції, які беруть аргументи як об'єктні пари і повертають числові значення, які стають вищими, оскільки об'єкти стають більш схожими. Міра близькості зазвичай визначається наступним чином.

Нарешті, дані змішаного типу включають як категоричні, так і числові значення. Поширеною практикою кластеризації змішаних наборів даних є перетворення категоричних значень у числові значення, а потім використання алгоритму чисельного кластеризації. Інший підхід полягає в порівнянні безпосередньо категоріальних значень, в яких два різних значення призводять до відстані 1, тоді як однакові значення призводять до відстані 0. Звичайно, можуть застосовуватися й інші заходи щодо категоричних даних. Дві відомі міри близькості, загальний коефіцієнт подібності та загальний коефіцієнт відстані для даних змішаного типу наведені в таблиці V. Такі методи можуть не враховувати інформацію про подібність, вкладену в категоричні значення. Отже, кластеризація не може точно виявити структуру подібності в наборі даних.

3) Маркування даних: Мітка, пов'язана з екземпляром даних, позначає, якщо цей примірник є нормальним або аномальним. Слід зазначити, що отримання точних маркованих даних як нормальних, так і аномальних типів часто є надмірно дорогим. Етикетки часто проводяться вручну фахівцями-людьми, тому необхідно докласти значних зусиль для отримання міток навчальних даних. Крім того, аномальна поведінка часто має динамічний характер, наприклад, можуть виникати нові типи аномалій, для яких немає мічених даних про навчання.

4) Класифікація методів на основі використання маркованих даних: Виходячи з того, наскільки доступні мітки, методи виявлення аномалій можуть працювати в трьох режимах: контрольований, напівпіднаглядний та непідконтрольний.

У контрольованому режимі передбачається наявність навчального набору даних, який позначає екземпляри як для нормального, так і для класу аномалії.

Типовим підходом у таких випадках є побудова прогнозної моделі для класів нормальних проти аномалій. Будь-який невидимий екземпляр даних порівнюється з моделлю, щоб визначити, до якого класу він належить. Є дві основні проблеми, які виникають при контрольованому виявленні аномалії. По-перше, аномальних випадків набагато менше порівняно з нормальними випадками даних тренувань. Питання, що виникають через незбалансований розподіл класів, були розглянуті в галузі вивчення даних та машинного навчання. По-друге, отримання точних та репрезентативних міток, особливо для класу аномалії, зазвичай є складним завданням. Ряд методик вводять штучні аномалії у звичайний набір даних, щоб отримати мічений навчальний набір даних.

Напівконтрольні методи передбачають, що дані тренувань мають мітки випадків лише для звичайного класу. Оскільки для класу аномалії вони не вимагають міток, їх можна легше використовувати порівняно з контрольованими методами. Наприклад, у космічних кораблях сценарій виявлення несправностей аномалії означатиме аварію, яку неможливо моделювати. Типовий підхід, що застосовується в таких методах, полягає у побудові моделі для класу, що відповідає нормальній поведінці, та використанні моделі для виявлення аномалій у тестових даних.

Нарешті, методи без нагляду не потребують даних про навчання, і, отже, вони є найбільш широко застосовними. Методи в цій категорії дозволяють неявно припустити, що нормальні випадки набагато частіші, ніж аномалії у тестових даних. Якщо це припущення не відповідає дійсності, такі методи страждають від високих помилок тривоги. Багато методів нагляду під наглядом можуть бути адаптовані для роботи в режимі без нагляду, використовуючи зразок немміченого набору даних як навчальних даних. Така адаптація передбачає, що дані тесту містять дуже мало аномалій, і модель, засвоєна під час тренінгу, є надійною для цих кількох аномалій.

5) Ідентифікація відповідних функцій: вибір функції відіграє важливу роль у виявленні мережевих аномалій. Методи вибору функцій використовуються в

області виявлення вторгнень для усунення неважливих або невідповідних функцій. Вибір функцій знижує обчислювальну складність, знімає надмірність інформації, підвищує точність алгоритму виявлення, полегшує розуміння даних та покращує узагальнення. Процес вибору функцій включає три основні етапи: (а) генерація підмножини, (б) оцінка підмножини та (в) перевірка. Три різні підходи до генерації підмножини: повний, евристичний та випадковий. Функції оцінювання класифікуються на п'ять різних категорій: на основі балів, ентропії або взаємної інформації, на основі кореляції, на основі послідовності та на основі точності виявлення. Моделювання та реалізація реального світу – це два способи перевірки оцінюваного набору. Концепція фреймворку процесу вибору ознак показана на рисунку 2.2

Алгоритми вибору функцій класифікуються на три типи: обгортковий, фільтруючий та гібридний методи. У той час як методи обгортки намагаються оптимізувати деякі заздалегідь визначені критерії відносно набору функцій як частини процесу вибору, методи фільтрації покладаються на загальні характеристики навчальних даних для вибору особливостей, які не залежать один від одного і сильно залежать від результату. Метод вибору гібридних функцій намагається використовувати найважливіші функції оболонки та методу фільтрації.

Приклад обгортка на основі методи вибору ознак iswhere автори пропонують алгоритм побудови полегшеної IDS за допомогою модифікованого Random Мутації Hill Climbing (RMHC) в якості стратегії пошуку, щоб визначити кандидат підмножина для оцінки, а також з допомогою модифікованої лінійної опорних векторів (SVM) базується на ітераційній процедурі як обгортковому підході для отримання оптимального підмножини функцій.

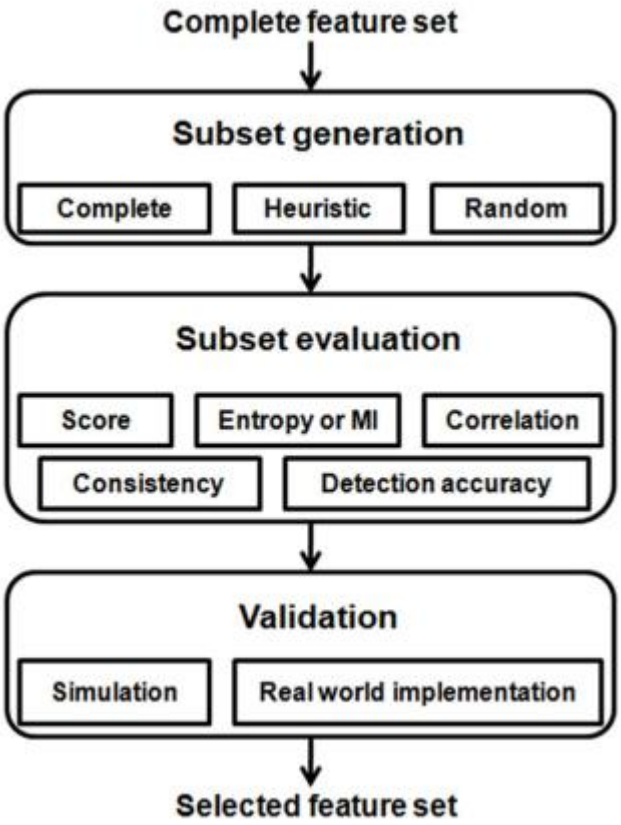

Рисунок 2.2 – Фреймворк для обрання властивостей виявлення ботнетів

Автори методу встановлюють ефективність їх методу з точки зору ефективності виявлення вторгнень без шкоди для швидкості виявлення. Прикладна модель фільтра для вибору особливостей є авторами, де автори сплавляють відповідні заходи на основі кореляції та мінімальної надмірності – максимальної релевантності. Вони оцінюють свій метод на основі наборів даних про вторгнення на еталони для точності класифікації. Є кілька інших методів вибору функцій.

6) Повідомлення про аномалії: Важливим аспектом будь-якої методики виявлення аномалії є спосіб повідомлення про аномалії. Як правило, результати, отримані методами виявлення аномалії, мають два типи: (a) оцінка, яка є величиною, що поєднує (i) відстань або відхилення з посиланням на набір профілів або підписів, (ii) вплив більшості в його сусідство та (iii) чітке домінування відповідного підпростору (як обговорено у розділі III-B5). (b) мітка,

яка є значенням (нормальним або аномальним), що надається кожному тестовому екземпляру. Зазвичай маркування екземпляра залежить від (i) розміру груп, створених методом без нагляду, (ii) компактності груп, (iii) голосування більшості на основі результатів, заданих множинними індексами (кілька прикладних індексів) наведені в таблиці VI) або (iv) чітке домінування підмножини ознак.

РОЗДІЛ 3
МЕТОДИ ТА СИСТЕМИ ДЛЯ ВИЗНАЧЕННЯ АНОМАЛЬНОЇ МЕРЕЖІ

Класифікація методів та систем виявлення мережевих аномалій показана на рисунку 3.1. Ця схема заснована на природі використовуваних алгоритмів. Скласти класифікаційну схему методів та систем виявлення мережевих аномалій нескладно, в першу чергу, тому що серед методів, які використовуються в різних класах, у будь-якій конкретній схемі, яку ми можемо застосувати, є суттєве перекриття. Ми визначилися із шістьма різними класами методів та систем. Ми називаємо їх статистичними, класифікаційними, кластеризованими та зовнішніми, м'якими обчисленнями, на основі знань та комбінованими учнями. Більшість методів мають підкласи, як показано на рисунку 3.1.

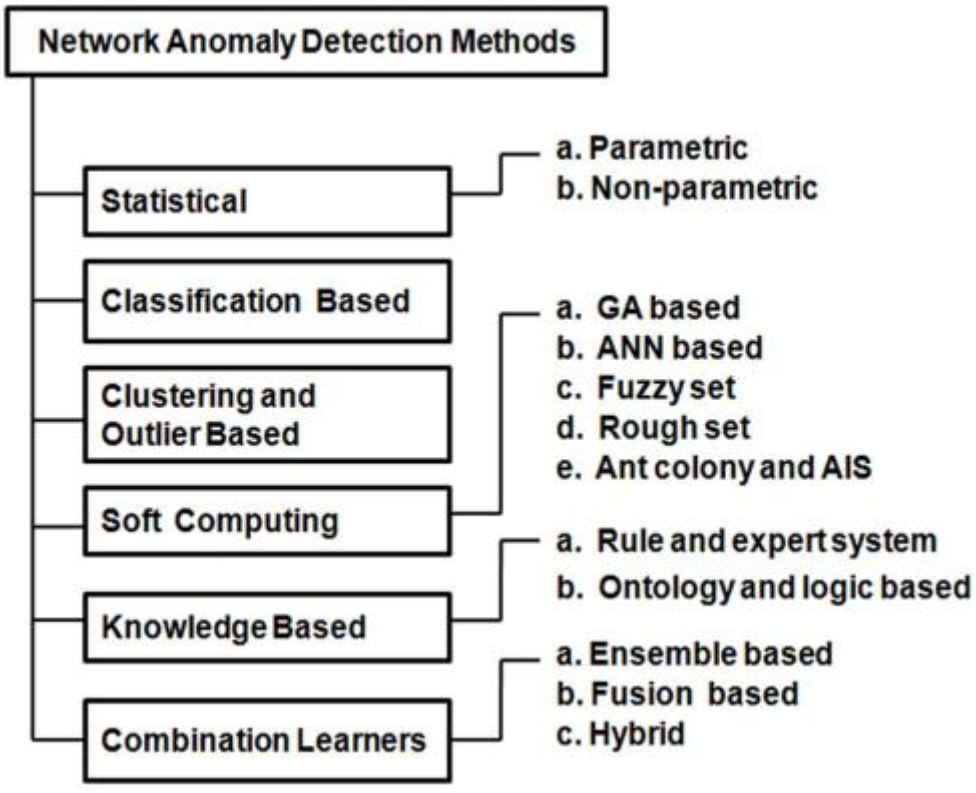

Рисунок 3.1 – Класифікація методів виявлення аномалій в комп'ютерних мережах

У цій роботі ми розрізняємо методи виявлення аномальних мереж та системи, хоча таке розрізнення іноді важко зробити. Мережева система виявлення вторгнень (NIDS) зазвичай інтегрує мережевий метод виявлення вторгнень в архітектуру, яка включає інші пов'язані підсистеми для побудови автономної практичної системи, яка може виконувати всю гаму дій, необхідних для виявлення вторгнень. Ми представляємо декілька NIDS з їх архітектурою та компонентами, коли ми обговорюємо різні категорії виявлення аномалій.

3.1 Статистичні методи та системи

Статистично кажучи, аномалія – це спостереження, яке, як підозрюється, є частково або повністю неактуальним, оскільки воно не породжене прийнятою стохастичною моделлю. Зазвичай статистичні методи підходять статистичній моделі (як правило, для нормальної поведінки) до даних, а потім застосовують статистичний тест висновку, щоб визначити, чи є невидимий екземпляр належить цій моделі. Приклади, які мають малу ймовірність отримати з вивченої моделі на основі застосованої статистики тесту, оголошуються аномаліями. Як параметричні, так і непараметричні методи були застосовані при розробці статистичних моделей для виявлення аномалії. Хоча параметричні методи припускають знання базового розподілу та оцінюємо параметри з цих даних непараметричних методів, як правило, не передбачають знання базового розподілу.

Прикладом статистичної IDS є HIDE. HIDE – система виявлення вторгнень на основі аномалії, яка використовує статистичні моделі та класифікатори нейронної мережі для виявлення вторгнень. HIDE – розподілена система, що складається з декількох ярусів з кожним рівнем, що містить кілька агентів виявлення вторгнень (IDA). ІДА – це компоненти IDS, які відстежують діяльність хоста або мережі. Рівень зонда (тобто верхній рівень, як показано на рисунку 6) збирає мережевий трафік на хості або в мережі, абстрагує трафік на набір

статистичних змінних для відображення стану мережі та періодично генерує звіти для препроцесора подій. Шар препроцесора подій отримує звіти як зонда, так і IDA нижчих ярусів і перетворює інформацію у формат, необхідний статистичній моделі. Статистичний процесор підтримує еталонну модель типових мережевих дій, порівнює звіти препроцесора події з еталонними моделями та формує вектор стимулу для подачі в класифікатор нейронної мережі. Класифікатор нейронної мережі аналізує вектор стимулу зі статистичної моделі, щоб вирішити, чи нормальний мережевий трафік. Пост-процесор генерує звіти для агентів вищих рівнів. Головною привабливістю HIDE є його здатність виявляти напади UDP затоплення навіть при інтенсивності атаки лише 10% фонового трафіку.

З багатьох статистичних методів та NIDS деякі з них описані нижче коротко.

Байєсівські мережі здатні виявляти аномалії в умовах багатьох класів. Запропоновано кілька варіантів основної методики для виявлення вторгнень у мережу та для виявлення аномалії в текстових даних. Основна методика передбачає незалежність між різними ознаками. Запропоновано також декілька варіацій основної методики, що фіксують умовні залежності між різними ознаками, використовуючи складніші байєсівські мережі. Наприклад, автори вводять схему виявлення вторгнень на основі класифікації подій за допомогою байєсівських мереж. Процес прийняття байєсівських рішень покращує рішення щодо виявлення, щоб значно зменшити помилкові тривоги.

Є варінат запровадження ієрархічної багаторівневої статистичної системи виявлення аномалій, яка працює автоматично, адаптивно та проактивно. Це стосується як дротових, так і бездротових спеціальних мереж. Ця система використовує статистичне моделювання та класифікацію нейронної мережі для виявлення мережевих аномалій та несправностей. Система досягає високої швидкості виявлення разом із низькою швидкістю помилкових класифікацій, коли інтенсивність трафіку аномалії становить 5% фонового трафіку, але швидкість виявлення нижча при нижчих рівнях інтенсивності атаки, таких як 1% та 2%.

Правило асоціації видобутку концептуально простий метод, заснований на підрахунку спільного виникнення елементів у базах даних транзакцій, використовувався для однокласного виявлення аномалії шляхом генерування правил із даних без нагляду. Найскладніша і домінуюча частина алгоритму виявлення правил асоціації – це пошук наборів елементів, які мають міцну підтримку. Махоні і Чан представляють алгоритм, відомий як LERAD, який вивчає правила пошуку рідкісних подій у даних часових рядів з великою залежністю і знаходить аномалії в мережевих пакетах протягом сеансів TCP. LERAD використовує алгоритм, подібний до Apriori, який знаходить умовні правила щодо номінальних атрибутів у часовому ряду, наприклад, послідовність вхідних клієнтських пакетів. Антицедент створеного правила – це сполучення рівностей, а наслідком – це набір дозволених значень, наприклад, якщо port = 80 і word3 = HTTP / 1.0, то word1 = GET або POST. Значення допускається, якщо воно спостерігається щонайменше в одному навчальному екземплярі, який задовольняє попередній випадок. Ідея полягає у виявленні рідкісних аномальних подій: тих, які давно не відбулися та мають високий показник аномалії. LERAD – це двопрохідний алгоритм. У першому проході набір правил кандидата формується з випадкової вибірки навчальних даних, що складається з безперебійного мережевого трафіку. У другому проході правила тренуються шляхом отримання набору дозволених значень для кожного попередника.

У роботі запропоновано детектор аномалії на основі корисного навантаження для виявлення вторгнень, відомий як PAYL. PAYL намагається виявити перше виникнення хробака або в мережевому системному шлюзі, або у внутрішній мережі, від пристрою-шахрая та запобігти його поширенню. Тут використовується статистична модель, заснована на мовній n-програмі, відібраних потоків даних. Насправді, PAYL використовує лише 1 -грамну модель (тобто, вона дивиться на розподіл значень, що містяться в одному байті), що вимагає лінійного сканування потоку даних та невеликої 256-елементної гістограми.

Іншими словами, для кожного символу ASCII в діапазоні 0-255 він обчислює його середню частоту, а також дисперсію та стандартне відхилення. Оскільки корисні навантаження (тобто вміст, що надходить або відходить) у різних портах відрізняються за довжиною, PAYL обчислює цю статистику для кожного конкретного спостережуваної довжини корисного навантаження для кожного порту, відкритого в системі. Спочатку спостерігається багато примірних корисних навантажень під час фази навчання та обчислюються профілі корисного навантаження для кожного порту для кожної тривалості корисного навантаження. Під час виявлення кожне надходить корисне навантаження сканується та обчислюється статистика. Новий розподіл корисного навантаження порівнюється з моделлю, створеною під час тренувань. Якщо є значна різниця, PAYL робить висновок, що пакет аномальний і генерує попередження. Автори виявили, що цей простий підхід працює напрочуд добре.

Пісня та ін. запропонувати умовний метод виявлення аномалії для обчислення відмінностей між атрибутами та представити три різні алгоритми максимізації очікування для вивчення моделі. Вони припускають, що атрибути даних розподіляються на атрибути індикаторів та атрибути навколишнього середовища на основі прийнятого користувачем рішення щодо того, які атрибути вказують на аномалію. Метод вивчає типові значення атрибута індикатора та спостерігає за поданими точками даних та позначає їх як аномальні чи ні, виходячи зі ступеня значення атрибутів індикатора, що відрізняються від звичайних значень атрибутів індикатора. Однак якщо значення атрибутів індикатора не обумовлені значеннями атрибутів навколишнього середовища, атрибути індикатора ефективно ігноруються. Точність / відкликання цього методу перевищує 90 відсотків.

Крім властивої їм здатності виявляти мережеві аномалії, статистичні підходи мають і ряд додаткових чітких переваг.

– Вони не вимагають попереднього знання нормальної діяльності цільової системи. Натомість вони мають можливість дізнатися очікувану поведінку системи з спостережень.

– Статистичні методи можуть забезпечити точне повідомлення або генерування тривоги про шкідливі дії, що відбуваються протягом тривалих періодів часу, за умови встановлення відповідних порогових значень або налаштування параметрів.

– Вони аналізують трафік на основі теорії різких змін, тобто тривалий час стежать за трафіком та повідомляють про тривогу, якщо виникають якісь різкі зміни (тобто значні відхилення).

– Недоліки статистичної моделі для виявлення аномалій мереж включають в себе наступне.

– Вони чутливі до того, що зловмисники навчаються таким чином, що мережевий трафік, що генерується під час нападу, вважається нормальним.

– Встановлення значень для різних параметрів або метрик є складним завданням, тим більше, що баланс між помилковими позитивами та помилковими негативами є проблемою. Більше того, передбачається статистичне розподіл на змінну, але не всі форми поведінки можна моделювати за допомогою стохастичних методів. Крім того, більшість схем спираються на припущення про квазістаціонарного процесу, який не завжди реальний. Потрібно тривалий час повідомляти про аномалію вперше, оскільки для побудови моделей потрібен тривалий час.

3.2 Методи та системи на основі класифікації

Класифікація – це проблема визначення того, до якої категорії наборів належить нове спостереження на основі навчального набору даних, що містять спостереження, належність до категорії яких відома. Якщо припустити, що у нас

є два класи, екземпляри яких показані як + і -, а кожен об'єкт може бути x1 та x2, визначений у вигляді двох атрибутів або ознак, лінійна класифікація намагається знайти лінію між класами, тобто провести межу. Межа класифікації може бути нелінійною. При виявленні вторгнень дані є багатомірними, а не лише двовимірні. Атрибути зазвичай змішані, числові та категоріальні, як обговорювалося раніше.

Таким чином, методи класифікації засновані на встановленні явної або неявної моделі, яка дозволяє класифікувати структури мережевого трафіку на кілька класів. Особливістю цих методів є те, що їм потрібні мічені дані для навчання поведінкової моделі – процедури, що пред'являє високі вимоги до ресурсів. У багатьох випадках застосування принципів машинного навчання, таких як класифікація, збігається з принципами статистичних прийомів, хоча попередня методика орієнтована на побудову моделі, яка покращує її результативність на основі попередніх результатів. Для виявлення аномалії в даних мережевого трафіку застосовано декілька методів, заснованих на класифікації (наприклад, k-найближчий сусід, векторні машини підтримки та дерева рішень).

Прикладом класифікації IDS на основі класифікації є автоматизований аналіз даних та майнінг (ADAM), який забезпечує тестовий блок для виявлення аномальних випадків. Діаграма архітектури ADAM показана на рисунку 8. ADAM використовує комбінацію методів класифікації та майнінгу правил асоціації, щоб виявити атаки в аудиторському слід TCP-дампу. По-перше, ADAM створює сховище "нормальних" частих наборів елементів з періодів без атаки. По-друге, ADAM запускає онлайн- алгоритм на основі розсувних вікон, який знаходить часті набори елементів у з'єднаннях і порівнює їх з тими, що зберігаються у звичайному сховищі наборів елементів, відкидаючи ті, які вважаються нормальними. ADAM використовує класифікатор, який був навчений класифікувати підозрілі з'єднання як відомий тип атаки або невідомий тип або помилковий сигнал тривоги.

Нижче описано кілька коротких методів виявлення мережевих аномалій та NIDS.

Методи виявлення аномалій на основі класифікації зазвичай можуть давати кращі результати, ніж методи без нагляду (наприклад, на основі кластеризації) через використання мічених навчальних прикладів. У традиційній класифікації нова інформація може бути включена шляхом перепідготовки з усім набором даних. Однак це час споживання. Алгоритми поступової класифікації роблять таке навчання більш ефективним. Хоча методи, засновані на класифікації, є популярними, вони не можуть виявити або передбачити невідомий напад або подію, поки не буде подано відповідну навчальну інформацію для перепідготовки.

На додаток до кількох методів виявлення, зокрема, зазначених вище, ми також обговорюємо IDS на основі класифікації, відомий як DNIDS (надійна система виявлення вторгнень у мережу). Цей IDS розроблений на основі міри комбінованої чутливості та ізоляції алгоритму k-Найближчого сусіда (CSI-KNN).

DNIDS може ефективно виявляти вторгнення в мережу, надаючи постійну послугу під атакою. Алгоритм виявлення вторгнень аналізує характеристики мережевих даних, застосовуючи два заходи: дивацтво та замкнутість. Ці заходи використовуються кореляційним підрозділом для підвищення сигналу про вторгнення разом з інформацією про довіру. Для більш швидкої інформації DNIDS паралельно використовує кілька класифікаторів CSF-KNN. Вона також включає в механізм вторгнення толерантного для моніторингу хостів і класифікаторів, що працюють на них, так що вихід з ладу будь-якого компонента можуть бути оброблені ретельно. Датчики захоплюють мережеві пакети з мережевого сегмента і перетворюють їх у вектори на основі з'єднання. Детектор – це сукупність класифікаторів CSI-KNN, які аналізують вектори, що подаються датчиками. Менеджер менеджерів, агенти сповіщення та агенти технічного обслуговування розроблені для допуску до вторгнень і встановлюються на захищеному адміністративному сервері під назвою Station. Менеджер виконує завдання з генерації мобільних агентів та відправлення їх на виконання завдань.

Підходи до виявлення аномалій на основі класифікації популярні для виявлення мережевих аномалій. Нижче наведено деякі переваги.

– Ці методи є гнучкими для навчання та тестування. Вони здатні оновлювати свої стратегії виконання шляхом включення нової інформації. Отже, пристосованість можлива.

– Вони мають високий показник виявлення для відомих атак з урахуванням відповідного встановлення порогу.

– Хоча такі методи популярні, вони мають такі недоліки.

– Методи сильно залежать від припущень, зроблених класифікаторами.

– Вони споживають більше ресурсів, ніж інші методи.

– Вони не можуть виявити або передбачити невідомий напад або подію, поки не буде подано відповідну навчальну інформацію.

3.3 Методи та системи на основі кластеризації

Кластеризація – це завдання розподілити набір об’єктів у групи, які називаються кластерами, щоб об'єкти в одному кластері були більш схожими в деякому розумінні один на одного, ніж на інших кластерах. Кластеризація застосовується при розвідувальному пошуку даних. Наприклад, якщо у нас є набір немаркованих об'єктів у двох вимірах, ми можемо мати можливість об'єднати їх у 5 кластерів, намалювавши навколо них кола або еліпси. Точки за межами фігур – малоймовірні. Кластеризація є прикладом некерованого машинного навчання.

Кластеризація може бути виконана при виявленні мережевої аномалії в офлайн-середовищі. Такий підхід додає додаткової можливості адміністраторам і дозволяє їм більш точно визначати загрози для їхньої мережі за допомогою використання декількох методів на даних із багатьох джерел. Отже, великий обсяг діяльності, яка може знадобитися для виявлення вторгнення в режимі реального часу в Інтернет-NIDS, може бути усунена, досягнувши ефективності.

Наприклад, MINDS (Minnesota Intrusion Detection System) – система базування даних для виявлення вторгнень у мережу. Архітектура MINDS наведена на рисунку 3.3.

Вона приймає дані NetFlow, зібрані через інструменти потоку, як вхідні дані. Інструменти потоку лише захоплюють інформацію заголовка пакетів і будують односторонні сеанси потоків. Аналітик використовує MINDS для аналізу цих файлів даних у пакетному режимі. Причина запуску системи в пакетному режимі пов’язана не з часом, необхідним для аналізу цих файлів, а в тому, що аналітику це зручно робити. Перед подачею даних у модуль виявлення аномалії виконується етап фільтрації даних для видалення мережевого трафіку, в якому аналітик не зацікавлений.

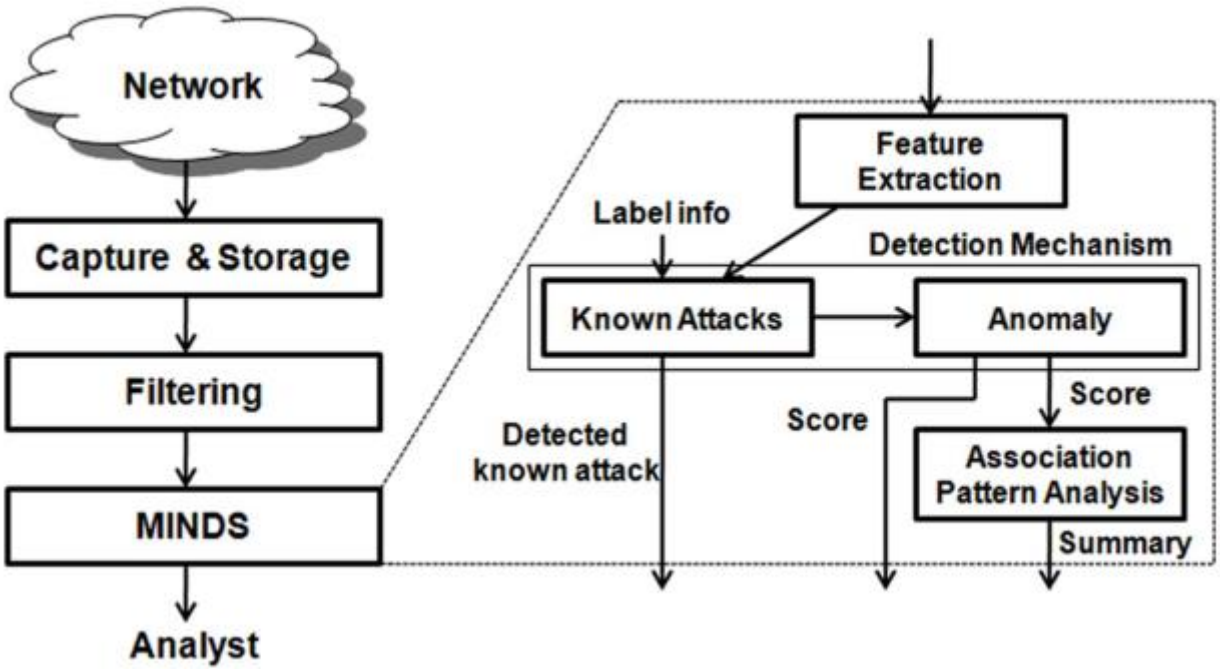

Рисунок 3.3 – Архітектура системи MINDS

Перший крок MINDS – витягнути важливі функції, які використовуються. Потім він підсумовує функції, засновані на часових вікнах. Після етапу побудови функції відомий модуль виявлення атак використовується для виявлення мережевих з'єднань, що відповідають атакам, для яких доступні підписи, та для

видалення їх з подальшого аналізу. Потім активізується техніка виходу, щоб призначити бал аномалії кожному мережевому з'єднанню. Тоді людський аналітик розглядає лише найаномальніші зв’язки, щоб визначити, чи це фактичні напади чи представляють іншу цікаву поведінку. Модуль аналізу шаблонів асоціацій цієї системи призначений для підведення підсумків мережевих з'єднань відповідно до присвоєного рангу аномалії. Аналітик надає зворотній зв'язок після аналізу створених резюме та вирішує, чи ці підсумки корисні для створення нових правил, які можуть бути використані для виявлення відомих атак.

Методи кластеризації часто застосовуються при виявленні аномалії. До них відносяться алгоритми кластеризації одноланцюгових, kmeans (кластеризація помилок у квадраті) та алгоритми ієрархічної кластеризації, щоб згадати декілька.

Є система виявлення вторгнень на основі аномалії, відому як ADMIT, яка виявляє зловмисників, створюючи профілі користувачів. Він відслідковує послідовність команд, які користувач використовує під час використання комп'ютера. Профіль користувача представлений кластеризацією послідовностей команд користувача. Таким чином, збирання та обробка даних базується на хості. Система кластеризує командну послідовність користувача, використовуючи LCS (Найдовша загальна послідовність) як показник подібності. Він використовує алгоритм динамічного кластеризації, який створює початковий набір кластерів, а потім уточнює їх шляхом розщеплення та об'єднання за необхідності. Коли новий користувач вводить послідовність команд, він порівнює послідовність з профілями користувачів, які він вже має. Якщо це довга послідовність, вона розбивається на ряд менших послідовностей. Послідовність, яка не схожа на звичайний профіль користувача, вважається аномальною. Одна аномальна послідовність переноситься як шум, але послідовність аномальних послідовностей, набраних одним одним користувачем, призводить до того, що користувач позначається як маскарадер або концепція дрейфу. Система також може використовувати додаткові кластеризації для виявлення маскарадерів.

Застосовують також розподілений алгоритм виявлення вторгнень, який кластеризує дані двічі. Перша кластеризація вибирає аномалії кандидатів на IDS агента, які розміщуються розподіленим способом у мережі, а друга кластерна обчислення намагається визначити справжні атаки на центральну IDS. Перший алгоритм кластеризації по суті такий же, як запропонований. В кожному IDS агента передбачається, що малі кластери містять аномалії, і всі малі кластери об'єднуються, утворюючи єдиний кандидат-кластер, що містить усі аномалії. Кандидатські аномалії з різних ідентифікаторів агента надсилаються до центрального IDS, який знову кластеризується за допомогою простого ієрархічного алгоритму кластеризації одноланцюгових каналів. Він вибирає найменші k кластери, що містять справжні аномалії. Вони отримують 90% частоти виявлення атак за тестовими даними про вторгнення.

Черви часто досить розумні, щоб приховати свою діяльність і ухилитися від виявлення IDS. Чжуан та ін. запропонувати метод під назвою PAIDS (сприяння близькості IDS) для виявлення нових глистів, коли вони починають поширюватися. PAIDS працює інакше, ніж інші IDS, і він був розроблений для спільної роботи з існуючими IDS, такими як IDS на основі аномалії для підвищення продуктивності. Мета дизайнерів PAIDS – виявити нових та інтелектуальних швидко розмножуються хробаків та перешкоджати їх розповсюдженню, зокрема, коли черв'як тільки починає поширюватися. Ні методи, засновані на підписах, ні аномалії, не можуть досягти таких можливостей. Підхід базується в основному на спостереженні, що під час початкової фази нового хробака заражені хости кластеруються з точки зору географії, IP-адреси та, можливо, навіть використовуваних DNS.

Нижче наведено деякі переваги використання кластеризації.

– Для розбиття підходу, якщо до може бути надана точно то завдання легко.

– Інкрементна кластеризація (в контрольованому режимі) методах є ефективним для швидкої генерації відповіді.

– Це вигідно в разі великих масивів даних в групу в аналогічні числа класів для виявлення мережевих аномалій, так як це зменшує складність обчислень під час виявлення вторгнень.

– Це забезпечує стабільну ефективність порівняно з класифікаторами або статистичними методами.

Недоліками методів на основі кластеризації наступні.

– Більшість методів запропоновано обробляти лише безперервні атрибути.

– У методах виявлення вторгнень, заснованих на кластеризації, припущення полягає в тому, що більші кластери є нормальними, а менші кластери – атаками або вторгненнями. Без цього припущення важко оцінити техніку.

– Використання невідповідної міри близькості негативно впливає на швидкість виявлення.

– Динамічне оновлення профілів займає багато часу.

Існує кілька методів ідентифікації мережевих аномалій на основі зовнішньої структури. Коли ми використовуємо алгоритми, що базуються на зовнішньому рівні, припущення полягає в тому, що аномалії – це рідкісні події в мережі. Набори даних про вторгнення зазвичай містять змішані, числові та категоріальні атрибути. Багато алгоритмів раннього виявлення раніше працювали лише з безперервними атрибутами; вони ігнорували категоричні атрибути або моделювали їх у манерах, що спричинили значну втрату інформації.

Щоб подолати цю проблему введено відстань для даних, що містять поєднання категоричних та безперервних атрибутів, і використовувати їх для виявлення аномалії на основі зовнішньої форми. Вони визначають показник аномалії, який може бути використаний для ідентифікації залишків у змішаному просторі атрибутів, розглядаючи залежності серед атрибутів різних типів. Їх функція оцінки балів аномалії базується на глобальній моделі даних, яку можна

легко побудувати, комбінуючи локальні моделі, побудовані незалежно на кожному вузлі.

Вони розробляють ефективний алгоритм наближення в один прохід для виявлення аномалії, який ефективно працює в розподілених середовищах виявлення з дуже малою втратою точності виявлення. Кожен вузол обчислює власні атрибути, а міжвузлова комунікація, необхідна для обчислення глобальних видатків, не є істотною. Крім того, автори показують, що їхній підхід добре працює в динамічних ситуаціях мережевого трафіку, коли дані, крім потокової передачі, також змінюються в природі в міру просування часу, що призводить до зрушення концепції.

Деякі з переваг виявлення аномалії на основі зовнішніх впливів полягають у наступному.

Легко виявити атакуючого, коли набори даних мають менші розміри.

– Бурхливі та поодинокі напади можна ефективно визначити за допомогою цього методу.

– Недоліки аномального значення на основі виявлення аномалій включають в себе наступне.

– Більшість методик використовують як кластеризацію, так і зовнішнє виявлення. У таких випадках складність може бути високою порівняно з іншими методами.

– Методи дуже залежать від параметрів.

Порівняння декількох методів виявлення аномалії мережевих мереж на основі кластеризації та зовнішнього вигляду наведено в таблиці IX.

3.4 Програмні обчислювальні методи та системи

М’які обчислювальні методи підходять для виявлення мережевої аномалії, оскільки часто не можна знайти точних рішень. М’які обчислення зазвичай вважаються такими, що охоплюють такі методи, як генетичні алгоритми, штучні

нейронні мережі, нечіткі набори, грубі набори, алгоритми колонії мурашок та штучні імунні системи. Нижче ми описуємо кілька методів та систем м'яких обчислень для виявлення мережевої аномалії.

1) Підходи до генетичного алгоритму: Генетичні алгоритми – це методи адаптивного евристичного пошуку, засновані на популяції, засновані на еволюційних ідеях. Підхід починається з перетворення проблеми в фреймворку, який використовує хромосомну структуру даних. Генетичний детектор вторгнень (GBID) заснований на вивченні поведінки окремих користувачів. Цей профіль поведінки використовується для виявлення вторгнення на основі минулої поведінки.

2) Підходи з використанням штучної нейронної мережі: Штучні нейронні мережі (ANN) мотивовані визнанням того, що людський мозок обчислює абсолютно інший спосіб, ніж звичайний цифровий комп'ютер. Мозок організовує свої складові, відомі як нейрони, для того, щоб виконувати певні обчислення (наприклад, розпізнавання образів, сприйняття та управління рухом) у багато разів швидше, ніж найшвидший цифровий комп'ютер.

Для досягнення високої продуктивності реальні нейронні мережі використовують масивні взаємозв'язки нейронів. Нейронні мережі набувають знань про навколишнє середовище за допомогою процесу навчання, який систематично змінює сили взаємозв'язку або синаптичні ваги мережі для досягнення бажаної мети проектування.

Прикладом IDS на основі ANN є RT- UNNID. Ця система здатна інтелектуально виявляти вторгнення в режимі реального часу за допомогою непідконтрольних нейронних мереж (UNN). Архітектура RT-UNNID наведена на рисунку 3.4.

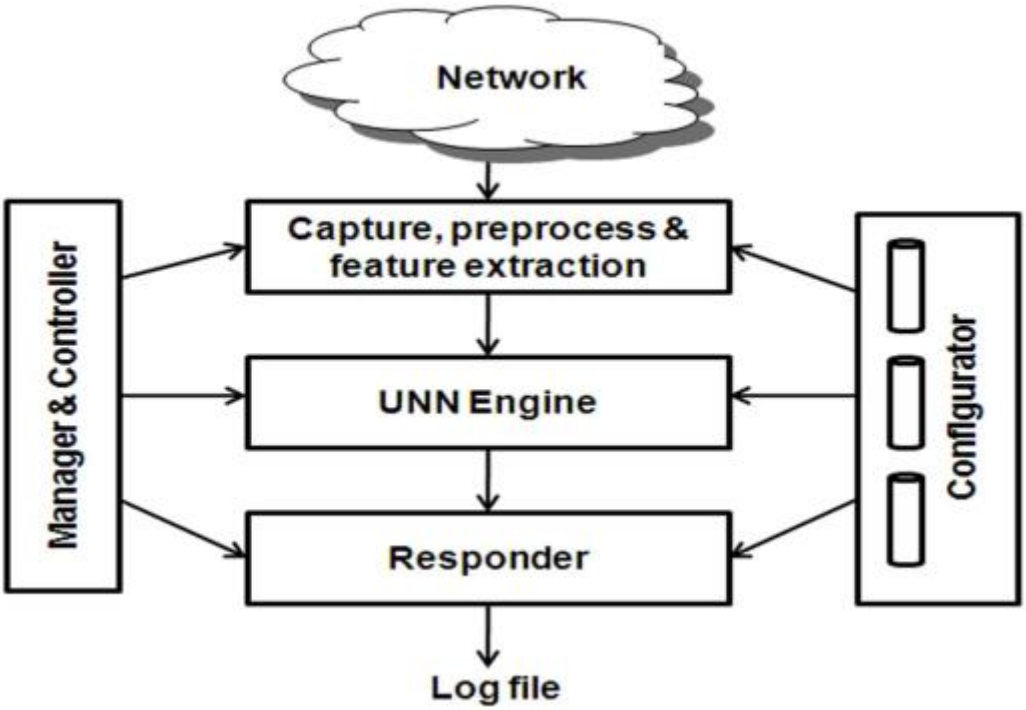

Рисунок 3.4 – Архітектура RT-UNNID системи

Перший модуль фіксує та попередньо обробляє дані мережевого трафіку в реальному часі для протоколів: TCP, UDP та ICMP. Він також витягує числові ознаки та перетворює їх у двійкову чи нормалізовану форму. Перетворені дані надсилаються до механізму виявлення на базі UNN, який використовує Адаптивну теорію резонансу (ART) та "Самоорганізуючу карту" (SOM), нейронні мережі. Нарешті, вихід двигуна виявлення надсилається респонденту для запису в системний файл журналу користувача та для створення тривоги при виявленні атак. RT-UNNID може працювати в режимі реального часу для виявлення відомих і невідомих атак у мережевому трафіку з високою швидкістю виявлення.

Підхід Кеннаді автономно навчається нових атак швидко, використовуючи модифіковане підкріплення. Його підхід використовує зворотний зв'язок для оновлення підписів, коли виникає нова атака і досягається задовільних результатів. Впроваджено вдосконалений підхід до виявлення мережевих аномалій за допомогою ієрархії нейронних мереж. Нейронні мережі навчаються

за допомогою даних, які охоплюють весь нормальний простір і здатні ефективно розпізнавати невідомі атаки.

Окрім методів виявлення, обговоримо декілька ідентифікаторів нижче.

NSOM (мережеві карти самоорганізації) – це мережевий IDS, розроблений за допомогою карт самоорганізації (SOM – Self-Organized Maps). Він виявляє аномалії, визначаючи звичайну або прийнятну поведінку, а нерегулярну поведінку – як потенційно нав'язливу. Для класифікації трафіку в режимі реального часу використовується структурований SOM. Він постійно збирає мережеві дані з мережевого порту, попередньо обробляє ці дані та вибирає функції, необхідні для класифікації. Потім він запускає процес класифікації – частину пакетів за один раз – і потім надсилає отриману класифікацію графічному інструменту, який динамічно зображує дії, що здійснюються на мережевому порту, коли він отримує більше пакетів. Гіпотеза полягає в тому, що звичайний трафік, який представляє нормальну поведінку, буде згрупований навколо одного або декількох центрів кластерів, а будь-який нерегулярний трафік, який представляє ненормальну та, можливо, підозрілу поведінку, буде кластеризований на додаток до звичайного кластеризації трафіку. Система здатна класифікувати регулярний та нерегулярний та, можливо, нав'язливий мережевий трафік для даного хоста.

Існує метод побудови класифікаторів за допомогою нечітких правил асоціації та використовувати його для виявлення мережевих вторгнень. Набори нечітких асоціаціативних правил використовуються для опису різних класів: нормальних та аномальних. Такі нечіткі правила асоціації є правилами асоціації класів, де наслідки задаються класами. Чи належить навчальний екземпляр до певного класу, визначається за допомогою відповідних показників, запропонованих авторами. Правила нечіткої асоціації індукуються за допомогою звичайних навчальних зразків. Тестовий зразок класифікується як нормальний, якщо сумісність створеного набору правил перевищує певний поріг; ті, хто має нижчу сумісність, вважаються аномальними. Автори також пропонують новий

метод прискорити алгоритм індукції правил за рахунок зменшення елементів із витягнутих правил.

Окрім нечітких заданих теоретичних методів виявлення, ми обговорюємо два IDS, а саме: NFIDS та FIRE нижче.

NFIDS – це мережева система виявлення вторгнень на основі нейро-нечіткої аномалії. Він складається з трьох ярусів. Рівень I містить декілька агентів виявлення вторгнень (MAP). ІДА – це компоненти IDS, які відстежують діяльність хоста або мережі та повідомляють про аномальну поведінку до рівня 2. Агенти TierII виявляють стан мережі локальної мережі на основі мережевого трафіку, який вони спостерігають, а також звіти від агентів першого рівня в локальній мережі. Рівень III поєднує звіти вищого рівня, співвідносить дані та надсилає тривогу в інтерфейс користувача. У цій системі є чотири основні типи агентів: TCPAgent, який відстежує з'єднання TCP між хостами та мережею, UDPAgent, який шукає незвичний трафік із залученням даних UDP, ICMPAgent, який контролює трафік ICMP та PortAgent, який шукає незвичні послуги в мережі.

FIRE (Fuzzy Intrusion Recognition Engine) – система виявлення вторгнень на основі аномалії, яка використовує нечітку логіку для оцінки того, чи відбувається зловмисна активність у мережі. Система поєднує просту метрику мережевого трафіку з нечіткими правилами для визначення ймовірності конкретних або загальних мережевих атак. Після того, як показники будуть доступні, вони оцінюються за допомогою нечіткого теоретичного підходу. Система приймає нечіткі профілі мережевого трафіку як входи до свого набору правил і повідомляє про зловмисність.

4) Підходи чорнової множини: Приблизний набір – це наближення чіткого набору (тобто звичайного набору) з точки зору пари множин, що є його нижньою та верхньою наближеннями. У стандартній і оригінальної версії чорнового набору теорії, два наближення чіткі множини, але і в інших варіантах аппроксимирующего множину може бути нечіткими множинами. Математичні

рамки грубої теорії множин дозволяють моделювати відносини з мінімальною кількістю правил.

Чорнові набори мають дві корисні особливості: (i) надання можливості навчатись із наборами даних щодо невеликих розмірів (ii) та загальною простотою. Вони можуть бути застосовані для виявлення аномалії шляхом моделювання нормальної поведінки в мережевому трафіку. Так, наприклад, в, автори представляють нечіткі Грубий С-засоби кластеризації методу для виявлення вторгнення в мережу шляхом інтеграції теорії нечітких множин і грубу теорії множин для досягнення високої швидкості виявлення.

5) Підходи на основі алгоритмів колонії мурашок та системи штучної імунної системи: Оптимізація колонії мурашок та пов'язані з ними алгоритми є імовірнісними методами вирішення обчислювальних задач, які можна переформулювати для пошуку оптимальних шляхів через графіки. Алгоритми засновані на поведінці мурашок, які шукають шлях між своєю колонією та джерелом їжі.

Такі системи навчання виявляють або класифікують стійкі функції без будь-якого зворотного зв’язку з навколишнього середовища.

Завдяки адаптивності ANN, можна тренувати та тестувати випадки поступово, використовуючи певні алгоритми. Багаторівневі методи на основі нейронної мережі є більш ефективними, ніж однорівневі нейромережі.

Непідконтрольне навчання за допомогою конкурентних нейронних мереж ефективне в кластеризації даних, вилученні функцій та виявленні подібності.

Чорнові набори корисні для усунення невідповідності в наборі даних та для створення мінімального, не надмірного та послідовного набору правил.

Нижче вказані деякі недоліки методів м'яких обчислень.

Під час тренувань нейронної мережі може виникнути перенапруга

Якщо достовірна кількість звичайних даних про дорожній рух недоступна, навчання методикам стає дуже важким.

Більшість методів мають проблеми з масштабуванням.

Грубе покоління правил на основі множин страждає від підтвердження повноти.

У нечітких методах, заснованих на правилах, складне завдання – скорочення відповідної ідентифікації підмножини правил та динамічне оновлення правил під час виконання.

3.5 Методи та системи на основі знань

У методах, заснованих на знаннях, мережеві або хостові події перевіряються за заздалегідь визначеними правилами або моделями атаки. Мета полягає в тому, щоб представити відомі напади узагальнено, щоб полегшити обробку фактичних подій. Прикладами методів, заснованих на знаннях, є експертні системи, засновані на правилах, онтологічний, логічний та перехідний аналіз.

Ці методи шукають випадки відомих атак, намагаючись співставити із заздалегідь визначеними уявленнями про атаку. Пошук починається, як і інші методи виявлення вторгнень, з цілковитою відсутністю знань. Подальше узгодження дій із відомою атакою допомагає здобути знання та ввійти в регіон з більш високою впевненістю. Нарешті, можна показати, що подія чи активність досягли максимального показника аномалії.

Нижче наведено кілька визначних методів виявлення мережевих аномалій та NIDS.

1) на основі правил і підходів на основі експертних систем: системний підхід експерта є одним з найбільш широко використовуваних на знаннях методів. Експертна система, в традиційному розумінні, – це система, заснована на правилах, з пов'язаною базою знань або без неї. Експертна система має механізм правил, який відповідає правилам відповідно до поточного стану системи, і залежно від результатів узгодження запускає одне або більше правил.

Snort – це фактично популярний IDS на основі правил. Цей IDS з відкритим кодом відповідає кожному пакету, який він дотримується, та сукупності правил. Антицедент правила Snort – булева формула, що складається з предикатів, які шукають конкретні значення полів, наявних у заголовках IP, заголовках транспорту та корисному навантаженні. Таким чином, правила Snort визначають пакети атак на основі IP-адрес, номерів портів TCP або UDP, кодів або типів ICMP та вмісту рядків у корисному навантаженні пакету. Правила Snort розподіляються в пріоритетні класи на основі потенційного впливу попереджень, які відповідають правилам. Правила Снорта склалися протягом його історії 15 років. Кожне правило Snort має пов'язану документацію з можливістю помилкових позитивів та негативів, а також коригувальні дії, які слід вжити, коли правило піднімає попередження. Правила фронт – прості та легко зрозумілі. Користувачі можуть вносити правила, спостерігаючи нові типи аномального чи зловмисного трафіку. В даний час Snort має понад 20 000 правил, включно з тими, які подали користувачі.

Система виявлення вторгнень на зразок Snort може працювати на комп'ютері загального призначення і може спробувати перевірити всі пакети, що проходять через мережу. Однак комплексне спостереження за пакетами у великій мережі, очевидно, є дорогим завданням, оскільки воно вимагає швидкого огляду великої кількості мережевих інтерфейсів. Багато сотень правил, можливо, повинні відповідати одночасно, що робить масштабування майже неможливим.

2) Онтологічний та логічний підходи: можна моделювати підписи атаки за допомогою виразної логічної структури в режимі реального часу, включаючи обмеження та статистичні властивості. Шаблони вторгнення задаються як формули у виразно насиченій та ефективно відслідковуваній логіці під назвою EAGLE та оцінюються за допомогою файлів журналів DARPA.

До основних переваг методів виявлення аномалії на основі знань можна віднести наступне.

Ці методи є надійними та гнучкими.

Ці методи мають високий показник виявлення, якщо можна належним чином отримати значну базу знань про атаки, а також про звичайні випадки.

Нижче наведені деякі недоліки методів, заснованих на знаннях.

Розвиток високоякісних знань часто важкий і трудомісткий.

Через відсутність упереджених нормальних даних та даних про атаку такий метод може генерувати велику кількість помилкових сигналів тривоги.

Такий метод може не виявити рідкісних або невідомих нападів.

Динамічне оновлення правил чи бази знань – дорога справа.

РОЗІДЛ 4
СПЕЦІАЛЬНА ЧАСТИНА. КЛАСИФІКАЦІЯ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Система виявлення вторгнень - це програмне забезпечення або пристрій, який відстежує мережу за ненормальними або шкідливими діями та попереджає адміністратора. Системи виявлення вторгнень (IDS) використовуються для виявлення різних атак. Ці атаки класифікуються як:

1. Відмова в обслуговуванні (DoS): Атака DoS - це атака, при якій зловмисник заповнює обчислювальний ресурс або ресурс пам’яті помилковими запитами, так що він не може обслуговувати законні запити і тим самим забороняє користувачам доступ до послуги.

2. Зондування: зондування - це атака з метою отримати конфігурацію цільової машини або мережі.

3. Користувач до кореня (U2R): ці атаки мають на меті отримати адміністративний доступ до машини, в якій зловмисник має доступ на рівні користувача.

4. Віддалене до локального (R2L): R2L - це атака, при якій користувач надсилає пакети на машину через Інтернет, до якої користувач не має доступу, щоб викрити вразливості та використовувати привілеї, які матиме місцевий користувач комп'ютер.

Класифікація системи виявлення вторгнень базується на таких чинниках:

1. Розташування.

2. Функціональність.

3. Підхід до розгортання.

4. Механізм виявлення.

4.1 Класифікація за розташуванням системи

1. Визначення вторгнень на основі хоста:

HIDS - це система, яка визначає єдину комп'ютерну систему виявлення вторгнень, яка відслідковує безпеку цієї системи або комп'ютера від внутрішніх і зовнішніх атак. Внутрішні атаки стосуються ситуації, коли вона виявляє, до якої програми доступ до якого ресурсу, і чи є якісь порушення безпеки. Для прикладу текстового процесора раптом починає доступ до бази даних паролів і починає його зміни. У другій частині, що стосується зовнішніх атак, HIDS аналізує пакети до та після цієї системи (комп'ютера) на її інтерфейсах. HIDS реагує, записуючи активність та повідомляючи про це призначеному органу. У програмах HIDS для загрози, таких як антивірус, шпигунське програмне забезпечення встановлюється в системі, яка стежить за безпекою.

Плюси:

1. HIDS може захистити від локальної мережі.
2. HIDS універсальний.
3. Вимагає меншої підготовки, ніж СНІД.
4. HIDS не вимагає пропускної здатності землі.
5. HIDS забезпечує сканування реєстру локальних машин .

Мінуси:

1. Пасивна система, яка повинна чекати, коли подія буде вказівкою нападу, і не може проактивно її запобігти.
2. Збір даних відбувається на основі хоста.
3. Запис у журнал чи діяльність звітності призведе до додаткового навантаження для мережі.
4. Розумні хакери можуть атакувати та відключати HIDS, а атакуюча HIDS вимагає часу на обробку, зберігання, пам'ять та інші системні ресурси.

2. Мережева системи виявлення вторгнень.

Мережева система виявлення вторгнень (NIDS) здійснює моніторинг мережевого трафіку та аналізує поточний рух для атак. Про виявлення нападу або при виявленні ненормальної поведінки попередження може бути надіслано адміністратору. NIDS може виявити 4 основні типи атак: відмова в послугах, зонд, користувач на root і віддалений для користувача. Прикладами реалізації N IDS є Snort ISS, Cisco Secure IDS і Dragon Enterasys.

Плюси:

1. Адаптований до навколишнього середовища платформи.
2. Управління СНІД здійснюється централізовано.

Мінуси:

1. Вимагає більшої підготовки.
2. Використовується пропускна здатність локальної мережі.
3. Частота відмов вище.

4.2 Класифікація за функціональністю

1. Система виявлення вторгнень.

Виявлення вторгнень - це процес виявлення шкідливої діяльності, спрямованої на обчислювальні та мережеві ресурси. Існує два типи систем виявлення вторгнень 1) HIDS 2) NIDS. Системи виявлення вторгнень виявляють, чи є вторгнення, і повідомляють про це адміністратору. Існує два види виявлення вторгнень 1) Виявлення аномалії 2) Виявлення неправильного використання. Виявлення аномалій аналізує зібрану інформацію та порівнює її з базовою лінією, яка є звичайною поведінкою служби. Виявлення зловживань засноване на підписі відомих атак. Це нічим не зупиняє їх. Він просто їх виявляє. IDS використовує різні алгоритми, такі як теорія адаптивного резонансу, самоорганізується та генетичний алгоритм.

1) система запобігання вторгнень.

IDS був здатний виявити вторгнення лише без запобіжних дій. Система виявлення вторгнень Проактивна методика, яка запобігає нападу перед входом у мережу, вивчаючи пакети та їхній малюнок та нехтуючи їх. IPS є активним та розумним та системою, яка забезпечує раннє виявлення атаки. IPS працює на 2, 3, 4 і 7 шарі OSI. IPS має функціональну функцію раннього виявлення, проактивну техніку, раннє запобігання нападу, коли напад ідентифікований, то блокує дані, що порушують.

2) Система виявлення та запобігання вторгнень:

Брандмауер не забезпечує захист від мережевих атак на відкриті порти, необхідні для мережевих служб (тобто атака відмови в обслуговуванні). Таким чином, IDPS можна використовувати для захисту мережевих служб за допомогою брандмауера. В основному є три частини в IDPS 1) попередня обробка 2) класифікація 3) захист. При попередній обробці частини sniffer пакету використовується захоплення інформації з пакетів. Тоді попередньо оброблені дані класифікуються в основному на два типи атакуючих пакетів і на звичайний пакет . Ця інформація передається захисній частині, яка вживає відповідних заходів відповідно до типу пакету для запобігання.

4.3 Класифікація на основі принципів поширення

1. Один хост.

При одиночному розгортанні системи виявлення вторгнень в мережу система встановлюється на одному хості в мережі, який може бути маршрутом r, сервером або мережевим комутатором. Весь трафік надходить і виходить з мережі через той вузол, де він перевіряється на атаки та нормальні пакети NIDS. Прикладами одиночних систем виявлення вторгнень в хост є GrIDS , Bro та NetRanger .

Плюси:

1. Окремі NIDS можуть контролювати широку підмережу

2. Вплив на систему дуже малий, це пасивний пристрій, який просто слухає

Мінуси:

1. Важко обробити всі пакети в зайнятій мережі.

2. Кілька хостів (розподілені агенти).

При розподіленому розгортанні NIDS система встановлюється на всіх (або їх може бути мало) вузлів у мережі, можна назвати агентами NIDS. Потім ці агенти контролюють трафік, який направляється через цей конкретний вузол, і генерують відповідні результати. Потім ці результати надсилаються до центрального контролера NIDS (системи управління NIDS). Ця система управління NIDS координується з агентами та генерує тривогу для відповідних пакетів та передає її по мережі. Прикладами декількох систем виявлення вторгнень в хост є AAFID та Micael .

Плюси:

1. Вирішена проблема обробки всіх пакетів поодинокими NIDS, які були присутніми в єдиному вузлі NIDS.

Мінуси:

1. Це важче керувати, і його потрібно налаштувати для кожного різного хоста.

2. Важко координувати між агентами СНІДу.

4.4 Класифікація на основі механізмів виявлення

1. На основі підпису.

У механізмі виявлення підписів шаблони атак зберігаються в базі даних. Кожен з пакетів мережевого трафіку порівнюється з моделями атаки для виявлення ненормальної поведінки. Система виявлення вторгнень на основі

підпису виявляє лише відомі атаки. Приклади Suricata - це система виявлення вторгнень на основі підпису .

Плюси:

1. Якщо ознаки нападів чітко визначені, то він має низький хибний позитив.

2. Простота у використанні.

Мінуси:

1. Вимагає специфічних знань щодо вторгнення та збирання даних до того, як вторгнення може бути застарілим.

2. Важко виявити невідомі напади.

3. Піднімає сповіщення незалежно від результату. Наприклад, якщо черв'як Windows намагається атакувати систему Linux, тоді IDS надсилає багато попереджень про невдалу атаку.

4. Знання атак залежать від конкретного середовища.

2. Система виявлення вторгнень на основі аномалії.

Система виявлення вторгнень на основі аномалії базується на поведінці мережі. Мережа поведінки або визначається адміністратором, або вивчається набором даних під час навчального етапу розробки IDS. Правила визначені для нормальної поведінки та ненормальної поведінки. Наприклад, Snort і Bro-IDS - це система виявлення вторгнень на основі аномалії .

Плюси:

1. Він має можливість виявляти невідомі напади.

Мінуси:

1. Визначити набір правил для виявлення вторгнень важко.

2. Ефективність системи залежить від придатності правил та її тестування на наборах даних тестування.

4.5 Класифікація на основі механізмів виявлення з нейронними мережами

1. На основі правил.

Система виявлення вторгнень на основі правил виявляє аномальну поведінку, порівнюючи особливості пакетів з деякими заздалегідь визначеними правилами, які визначені адміністратором або створені за допомогою певного алгоритму шляхом навчання. Системи, засновані на правилах, використовують високочастотні попередньо визначені підписи для виявлення відомих атак.

Плюси :

1. Він має дуже високий показник виявлення відомих атак.

Мінуси :

1. Вибір особливостей для ідентифікації кожної атаки утруднений.

2. Щоб система виявлення вторгнень мала високу швидкість виявлення, правила повинні бути ретельно визначені.

2. Штучний інтелект / нейронна мережа / Генетичний алгоритм на основі виявлення вторгнень Система виявлення вторгнень на основі штучного інтелекту відрізняється від усіх алгоритмів тим, що штучний інтелект використовується для визначення нового набору правил виявлення атак. Нейронні мережі - це найпоширеніший тип штучного інтелекту для виявлення вторгнень. Нейронна мережа - це набір комірок, який має зважене з'єднання з іншими клітинами. Під час тренування ваги з'єднань змінюються і вихід порівнюється з потрібним. Ітерації проводяться до тих пір, поки бажана точність не буде отримана для набору даних тесту. У генетичному алгоритмі визначені правила . Кожне правило складається з особливостей, які дозволяють чітко визначити клас атаки. Ці правила перевіряються, і після кожної ітерації правила з більш високим коефіцієнтом придатності вибираються та змінюються для створення нових правил, поки бажаний показник виявлення не буде досягнутий.

Плюси:

1. Швидкість виявлення невідомих атак збільшується за допомогою комбінації генетичного алгоритму з системою виявлення вторгнень на основі підпису .

Мінуси:

1. Ретельний вибір функцій для визначення правил потребує знань у цій галузі.

2. Швидкість виявлення залежить від підготовки даних і введених правил.

Контрольоване навчання застосовується, коли доступний набір навчальних даних. Набір навчальних даних складається з вхідних значень, які підключені до конкретного виводу. У навчанні супервидання навчальні дані використовуються для вивчення схеми атаки. Вихідні значення використовуються для обчислення коефіцієнта придатності правил.

Система вчиться представляти схему введення, щоб знайти статистичну структуру на цьому вході. Входи, що мають подібні функції, поділяються на кластери. Середнє значення обчислюється для кожного кластеру. При додаванні нового вводу в кластер середнє значення перераховується. Ці кластери використовуються для визначення невідомих моделей атаки.

4.6 Класифікація на основі способу виявлення

1. В режимі реального часу.

Системи виявлення вторгнень в режимі реального часу працюють в Інтернеті, тобто ці системи виявлення вторгнень захоплюють пакети з мережі (наживо) для виявлення ненормальних дій. Ефективність систем виявлення вторгнень в режимі реального часу значно залежить від кількості вибраних функцій, оскільки вона має дуже високою швидкістю порівнювати ці функції з

особливостями вхідних пакетів. Кількість функцій також впливає на споживання ресурсів системи реального часу.

Плюси:

1. Реальні системи мене виявляють ненормальну поведінку, поки це відбувається, що бажано від системи виявлення вторгнень.

Мінуси:

1. Системи в режимі реального часу вимагають більше ресурсів.

2. Системи в режимі реального часу можуть стати вузьким місцем.

2. Офлайн.

Автономні системи виявлення вторгнень працюють в автономному режимі, тобто ці системи виявлення вторгнень обробляють збережені набори даних про атаку, такі як набір даних KDD cup 99. Автономні системи виявлення вторгнень надають інформацію про атаку та допомагають відновити шкоду, заподіяну атакою. Ці системи виявлення допомагають зрозуміти механізм атаки та зменшують можливості майбутніх атак одного типу.

У даній роботі представлені різні класифікації системи виявлення вторгнень. Продуктивність будь-якої системи виявлення вторгнень залежить від особливостей пакету, обраного для виявлення атаки. У кожній категорії є плюси і мінуси, але поєднання різних категорій, доповнених відповідними функціями пакету, допомагає створити хорошу систему виявлення вторгнень.

5 ОБҐРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ

Метою цього розділу дипломної роботи є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності від розробки, а також прийняття рішення щодо подальшого розвитку і впровадження або ж недоцільність впровадження відповідної розробки.

Для реалізації методики, описаної в дипломній роботі можна створиит спеціальне програмне забезпечення, яке б виконувало аналіз VPN на предмет безпеки.

Для здійснення оцінки потрібно зробити розрахунки трудомісткості кожної операції.

5.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

Витрати часу по окремих операціях технологічного процесу відображені в таблиці 5.1.

Таблиця 5.1 – Операції технологічного процесу та час їх виконання

№	Назва операції (стадії)	Викона-вець	Середній час виконання операції, год.
1.	Витрати праці на підготовку опису задачі	інженер	7
2.	Витрати праці на розробку проекту	інженер	20
3.	Витрати праці на розробку структури системи	інженер	12
5.	Витрати праці на створення системи по вибраному проекту та структурі	інженер	79
5.	Витрати праці на підготовку документації	інженер	16
6.	Витрати праці на відлагодження роботи зпроектованої системи при комплексній відладці	інженер	48
Разом			186

Загальні затрати на дипломний проект становить 169 годин.

5.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Відповідно до Закону України “Про оплату праці” заробітна плата – це “винагорода, обчислена, як правило, у грошовому виразі, яку власник або уповноважений ним орган виплачує працівникові за виконану ним роботу”.

Розмір заробітної плати залежить від складності та умов виконуваної роботи, професійно-ділових якостей працівника, результатів його праці та господарської діяльності підприємства. Заробітна плата складається з основної та додаткової оплати праці.

Основна заробітна плата нараховується на виконану роботу за тарифними ставками, відрядними розцінками чи посадовими окладами і не залежить від результатів господарської діяльності підприємства.

Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов’язані з виплатами за фактично відпрацьований час. Нараховують додаткову заробітну плату залежно від досягнутих і запланованих показників, умов виробництва, кваліфікації виконавців. Джерелом додаткової оплати праці є фонд матеріального стимулювання, який створюється за рахунок прибутку.

При розрахунку заробітної плати кількість робочих днів у місяці слід в середньому приймати – 24,5 дні/міс., або ж 196 год./міс. (тривалість робочого дня – 8 год.).

Місячний оклад кожного працівника слід враховувати згідно існуючих на даний час тарифних окладів. Згідно закону України «Про Державний бюджет України на 2018 рік», зокрема Статтею восьмою мінімальна заробітна плата у погодинному розмірі встановлена у розмірі 22,41 грн. Рекомендовані тарифні ставки: керівник дипломної роботи – 30,00...50,00 грн./год., інженер – 22,41...30,00

грн./год., консультант – 22,41...30,00 грн./год., технік – 22,41...30,00 грн./год., лаборант – 22,41...25,00 грн./год.

Основна заробітна плата розраховується за формулою:

$$З_{осн.} = Т_с \cdot К_г \,, \qquad (5.1)$$

де $Т_с$ – тарифна ставка, грн.;

$К_г$ – кількість відпрацьованих годин.

Оскільки всі види робіт в даному проекті виконує інженер, то основна заробітна плата буде розраховуватись тільки за однією формулою

$$З_{осн.} = 30 \cdot 186 = 5070 \text{ грн.}$$

Додаткова заробітна плата становить 10–15 % від суми основної заробітної плати.

$$З_{дод.} = З_{осн.} \cdot К_{допл.}, \qquad (5.2)$$

де $К_{допл.}$ – коефіцієнт додаткових виплат працівникам, 0,1–0,15 (візьмемо його рівним 0,15).

$$З_{дод.} = 5070 \cdot 0,15 = 760,50 \text{ грн.}$$

Звідси загальні витрати на оплату праці ($В_{о.п.}$) визначаються за формулою:

$$В_{о.п.} = З_{осн.} + З_{дод.}. \qquad (5.3)$$

$В_{о.п.}$=5070+760,50 = 5830,50 грн.

Крім того, слід визначити відрахування на соціальні заходи:

1) ЄСВ + ПДФО 22 %;

2) військовий збір – 1,5 %.

У сумі зазначені відрахування становлять 23,5 %.

Отже, сума відрахувань на соціальні заходи буде становити:

$$B_{с.з.} = Ф_{оп} \cdot 0{,}235, \qquad (5.4)$$

де $Ф_{ОП}$ – фонд оплати праці, грн.

$$B_{с.з.} = 5830{,}5 \cdot 0{,}235 = 1370{,}05 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 5.2.

Таблиця 5.2 – Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівник-ків	Основна заробітна плата, грн.			Додаткова заробітна плата, грн.	Нарахув. на ФОП, грн.	Всього витрати на оплату праці, грн. *6=3+4+5*
		Тарифна ставка, грн.	К-сть відпра-цьов. год.	Фактично нарах. з/пл., грн.			
А	Б	1	2	3	4	5	6
1	інженер	30	169	5070	760,5	1370,05	7200,55

Загальні витрати на оплату праці становить 7200,55 грн.

5.3 Розрахунок матеріальних витрат

Матеріальні витрати визначаються як добуток кількості витрачених матеріалів та їх ціни:

$$M_{в\,i} = q_i \cdot p_i, \qquad (5.5)$$

де: q_i – кількість витраченого матеріалу *i*-го виду;

p_i – ціна матеріалу *i*-го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} = \sum M_{в\,i}. \qquad (5.6)$$

Проведені розрахунки занесемо у таблицю 5.3.

Таблиця 5.3 – Зведені розрахунки матеріальних витрат

Найменування матеріальних ресурсів	Одиниця виміру	Норма витрат	Ціна за одиницю, грн	Затрати матеріалів, грн	Транс-портно-заготівель-ні витрати, грн	Загальна сума витрат на матеріа-ли, грн
1. Основні матеріали						
Програмне забезпечення	комп.	1	23156	23156	–	23120
2. Допоміжні матеріали						
Папір формату А4	шт.	200	0,18	36	–	36
Разом:						23156

Загальні матеріальні затрати становлять 23156 гривень.

5.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1-ці обладнання визначаються за формулою:

$$З_е = W \cdot T \cdot S, \qquad (5.7)$$

де W – необхідна потужність, кВт;

Т – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Вартість кіловат-години електроенергії слід приймати згідно існуючих на даний час тарифів. Отже, 1 кВт з ПДВ коштує 2,42 грн.

Потужність комп'ютера для створення проекту – 550 Вт, кількість годин роботи обладнання згідно таблиці 5.1 – 169 годин.

Тоді, $З_е = 0{,}55 \cdot 169 \cdot 2{,}42 = 224{,}94$ грн.

5.5 Розрахунок суми амортизаційних відрахувань

Характерною особливістю застосування основних фондів у процесі виробництва є їх відновлення. Для відновлення засобів праці у натуральному виразі необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації.

Амортизація – це процес перенесення вартості основних фондів на вартість новоствореної продукції з метою їх повного відновлення.

Комп'ютери та оргтехніка належать до четвертої групи основних фондів. Для цієї групи річна норма амортизації дорівнює 60 % (квартальна – 15 %).

Для визначення амортизаційних відрахувань застосовуємо формулу:

$$А = \frac{Б_В \cdot Н_А}{100\%}, \qquad (5.8)$$

де $А$ – амортизаційні відрахування за звітний період, грн.;

$Б_В$ – балансова вартість групи основних фондів на початок звітного періоду, грн.;

$Н_А$ – норма амортизації, %.

Для даного проекту засобом розробки є комп'ютер. Його сума становить 7335 грн. Отже, амортизаційні відрахування будуть рівні:

$$A = \frac{7335 \cdot 5\%}{100\%} = 366{,}75 \text{грн.}$$

Оскільки робота виконувалась 169 годин, то амортизаційні відрахування будуть становити:

$$A = \frac{366{,}75 \cdot 169}{150} = 413{,}21 \text{грн.}$$

5.6 Обчислення накладних витрат

Накладні витрати пов’язані з обслуговуванням виробництва, утриманням апарату управління спілкою та створення необхідних умов праці.

В залежності від організаційно-правової форми діяльності господарюючого суб’єкта, накладні витрати можуть становити 20 – 60 % від суми основної та додаткової заробітної плати працівників.

$$H_в = B_{о.п.} \cdot 0{,}2 \ldots 0{,}6 \,, \qquad (5.9)$$

де H_B – накладні витрати.

Отже, накладні витрати:

H_B = 5830,5· 0,2 = 1166,10 грн.

5.7 Складання кошторису витрат та визначення собівартості НДР

Результати проведених вище розрахунків зведемо у таблицю 5.4.

Таблиця 5.4 – Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
Витрати на оплату праці (основну і додаткову заробітну плату)	5830,5	19%
Відрахування на соціальні заходи	370,05	1%
Матеріальні витрати	23156	74%
Витрати на електроенергію	224,94	1%
Амортизаційні відрахування	413,21	1%
Накладні витрати	1166,1	4%
Собівартість	31160,8	100%

Собівартість (C_B) проекту розрахуємо за формулою:

$$C_в = B_{о.п.} + B_{с.з.} + З_{м.в.} + З_в + А + Н_в. \quad (5.10)$$

Отже, собівартість проекту дорівнює:

$C_в$ = 5830,50 + 370,05 + 23156 + 224,94 + 413,21 + 1166,10 = 31160,80 грн.

5.8 Розрахунок ціни проекту

Ціну НДР можна визначити за формулою:

$$Ц = \frac{C_B \cdot (1 + P_{рен}) + К \cdot B_{н.і.}}{К} \cdot (1 + ПДВ), \quad (5.11)$$

де $P_{рен.}$ – рівень рентабельності, 30 %;

$К$ – кількість замовлень, од. (встановлюється лише при розробці програмного продукту та мікропроцесорних систем);

$B_{н.і.}$ – вартість носія інформації, грн. (встановлюється лише при розробці програмного продукту);

$ПДВ$ – ставка податку на додану вартість, (20 %).

Оскільки розробка є прикладною, і використовуватиметься тільки для одного підприємства, то для розрахунку ціни не потрібно вказувати коефіцієнти K та $B_{i.н}$, оскільки їх в даному випадку не потрібно.

Тоді, формула для обчислення ціни розробки буде мати вигляд:

$$Ц = C_B \cdot (1 + P_{рен}) \cdot (1 + ПДВ). \quad (5.12)$$

Звідси ціна на проект складе:

Ц = с · (1+0,3)(1+0,2) = 51177,61 грн.

5.9 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці на підприємстві за певний проміжок часу.

Економічна ефективність (E_p) полягає у відношенні результату виробництва до затрачених ресурсів:

$$E_p = П / C_B, \quad (5.13)$$

де $П$ – прибуток;

C_B – собівартість.

Плановий прибуток ($П_{пл}$) знаходимо за формулою:

$$П_{пл} = Ц - C_B. \quad (5.14)$$

Розраховуємо плановий прибуток:

$П_{пл}$ = 51177,61 – 31160,80 = 18371,45 грн.

Отже, формула для визначення економічної ефективності набуде вигляду:

$$E_р = \frac{П_{пл}}{Св} . \quad (5.15)$$

Тоді, $E_р$ = 18371,45 / 31160,80 = 0,56

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень ($T_р$):

$$T_р = 1/ E_р , \quad (5.16)$$

Термін окупності дорівнює:

$T_р$ = 1/0,56 = 1,8 роки.

В цьому розділі дипломної роботи було розраховано основні техніко-економічні показники проекту (див. таблицю 5.5).

Розраховане значення економічної ефективності становить 0,56 що є високим значенням.

Так само нормальним є термін окупності. Для даного продукту він становить 1,8 роки.

Таблиця 5.5 – Техніко-економічні показники НДР

№ п/п	Показник	Значення
1.	Собівартість, грн.	31160,80
2.	Плановий прибуток, грн.	18371,45
3.	Ціна, грн.	51177,61
4.	Економічна ефективність	0,56
5.	Термін окупності, рік	1,8

Отже, даний проект може бути впроваджений та мати подальший розвиток, оскільки він є економічно вигідним за всіма основними техніко-економічними показниками.

6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

6.1 Охорона праці

Нормативно-правові акти з охорони праці – це правила, норми, регламенти, положення, стандарти, інструкції та інші документи з охорони праці. Вони є обов'язковими до виконання і дотримання усіма підприємствами, для яких вони розроблені [18].

Опрацювання та прийняття нових, перегляд і скасування чинних нормативно-правових актів з охорони праці проводяться спеціально уповноваженим центральним органом виконавчої влади з нагляду за охороною праці за участю професійних спілок і Фонду соціального страхування від нещасних випадків та за погодженням з органами державного нагляду за охороною праці, а санітарні правила та норми затверджуються спеціально уповноваженим центральним органом виконавчої влади в галузі охорони здоров'я.

Нормативно-правові акти з охорони праці розглядаються в міру впровадження досягнень науки і техніки, але не рідше одного разу на десять років. Розгляд та впровадження їх має за мету поліпшення безпеки, гігієни праці та виробничого середовища.

У разі неможливості повного усунення небезпечних і шкідливих для здоров'я умов праці роботодавець зобов'язаний повідомити про це відповідний орган державного нагляду за охороною праці, а також звернутись до нього при необхідності з клопотанням про встановлення строку для проведення умов праці згідно нормативних вимог.

Вимоги щодо охорони праці регламентуються також Державними стандартами України з питань безпеки праці, Будівельними нормами та правилами, Санітарними нормами, Правилами улаштування електроустановок, нормами технічного проектування та іншими нормативними актами.

Крім державних нормативних актів з охорони праці існують і нормативні акти, що діють на окремих об’єктах. Власники підприємств, установ, організацій або уповноважені ними органи розробляють на основі Державних нормативних актів з охорони праці (ДНАОП) і затверджують власні положення, інструкції або інші нормативні акти з охорони праці, що діють в межах підприємства, установи, організації. До таких актів належать:

– Положення про систему управління охороною праці на підприємстві.

– Положення про службу охорони праці на підприємстві.

– Положення про комісію з питань охорони праці на підприємстві.

– Положення про роботу уповноважених трудового колективу.

– Положення про навчання, інструктаж і перевірку знань працівників з питань охорони праці.

– Положення про організацію і проведення первинного і повторного інструктажу, а також пожежно-технічного мінімуму.

– Положення про організацію попереднього і періодичного медичних оглядів працівників.

– Положення про санітарну лабораторію на підприємстві.

– Інструкції з охорони праці для працюючих за професіями і видами робіт.

– Інструкції про заходи пожежної безпеки.

– Інструкції про порядок проведення зварювальних та інших вогневих робіт на підприємстві.

– Перелік робіт з підвищеною небезпекою.

– Перелік посад посадових осіб підприємства, які зобов’язані проходити попередню і періодичну перевірку знань з охорони праці.

– Наказ про порядок забезпечення працівників підприємства спецодягом, спецвзуттям та іншими засобами індивідуального захисту.

Основними нормативними документами, що регламентують виконання трудової діяльності з використання ЕОМ є:

- ДСанПІН 3.3.2.007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин»;
- *НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями»;*
- ДСН 3.3.6.037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку»;
- ДБН В.2.5-28:2018 «Природне і штучне освітлення»;
- «Порядок проведення медичних оглядів працівників певних категорій», затвердженого наказом Міністерства охорони здоров'я України від 21 травня 2007 року № 246 та ін.

При експлуатації ЕОМ необхідно дотримуватись таких правил та вимог:

– ЕОМ, периферійні пристрої ЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ, інше устаткування (апарати управління, контрольно-вимірювальні прилади, світильники тощо), електропроводи та кабелі за виконанням та ступенем захисту мають відповідати класу зони за ПВЕ, мати апаратуру захисту від струму короткого замикання та інших аварійних режимів;

– під час монтажу та експлуатації мережі необхідно повністю унеможливити виникнення електричного джерела загоряння внаслідок короткого замикання та перевантаження проводів, обмежувати застосування проводів з легкозаймистою ізоляцією і, за можливості, перейти на негорючу ізоляцію;

– лінія мережі і живлення ЕОМ, периферійних пристроїв ЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ виконується як окрема групова трипровідна мережа, шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів.

Оскільки, у приміщенні одночасно експлуатується більше п'яти персональних ЕОМ, на помітному та доступному місці встановлено аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення.

Відеотермінали, ЕОМ, спеціальні периферійні пристрої ЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ повинні відповідати вимогам чинних в Україні стандартів, нормативних актів з охорони праці.

За способом захисту людини від ураження електричним струмом відеотермінали, ЕОМ, периферійні пристрої ЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ мають відповідати I класу захисту. Для захисту від ураження електричним струмом при експлуатації комп’ютерів використовується захисне заземлення. Є неприпустимим використання клем функціонального заземлення для підключення захисного заземлення.

Площа, виділена для одного робочого місця з відеотерміналом або персональною ЕОМ, складає не менше 6 $м^2$, а обсяг - не менше 20 $м^3$.

Робочі місця з відеотерміналами відносно світлових прорізів розміщуються так, щоб природне світло падало збоку, переважно зліва.

При розміщенні робочих місць з відеотерміналами та персональними ЕОМ необхідно дотримуватись таких вимог:

– робочі місця з відеотерміналами та персональними ПЕОМ розміщуються на відстані не менше 1 м від стін зі світловими прорізами;

– відстань між бічними поверхнями відеотерміналів має бути не меншою за 1,2 м;

– відстань між тильною поверхнею одного відеотермінала та екраном іншого не повинна бути меншою 2,5 м;

– прохід між рядами робочих місць має бути не меншим 1 м.

Таким чином, дотримання всіх норм та вимог, дозволить забезпечити безпечні умови з точки зору охорони праці.

6.2 Кольорове оформлення виробничих приміщень як фактор підвищення продуктивності праці

Встановлено, що кольори діють на людину по-різному: одні кольори заспокоюють, а інші – збуджують.

Червоний колір стимулює нервові центри та енергетичні процеси в печінці і м'язах, підвищує увагу людини та її самозахист. Але при довго

тривалій дії цей колір викликає відчуття втоми і тахікардію. Червоний колір негативно впливає на людину у разі наявності гіпертонії, запальних процесів, особливо негативно він діє на яскраво-рудих людей.

Оранжевий колір сприймається людьми як теплий, він зігріває, бадьорить, стимулює до активної діяльності.

Жовтий колір активує рухомі центри, генерує енергію м'язів, надає хороший настрій, стимулює діяльність печінки, нирок, шлунково-кишкового тракту. Протипоказаний жовтий колір при лихоманках, надмірному збудженні, ейфорії, зорових галюцинаціях.

Зелений колір – колір спокою, свіжості (прохолоди), знімає спазми кровоносних судин і знижує тиск крові, а в поєднанні з жовтим кольором позитивно впливає на настрій людини.

Синій і блакитний кольори – свіжі та прозорі, здаються легкими, знімають фізичну напругу, тахікардію, регулюють ритм дихання, володіють протимікробною дією. Але при довготривалій дії ці кольори можуть викликати втому і депресію.

Чорний колір – похмурий і тяжкий, різко знижує настрій, працездатність, викликає розпорошування уваги.

Білий колір – холодний, одноманітний, здатний викликати апатію.

Різностороння дія кольорів на фізіологічні процеси та емоційну сферу людини дозволяє широко використовувати їх з гігієнічною метою. При оформленні інтер’єру виробничих приміщень колір використовують як композиційний засіб, що забезпечує гармонійну єдність приміщення і технологічного устаткування, як фактор оптимізації умов праці, як засіб інформації і сигналізації, для забезпечення безпеки праці.

Підтримка раціональної кольорової гами у виробничих приміщеннях досягається правильним добором світильників, які забезпечують необхідний світловий спектр.

6.3 Концепція безпеки життєдіяльності

Загальна структура концепцій безпеки життєдіяльності людини зображена на рисунку 6.1

Розвиток науки і практики "Безпеки життєдіяльності" передбачає:

- визначення пріоритетів у встановленні безпеки життєдіяльності;
- розробку теоретичних основ науки;
- формування довгострокової єдиної державної політики у сфері забезпечення безпеки, освіти та ін.;
- побудову глибоко пророблено "правового поля" і нормативно-законодавчої бази у сфері безпеки життєдіяльності;
- формування науково-методичного та інформаційного забезпечення;
- забезпечення науковими й управлінськими кадрами за визначеним рівнем професіоналізму та компетенції;
- участь у міжнародному співробітництві.

Визначення пріоритетів розвитку у безпеці життєдіяльності пов'язано із суспільним розвитком країни і складається із:

- формування передумов для забезпечення здоров'я нації шляхом соціально-економічного розвитку держави;

− визначення безумовності головної ролі питань щодо встановлення безпеки людини у процесі її життєдіяльності;

− регіональних і локальних завдань у сфері безпеки, які мають бути підпорядковані глобальним і національним цілям;

− запобігання кризам у життєдіяльності з одночасною оптимізацією середовища існування людини;

− встановлення регіональної безпеки, яка вміщує функцію раннього попередження негативних тенденцій та передбачає гарантії їх мінімізації;

− уявлення про те, що цілі безпеки життєдіяльності є первинні відносно цілей економічного розвитку;

− розміщення і розвиток матеріального виробництва на певній території повинні здійснюватися відповідно до її еколого-економічної збалансованості;

− безпека життєдіяльності в суспільстві тісно пов'язана з рівнем культури, освіти і виховання людей у цьому суспільстві.

Концепція освітянської діяльності з напряму "Безпека життя і діяльності людини" укладається в рамки (для досягнення мети, що проголошує безпеку):

− співвідношення з базисною Концепцією ООН про "сталий людський розвиток";

− створення умов для збалансованого безпечного існування кожної окремої людини сучасності і наступних поколінь;

− відповідних вимог до стабільної економіки, державних кордонів, суспільних цінностей;

− стратегічного принципу розв'язання проблем БЖ завдяки реалізації управління безпекою як складової якості життя людини в умовах допустимого ризику;

− інтегрування питань БЖ у тематику навчальних традиційних дисциплін, які встановлюють вимоги безпеки в побуті, екологічної безпеки, безпеки здоров'я, ергономіки та ін.;

– посилення інтеграційних процесів дослідження проблем БЖ з дисциплінами суспільних наук;

– переходу від епізодичного до систематичного вивчення тематики БЖДЛ упродовж всього терміну навчання громадян у навчальних закладах та ін.

Зміст навчання реалізується шляхом виконання встановленої мети та завдань освіти у сфері БЖДЛ.

Мета освіти БЖДЛ – підготовка особи до активної участі в забезпеченні тривалого повноцінного життя в суспільстві, що динамічно змінюється.

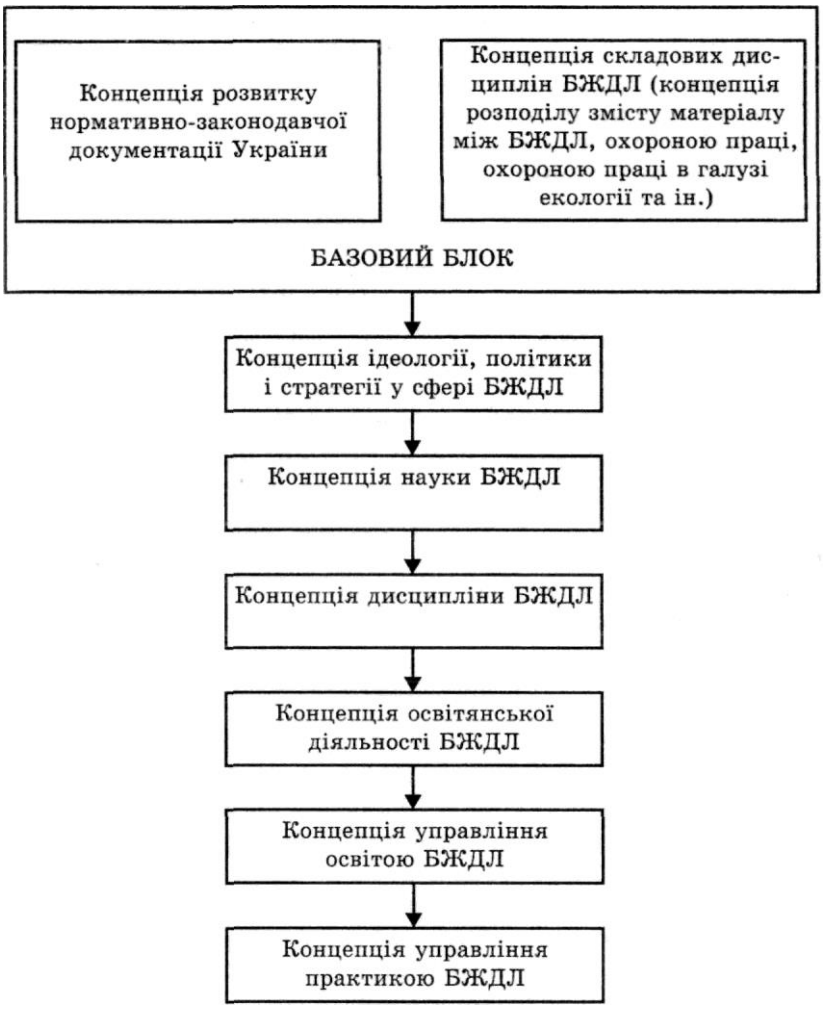

Рисунок 6.1 – Структура концептів БЖДЛ

Основні завдання освіти з БЖДЛ:

- формування культури щодо безпеки, моральних цінностей людини, її поглядів, поведінки тощо;
- забезпечення стану індивідуальної захищеності людини шляхом формування і розвитку певних (за змістом безпеки) якостей, чому сприяють необхідні знання й уміння;
- інтенсифікація методичної, наукової та інших форм освітянської діяльності;
- вдосконалення управління освітою за критеріями напряму БЖДЛ.

Пріоритетним напрямом підготовки у сфері БЖДЛ вважається формування правильної соціальної позиції особи щодо власної безпеки, мотивація безпечної поведінки в побуті, виробництві, в інших сферах існування, засвоєння нових знань і вмінь.

Навчання із БЖДЛ організовується на всіх ланках освіти, що зазначені в ст. 29 Закону України "Про освіту". Пріоритетом у роботі є розробка і впровадження елементів державних стандартів освіти в кожен освітній і освітньо-кваліфікаційний рівень громадян, незалежно від форми освіти.

7 ЕКОЛОГІЯ

7.1 Отримання енергії за рахунок альтернативних джерел

Енергетичний баланс в Україні поступово переміщується. Але головну роль у ньому досі грають викопні джерела енергії з дорогими і «брудними» технологіями.

«Брудні» технології вперто лідирують, але це тимчасово.

Головну роль в енергетичному балансі продовжують грати викопні джерела енергії з дорогими і «брудними» технологіями. Хоча сам енергетичний баланс поступово переміщується у бік альтернатив.

Україна отримує електричну енергію спалюючи традиційні види палива – вугілля й газ. За прогнозами на 2017 рік, із запланованого до виробництва обсягів електроенергії майже 41% складуть вугільно-газові ТЕС і ТЕЦ. Атомні електростанції вироблятимуть 53% енергії.

Наша країна залишається реліктом радянської енергетичної системи. Поки що атомна енергія та енергетика на вугіллі й газі дозволяє працювати економічному і невиробничому секторам України. Але динаміка змін говорить про нові тенденції: зростає виробництво атомної, відновлюваної енергії та альтернативних джерел енергії.

Старі енерготехнології – дорогі й невигідні в експлуатації та отриманні інвестицій

Теплові станції балансують на межі спаду/утримання рівня виробництва. Так, уведення в експлуатацію нового енергоблока АЕС коштує €7 млн. Для того, щоб «погасити» цей же енергоблок, потрібно витратити близько €1,3 млн. Витрачають гроші й на підтримку безпеки експлуатації такої станції.

Вугільна енергетика ще дорожча та шкідливіша. Вугільний пил глибоко проникає в тіло людини і шкодить його здоров’ю. А аварійність вугільних шахт

дуже висока: тільки в 2014 році понад двох тисяч гірників отримали травми при роботі в забої, а 100 з них загинуло.

З економічної точки зору, теплові вугільні станції малорентабельні – на електроенергію перетворюється лише 33% енергії, яку отримують від спалювання вугілля. Трохи вищий показник мають газогенераторні станції.

Вугільні станції отримують вугілля для отримання тепла та електроенергії від експортних поставок або із зони АТО. Це нестабільні й ризиковані канали постачання сировини. Економіка країни програє від фінансування зарубіжних постачальників або від спроб налагодити постачання через зону бойових дій.

Газові труби наповнюються вуглеводами Росії, яка, хоча й отримала негативний результат у Стокгольмському арбітражі, продовжує тяжби і тиск на ЄС та Україну для збереження монопольного контролю ринку газу.

Тому щораз більше підприємців створюють для себе енергетичну незалежність і прагнуть отримати прибуток від малої генерації. Законодавство й нові технології доступні в Україні, а сектор відновлюваної енергетики зростає настільки стрімко, що випереджає класичні схеми отримання електроенергії.

До 2040 року відновлювані джерела енергії складуть 3/4 світових інвестицій в електроенергію

Обсяг альтернативної енергії може в 2,5 рази перевищувати обсяги сьогоднішньої енергогенерації. Це висновки експертів, які провели аналіз потенційних можливостей доступних сьогодні «чистих» енергетичних технологій.

Київський інститут відновлюваної енергетики оцінює технічний потенціал альтернативних джерел енергії у 81 мільйон еквівалентних тонн. Значний відсоток має в цьому виробництві енергії біомаса та геотермальна енергія – 30%.

Але від теоретичних розробок Україна перейшла до практичної реалізації бізнес-проектів. Динаміка зростання в альтернативній енергетиці значна: встановлена потужність енергоустановок на відновлюваних джерелах з 2009 року

в Україні зросла вдесятеро. У березні 2017 року було вироблено «зеленої» енергії за потужністю рівної одному блоку атомної станції.

В Україні стає чимраз більше електроустановок, і відповідно – енергії, яку вони виробляють

Ще в 2014 році частка альтернативних джерел становила майже 1%. При цьому Крим, де зосереджено чимало потенціалу і діючих альтернативних джерел, сьогодні не входить до статистики українського енергоринку.

Реалії нашого ринку енергетики перегукуються із загальносвітовою тенденцією альтернативної енергетики, яка динамічно зростає та розвивається, а класична знижує виробництво та отримує дедалі менше інвестицій.

Із 70-х років ціна виробництва сонячної енергії впала у 150 разів. А з 2000-х обсяг виробництва сонячної енергії збільшився у 7 разів, вітроенергетика зросла в чотири рази. До 2040 року відновлювані джерела енергії складуть ¾ інвестицій з $10,2 трлн, які вкладають у нові технології виробництва електроенергії в усьому світі.

Масштаб «зелених» компаній в Україні вражає. Якщо традиційні енергетичні ресурси вимагають виділення виробництва енергії в спеціалізовану галузь навіть усередині однієї компанії, то поновлювані джерела енергії – це невеликі підрозділи всередині компаній. Вони виробляють енергію для власних потреб і для отримання прибутку за рахунок «зеленого» тарифу.

Приватні українські компанії, які спеціалізуються винятково на виробництві енергії, виробляють її і для свого споживання. Вони поширені по всій країні:

Сонячна й вітрова енергія можуть вироблятися до 90 ТВт у рік. Геотермальна енергетика привабливішим для інвесторів в Закарпатті, де є природні можливості для її розвитку.

Лідери української альтернативної енергетики – компанії України і Китаю. В українській відновлюваній енергетиці є свої лідери. Найбільший виробник енергії вітру – це «Вінд Пауер», дочірня компанія ДТЕК.

На другому місці у вітроенергетиці України – «Вітряний парк Новоазовський». Цей комплекс – енергетична демонстрація можливостей унікального для України та більшості країн Східної Європи краматорського підприємства «Фурлендер Віндтехнолоджі». Там виробляють вітроенергетичні установки мультимегаватної потужності й аналогів йому немає на пострадянському просторі.

Замикає трійку вітроенергетики України «Вітряний парк Очаківський». Компанія «Вітряні парки України» управляє цими енергетичними компаніями, які можуть проводити разом з іншими енергетичними вітровими об'єктами 215,5 МВт електроенергії.

Серед виробників і постачальників вітрової енергії за «зеленим» тарифом зареєстровано всього 11 компаній. Виробників сонячної енергії значно більше – це 85 зареєстрованих постачальників сонячної енергії в наземному варіанті і ще десятки великих панельних станцій на поверхнях будівель.

Найбільша компанія на ринку сонячної енергетики в Україні – «Восход Солар» із заявленою потужністю 53,3 МВт. Це підрозділ китайської компанії CNBM New Energy Engineering, яке володіє близько 60% «сонячного» енергоринку України потужністю до 267 МВт.

Але, крім таких великих постачальників, є невеликі компанії, які виробляють сонячну енергію по всій Україні, зокрема у Хмельницькій, Вінницькій, Одеській, Кіровоградській, Львівській, Волинській, Дніпропетровській та інших областях.

Україна залишається привабливою для мікро-, міні – та малої гідроенергетики. У цій галузі лідирують два бізнес-проекти: Гідроенергоінвест, який володіє 12 ГЕС, зокрема сімома станціями в Кіровоградській області та кількома електростанціями в Сумській, Вінницькій, Полтавській, Житомирській областях. Найпотужніша з них – Гайворонська ГЕС потужністю 5,7 МВт.

Ще одна компанія – «Енергія – 1» володіє Касперівської ГЕС на Тернопільщині з потужністю 5,1 МВт. На третьому місці – Червонооскільська ГЕС, яка працює в Харківській області та виробляє 4 МВт.

Ривок у цих напрямках виводить Україну на рівень тих країн, які поступово позбавляються нафтогазової залежності. Зараз у Казахстані проходить масштабна міжнародна виставка Expo 2017, де Україна представляє свої досягнення в розробці технологій по видобутку енергії вітру та сонця.

7.2 Індексний метод в екології

Статистична практика при вивченні екологічних явищ широко використовує індекси (хоча деякі екологи не підготовлені для такої роботи). Знання методології побудови індексів значно розширює аналітичні можливості дослідника, збагачує результативну інформацію досліджень.

Індекс англійський термін «index number» означає число-показник. Статистичні індекси – це відносні величини, які одержують внаслідок порівняння складних екологічних явищ, утворених з різнорідних елементів, що не підлягають безпосередньому підсумовуванню.

Індекс у статистиці узагальнюючий відносний показник, який характеризує співвідношення в часі чи просторі соціально-екологічних явищ і процесів. За своєю суттю статистичний індекс характеризує зміну рівня будь-якого суспільного явища в часі, просторі чи порівняно з планом, нормою, стандартом. У цих випадках зіставляються між собою числові значення однойменних показників, що мають однаковий екологічний зміст. Отже, індексом можна назвати відносну величину динаміки, виконання плану, порівняння.

За допомогою індексів можна характеризувати зміну в часі і просторі найрізноманітніших показників: обсяги викидів в атмосферу, скидів шкідливих речовин у водне середовище, інтенсивність забруднень і т. д. їх поділяють на дві групи: до першої належать об'ємні (сумарні) показники (наприклад, обсяг викидів

та скидів кількість забруднювачів, площа забрудненої території та ін.), які виражаються абсолютними величинами; до другої – показники, розраховані на певну одиницю (наприклад, викиди в розрахунку на одиницю земельної площі або на одного жителя, працівника і т.д.). Останні умовно можна назвати якісними показниками, і виражаються вони у вигляді середніх величин. Ця особливість зумовлює поділ індексів на індекси кількісних та індекси якісних показників.

За допомогою статистичних індексів можна відображувати зміну в часі і просторі як окремих простих показників (наприклад, обсяг викидів вуглецю, окислів азоту, сірки і т.д.), так і однойменних показників за складними сукупностями (наприклад, зміна обсягу викидів по місту, району, області в цілому і т.д.).

За допомогою індексного методу вирішуються такі завдання:

– характеризують загальну зміну складного економічного явища чи окремих його елементів (складових);

– виділяють вплив одного з факторів через елімінування впливу інших;

– відокремлюють впливу зміни структури явища на зміну індексованої величини.

При цьому сама міра впливу може бути визначена як у відносних вимірниках, так і в абсолютних

Класифікація індексів. Класифікують індекси за різними ознаками:

– за змістом досліджуваних об'єктів, явищ і процесів індекси обсягу, індекси якісних показників;

– за повнотою охоплення елементів сукупності індивідуальні індекси, зведені (групові, загальні) індекси;

– за формою зображення агрегатні індекси, середні зважені індекси (арифметичні, гармонійні);

– за базою порівняння індекси динаміки (базові, ланцюгові), індекси виконання плану, територіальні індекси;

– за характером впливу на зміну складного явища індекси сталого складу, індекси структурних зрушень;

– за коефіцієнтами співвимірювання індекси зі змінними вагами, індекси зі сталими вагами.

Обчислення загальних індексів, що дають змогу співвіднести між собою показники за складними сукупностями, являє собою особливий прийом дослідження, який називається індексним методом. За його допомогою можна не тільки вивчати динаміку показників, а й вимірювати вплив окремих факторів на динаміку складного показника. При цьому залежно від завдань аналізу можна фактори вивчати ізольовано, абстрагуючись від дії інших, або розглядати їх взаємопов'язано.

Методологічні принципи побудови індексів. Індексний метод має свою термінологію та символіку. Її дотримання є обов'язковою умовою в індексному аналізі.

Для побудови статистичного індексу необхідно мати вихідну інформацію, як мінімум, за два періоди. Один з таких періодів називається базисним, другий – поточним. Базисний – це період, з яким порівнюють досліджувані явища, поточний – період, що порівнюється. Так, в індексах динаміки базисним є показник попереднього періоду (моменту) часу, в індексах порівняння з нормативною базою нормативний рівень, а в індексах порівняння (в просторі) базисним може бути показник, що належить до якоїсь з територій. Якщо досліджуються дані за кілька періодів, то один з них (як правило, початковий) буде базисним, а решта – поточними, або звітними.

У теорії індексів показник, зміну якого характеризує індекс, називають індексованою величиною, а пов'язану з нею величину, що використовують як постійну, – елімінованою величиною, або вагою. Остання відіграє роль сумірника. Використання цих двох видів величин вважається особливістю індексного методу аналізу. При побудові статистичних індексів насамперед необхідно вирішити такі питання:

– який набір різнорідних елементів досліджуватиметься;

– які показники виступатимуть індексованими величинами;

– які величини виступатимуть сумірниками (вагами).

При цьому встановлюють, які досліджувані показники при побудові індексів вважаються базисними, а які – поточними.

Стандартні позначення, що використовують при побудові індексів:

– підписна нумерація за її допомогою позначається період, до якого належать дані показники базисного періоду мають у формулах підрядковий знак «0», а поточного «1»; якщо зміна явища вивчається не за два, а більше періодів, то кожний з них позначається відповідно «0», «1», «2», «3» тощо.;

– основні умовні позначення показників: x рівень показника, який вивчається; x_0 рівень показника за базовий період;

– x_i рівень цього ж показника за поточний період (якісний показник);

– u статистична вага показника в ряду розподілу, або об'ємний показник;

– u_0 і u_i теж за базисний та поточний періоди;

– i індивідуальний індекс;

Числове значення індексу (i) означає, що відповідний показник за досліджуваний період змінився в (i) разів, на певну кількість відсотків.

ВИСНОВКИ

Методи кластеризації, які використовують лише звичайні мітки, часто можуть бути ефективнішими, ніж методи, засновані на класифікації. У ситуаціях, коли визначити хороший показник відстані важко, класифікація або статистичні методи можуть бути кращим вибором. Однак на успіх статистичних методів значною мірою впливає застосовність статистичних припущень у конкретних сценаріях реального життя.

Для реального часу виявлення вторгнень, складність аномалії процесу виявлення грає життєво важливу роль. У разі класифікації, кластеризації та статистичних методів, хоча навчання є дорогим, вони все ще прийнятні, оскільки тестування проходить швидко, а навчання в режимі офлайн. На відміну від таких методів, як найближчий сусід та спектральні методи, які не мають фази навчання, мають дорогу фазу тестування, яка може бути обмеженням у реальній обстановці.

Методи виявлення аномалій зазвичай передбачають, що аномалії даних є рідкісними порівняно із звичайними випадками. Взагалі такі припущення справедливі, але не завжди. Часто непідконтрольні методи страждають від великої помилкової частоти тривоги, коли аномалії знаходяться у великій кількості. Для виявлення об'ємних аномалій можуть застосовуватися методи, що працюють в режимах, що контролюються.

Нижче наведено деякі рекомендації, про які слід пам’ятати, розробляючи метод виявлення мережевої аномалії чи систему.

Більшість існуючих IDS для провідникового середовища працюють трьома способами: трафік рівня потоку або аналіз даних на рівні пакета, аналіз даних, аналіз протоколу або перевірка корисного навантаження. Кожна з цих категорій має свої переваги та обмеження. Отже, гібридизація цих (наприклад, аналіз рівня протоколу з подальшим аналізом трафіку на рівні потоку) може дати кращі показники з точки зору відомого (з високою швидкістю виявлення), а також невідомого виявлення атаки.

Мережеві аномалії можуть походити з різних джерел, про що йдеться у розділі III. Отже, кращий ІДС повинен мати можливість розпізнавати джерела аномалій перед початком процесу виявлення.

IDS, здатна ідентифікувати як відомі, так і невідомі атаки, повинна використовувати як під контролем (навчання, засноване на правилах чи підписах), так і без нагляду (кластеризація або групування) на декількох рівнях для роботи в режимі реального часу з низькою помилковою помилкою. показники тривоги.

Розробник IDS повинен вибирати основні компоненти, метод (и), методи або базу правила / підпису / профілю для подолання чотирьох важливих обмежень: суб'єктивна ефективність, обмежена масштабованість, ефективність залежно від сценарію та обмежена безпека.

Ефективність кращої ІДС повинна встановлюватися як якісно, так і кількісно.

Краща класифікація або метод ідентифікації аномалій дозволяє нам настроїти її (відповідні нормальні профілі, пороги тощо) залежно від сценарію мережі.

Хоча дослідницькою спільнотою було розроблено багато методів та систем, все ж існує низка відкритих дослідницьких питань та проблем. Відповідність показників продуктивності є загальновизнаним недоліком у виявленні вторгнень. Оцінюючи ІДС, три найважливіші якості, які потрібно виміряти, – це повнота, коректність та продуктивність. Поточний стан сучасного виявлення вторгнень обмежує оцінку нових систем тестуванням неповних наборів даних, які тестують вузько визначені компоненти системи. Деякі системи, засновані на аномалії, були протестовані за допомогою надуманих наборів даних. Така оцінка обмежена якістю набору даних, щодо якої оцінюється система. Побудова об'єктивного набору даних, що є об'єктивним, реалістичним та всеосяжним, є надзвичайно складним завданням.

Офіційне підтвердження правильності в області виявлення вторгнень є винятково складним і дорогим. Тому "досить хороша впевненість" представляє спосіб вимірювання систем, дозволяючи нечіткі рішення, компроміси та пріоритети. Такий захід повинен враховувати обсяг роботи, необхідної для виявлення вразливості чи слабкості для використання для нападу та здійснення атаки на систему.

Після дослідження існуючих NIDSів, ми виявимо, що розробити новий NIDS все ще вкрай важко для забезпечення надійності, масштабованості та високої продуктивності. Зокрема, практикам важко вирішити, де розмістити NIDS та як найкраще налаштувати його для використання в середовищі з кількома зацікавленими сторонами. Деякі важливі питання ми розбираємо як виклики та перелічуємо їх нижче.

I. Обмеження часу виконання є важливою проблемою для NIDS. Не втрачаючи жодних пакетів, IDS у реальному часі повинен бути в ідеалі здатним захоплювати та перевіряти кожен пакет.

II. Більшість NIDSів та мережевих методів виявлення вторгнень в мережу залежать від середовища. В ідеалі система чи метод повинні бути незалежними від середовища.

III. Характер аномалій постійно змінюється, оскільки зловмисники адаптують свої мережеві атаки, щоб уникнути існуючих рішень виявлення вторгнень. Отже, адаптованість NIDS або методу виявлення необхідна для оновлення з поточними аномаліями, що зустрічаються в локальній мережі або Інтернеті.

IV. В ідеалі, NIDS або метод виявлення повинен уникати високої кількості помилкових тривог. Однак не можна повністю врятуватися від помилкових тривог, навіть якщо йому потрібно прагнути до цього в будь-якому середовищі та полегшити адаптивність під час виконання. Це ще один виклик для спільноти розвитку NIDS.

V. Важливим завданням є динамічне оновлення профілів при NIDS на основі аномалії без конфлікту та без шкоди для виконання. Базу даних профілів потрібно оновлювати кожного разу, коли система виявляє та вирішує новий тип атаки.

VI. Підготовка об'єктивного набору даних про вторгнення в мережу з усіма ненормальними варіаціями профілів – ще одне складне завдання. Кількість нормальних випадків зазвичай велика, і їх частка із випадками нападу дуже перекошена у існуючих загальнодоступних наборах даних про вторгнення. Лише кілька наборів даних про вторгнення з достатньою кількістю інформації про атаку доступні загальнодоступним. Таким чином, існує загальна потреба у контрольних наборах даних про вторгнення для оцінки NIDS та методів виявлення.

VII. Зменшення складності обчислювальної техніки при попередній обробці, навчанні та розгортанні – ще одне завдання, яке потрібно вирішити.

1. Розробка відповідного та швидкого методу вибору функцій для кожного класу атаки – наступна проблема.

2. Вибір відповідної кількості некорельованих, неупереджених класифікаторів з пулу класифікаторів шляхом формування гіпотези класифікатора для побудови ефективного підходу ансамблю для виявлення мережевої аномалії є додатковим завданням.

ПЕРЕЛІК ПОСИЛАНЬ

1. V. Chandola, A. Banerjee, and V. Kumar, “Anomaly Detection : A Survey,” ACM Computing Surveys, vol. 41, no. 3, pp. 15:1–15:58, September 2009.

2. N. K. Ampah, C. M. Akujuobi, M. N. O. Sadiku, and S. Alam, “An intrusion detection technique based on continuous binary communication channels,” International J. Security and Networks, vol. 6, no. 2/3, pp. 174–180, November 2011.

3. M. Agyemang, K. Barker, and R. Alhajj, “A comprehensive survey of numeric and symbolic outlier mining techniques,” Intelligence Data Analysis, vol. 10, no. 6, pp. 521–538, 2006.

4. J. Ma and S. Perkings, “Online novelty detection on temporal sequences,” in Proc. 9th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM, 2003, pp. 613–618.

5. D. Snyder, “Online intrusion detection using sequences of system calls,” Master’s thesis, Department of Computer Science, Florida State University, 2001.

6. Z. Bakar, R. Mohemad, A. Ahmad, and M. Andderis, “A comparative study for outlier detection techniques in data mining,” in Proc. IEEE Conference on Cybernetics and Intelligent Systems, 2006, pp. 1–6.

7. P. Gogoi, D. K. Bhattacharyya, B. Borah, and J. K. Kalita, “A Survey of Outlier Detection Methods in Network Anomaly Identification,” Computer Journal, vol. 54, no. 4, pp. 570–588, April 2011.

8. A. Callado, C. Kamienski, G. Szabo, B. Gero, J. Kelner, S. Fernandes, and D. Sadok, “A Survey on Internet Traffic Identification,” IEEE Commun. Surveys Tutorials, vol. 11, no. 3, pp. 37–52, 2009.

9. W. Zhang, Q. Yang, and Y. Geng, “A Survey of Anomaly Detection Methods in Networks,” in Proc.International Symposium on Computer Network and Multimedia Technology, January 2009, pp. 1–3.

10. A. Sperotto, G. Schaffrath, R. Sadre, C. Morariu, A. Pras, and B. Stiller, “An Overview of IP Flow-Based Intrusion Detection,” IEEE Commun. Surveys Tutorials, vol. 12, no. 3, pp. 343–356, quarter 2010.

11. B. Sun, F. Yu, K. Wu, Y. Xiao, and V. C. M. Leung, “Enhancing security using mobility-based anomaly detection in cellular mobile networks,” IEEE Trans. Veh. Technol., vol. 55, no. 4, pp. 1385 –1396, July 2006.

12. B. Sun, L. Osborne, Y. Xiao, and S. Guizani, “Intrusion detection techniques in mobile ad hoc and wireless sensor networks,” IEEE Wireless Commun., vol. 14, no. 5, pp. 56–63, October 2007.

13. B. Sun, Y. Xiao, and R. Wang, “Detection of Fraudulent Usage in Wireless Networks,” IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3912–3923, November 2007.

14. B. Sun, K. Wu, Y. Xiao, and R. Wang, “Integration of mobility and intrusion detection for wireless ad hoc networks,” International J. Communication Systems, vol. 20, no. 6, pp. 695–721, June 2007.

15. T. Peng, C. Leckie, and K. Ramamohanarao, “Survey of network-based defense mechanisms countering the DoS and DDoS problems,” ACM Computing Surveys, vol. 39, no. 1, pp. 1–42, April 2007.

16. G. Liu, Z. Yi, and S. Yang, “A hierarchical intrusion detection model based on the PCA neural networks,” Neurocomputing, vol. 70, no. 7-9, pp. 1561–1568, 2007.

17. H. Yong and Z. X. Feng, “Expert System Based Intrusion Detection System,” in Proc. International Conference on Information Management, Innovation Management and Industrial Engineering, vol. 4, November 2010, pp. 404 –407.

18. Методичні вказівки по виконанню організаційно-економічної частини дипломних проектів науково-дослідницького характеру для студентів спеціальності 7.080401 “Інформаційні управляючі системи та технології” / Кирич Н.Б., Зяйлик М.Ф., Брощак І.І., Шевчук Я.М – Тернопіль, ТНТУ, – 2009. –11 с.

19. Основы охраны труда: учебник / А. С. Касьян, А. И. Касьян, С. П. Дмитрюк. – Дн-ськ: Журфонд, 2007. – 494 с.

20. Безпека життєдіяльності: Навч. посібник./ За ред. В.Г. Цапка. 4–те вид., перероб. і доп. – К.: Знання, 2006. – 397 с.

ДОДАТКИ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

VII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ »

11–12 грудня 2019 року

ТЕРНОПІЛЬ
2019

УДК 004.056
Р. Яворський, В. Амбок, В. Леньо
Тернопільський національний технічний університет імені Івана Пулюя

ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ РОЗГОРТАННІ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

UDC 004.056
R. Yavorskii, V. Ambok, V. Lenio
(Ternopil Ivan Puluj National Technical University, Ukraine)

INFORMATION SECURITY CHALANGES FOR DEPLOYMENT OF INTRUSION DETECTION SYSTEMS

Розглянемо основні класи небезпек, характерних для розгортання систем виявлення вторгнень на основі віртуальних машин – Virtual Machines (VM), оскільки саме вони є основним елементом побудови інформаційної інфраструктури організації у хмарних сервісах [1].

VM image sharing. Вважається, що існує репозиторій образів різних VM, а користувач на їх основі може сконфігурувати потрібний образ. Таке використання образів з репозиторію може спричинити появу вразливостей у системі [2]. Зловмисник може знайти вразливості в існуючому образі або завантажити у репозиторій власний, шкідливий, образ VM.

VM isolation. З іншого боку проблему становить використання VM в ізоляції від інших віртуальних машин, що працюють на тому ж комп'ютері. Очевидно, що вони мають бути ізольовані одна від одної. Попри логічну ізоляцію існує проблема доступу до спільних ресурсів (пам'яті, дискового простору). Через що виникає проблема крос-VM атак.

VM escape. Це ситуація, коли зловмисник обходить систему управління VM [3]. В цьому випадку зловмисник отримає доступ до інших VM, що може спричинити також неавторизований доступ до файлів на жорстких дисках. До таких вразливостей в основному схильні системи
IaaS [4].

VM migration. Під час міграції весь інформаційний контент VM стає відкритим при передачі даних по мережі [5]. На додачу модуль міграції може бути скомпрометований атакуючим зловмисником для переміщення VM на сторонній сервер. Тому критично важливим є виконання операції міграції VM з дотриманням всіх заходів безпеки.

Безпечне управління образами забезпечується за допомогою спеціально розробленого фреймворку, згідно якого кожну операцію може виконувати тільки авторизований користувач. Крім того рекомендується використовувати журналювання всіх операцій.

Література

1. F. Sabahi, “Secure Virtualization for Cloud Environment Using Hypervisor-based Technology,” Int. Journal of Machine Learning and Computing, vol. 2, no. 1, 2012.
2. S.-F. Yang, W.-Y. Chen, and Y.-T. Wang, “ICAS: An inter-VM IDS Log Cloud Analysis System,” in 2011IEEE International Conference on Cloud Computing and Intelligence Systems, 2011, pp. 285–289.
3. S. L. and Z. L. and X. C. and Z. Y. and J. Chen, S. Luo, Z. Lin, X. Chen, Z. Yang, and J. Chen, “Virtualization security for cloud computing service,” in International Conference on Cloud and Service Computing (CSC), 2011, pp. 174–179.
4. M. Ibrahim, A.S. and Hamlyn-Harris, J. and Grundy, J. and Almorsy, “CloudSec: A security monitoring appliance for Virtual Machines in the IaaS cloud model,” in 5th International Conference on Network and System Security (NSS), 2011, pp. 113–120.
5. J. Sedayao, S. Su, X. Ma, M. Jiang, and K. Miao, “A Simple Technique for Securing Data at Rest Stored in a Computing Cloud,” in Proceedings of the 1st International Conference on Cloud Computing, 2009, pp. 553–558.

М. Садівник
МАШИННЕ НАВЧАННЯ У БРАУЗЕРІ З ВИКОРИСТАННЯМ TENSORFLOW.JS 89
Р. Самець
ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ ОЗОНОГЕНЕРАТОРІВ ДЛЯ МЕДИЧНИХ ОЗОНОТЕРАПЕВТИЧНИХ СИСТЕМ 90
Я. Самиця, М. Горалечко, Ю. Дзига
ІЄРАРХІЧНА СТРУКТУРА МОДЕЛЕЙ ЯКОСТІ СИСТЕМ ЕЛЕКТРОННОЇ КОМЕРЦІЇ 91
Я. Самиця, С. Магула
ПРИНЦИПИ ІНТЕГРАЛЬНОЇ ОЦІНКИ РІВНЯ ЯКОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ АВТОМАТИЗОВАНИХ СИСТЕМ КЕРУВАННЯ 93
Т. Сачик, Н. Загородна
ЗАХИСТ ПЕРСОНАЛЬНОЇ ІНФОРМАЦІЇ В ЗАДАЧАХ АНАЛІЗУ ТА ОБРОБКИ ВЕЛИКИХ ДАНИХ 95
Д. Северин
ПРОГРАМНИЙ ЗАСІБ ДЛЯ УПРАВЛІННЯ ПРОЦЕСОМ МІГРАЦІЇ ВІРТУАЛЬНИХ МАШИН В ОБЧИСЛЮВАЛЬНІЙ ХМАРІ 96
О. Ситник, А. Лазорко
МЕТОД РЕПЛІКАЦІЇ ДАНИХ З ВИКОРИСТАННЯМ NFC-ТЕХНОЛОГІЇ 97
Т. Склярова, О. Палка
ІСТОРІЯ РОЗВИТКУ ГЕОІНФОРМАЦІЙНИХ СИСТЕМ 98
В. Соборук, Л. Матійчук
ЗАДАЧІ ТЕСТУВАННЯ СИСТЕМ МОБІЛЬНОГО ЗВ'ЯЗКУ 99
А. Тарапата, М. Іваник
ВИКОРИСТАННЯ МЕТОДУ АНАЛІЗУ ІЄРАРХІЙ ДЛЯ ОЦІНЮВАННЯ ЯКОСТІ ПРОЕКТУ КОМП`ЮТЕРНИХ МЕРЕЖ 100
А. Тарапата, А. Гулик
ВИКОРИСТАННЯ МОДЕЛЕЙ ЯКОСТІ ДЛЯ РОЗРОБКИ ВИМОГ 101
П. Телевяк, Л. Матійчук
АНАЛІЗ СУЧАСНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ ТА ЇХ КЛАСИФІКАЦІЯ 102
О. Топчак, Н. Кунанець
РЕКОМЕНДАЦІЙНА СИСТЕМА РЕАБІЛІТАЦІЇ ХВОРИХ З ПРОБЛЕМАМИ ОПОРНО-РУХОВОГО АПАРАТУ 103
Б. Тригубець
РОЗРОБКА CMS ТА МЕТОДІВ ЗАХИСТУ WEB-САЙТІВ НА ЇЇ ОСНОВІ 104
Л. Тучапський, М. Поліщук
ЦИФРОВА ФІЛЬТРАЦІЯ РАДІОСИГНАЛІВ 105
М. Шмигельський, В. Ліщинський
ОСНОВНІ МЕТОДИ І ПРИЙОМИ ПОРУШЕННЯ БЕЗПЕКИ СУЧАСНИХ БЕЗДРОТОВИХ МЕРЕЖ 106
А. Шум'як, О. Палка, І. Пятківський
АНАЛІЗ ІНТЕЛЕКТУАЛЬНИХ ТРАНСПОРТНИХ СИСТЕМ 107
Р. Яворський, В. Амбок, В. Леньо
ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ РОЗГОРТАННІ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ 108