**Метод виявлення вторгнень**

**Abstract**

***Method of detection of invaders***

*This paper presents an advanced intrusion detection method for computer systems and networks. The proposed approach combines signature-based techniques, anomaly detection, and neural network technologies with machine learning algorithms. The method incorporates multi-stage analysis, including data preprocessing, neural network-based anomaly detection, signature analysis, and adaptive detector generation. Key features include the integration of machine learning classifiers with neural networks and a continuous adaptation mechanism. The paper discusses the method's effectiveness in detecting both known and novel attacks while minimizing false positives. It also addresses implementation challenges and the method's applicability across various network environments. The research emphasizes the importance of adaptive security measures in the face of evolving cyber threats.*

**Вступ**

У сучасному світі одним з найбільш пріоритетних напрямків кібербезпеки є розробка ефективних систем виявлення вторгнень, які забезпечують захист комп'ютерних мереж та інформаційних систем від зловмисних атак. Виявлення вторгнень є критично важливим компонентом загальної стратегії безпеки, що дозволяє своєчасно ідентифікувати та реагувати на потенційні загрози.

Щодня кількість та складність кібератак зростає: їх використовують не лише для крадіжки даних, але й для промислового шпіонажу, порушення роботи критичної інфраструктури і навіть для впливу на політичні процеси. В цьому контексті, розробка передових методів виявлення вторгнень стає все більш актуальною.

Стаття присвячена аналізу відомих підходів до виявлення вторгнень на основі машинного навчання на великих обсягах мережевого трафіку.

**Постановка задачі**

Задача полягає у визначенні недоліків відомих методів виявлення вторгнень у комп'ютерні системи та мережі, а також обґрунтуванні підходів до їх виправлення.

**Термінологія**

Система виявлення вторгнень (IDS) – це програмне або апаратне забезпечення, яке автоматично виявляє і попереджає про несанкціоновані спроби доступу, атаки або порушення безпеки в комп'ютерній мережі або системі.

Сигнатурний аналіз – метод виявлення вторгнень, що базується на порівнянні шаблонів відомих атак з поточною активністю в мережі.

Виявлення аномалій – підхід до ідентифікації вторгнень, який фокусується на виявленні відхилень від нормальної поведінки системи або мережі.

Машинне навчання в кібербезпеці – застосування алгоритмів, які дозволяють комп'ютерним системам автоматично вдосконалювати свою здатність виявляти загрози на основі аналізу даних без явного програмування.

**Опис методу**

Системи виявлення вторгнень (СВВ) поділяються на два основні типи: локальні та мережеві [1]. Локальні СВВ встановлюються на кожному окремому комп'ютері, тоді як мережеві СВВ аналізують пакети, що надходять в мережу через один пристрій, перш ніж пересилати їх заданим вузлам. Мережеві СВВ стають менш ефективними зі збільшенням кількості вузлів у мережі, оскільки забезпечення надійної фільтрації пакетів ускладнюється.

Методи виявлення атак можна розділити на три основні групи:

1. Сигнатурні методи.
2. Методи виявлення аномалій.
3. Комбіновані методи.

Сигнатурні методи описують кожну атаку особливою моделлю або сигнатурою. Ці методи мають високу точність визначення факту атаки, але не здатні виявляти атаки, сигнатури яких ще не визначені. Найпоширенішим серед сигнатурних методів є метод контекстного пошуку, який полягає у виявленні у вихідній інформації певної множини символів.

Пропонований метод виявлення вторгнень базується на комбінованому підході, що поєднує переваги сигнатурних методів, методів виявлення аномалій та нейромережевих технологій. Цей інтегрований підхід дозволяє ефективно виявляти як відомі, так і нові типи атак, одночасно знижуючи кількість помилкових спрацьовувань [2].

Метод починається з етапу попередньої обробки мережевого трафіку. На цьому етапі сенсорна система отримує трафік від датчиків мережі, здійснюється збір та нормалізація даних, а також виділення ключових ознак пакетів. Отриманий набір даних нормалізується і перетворюється на масштабований вектор даних, що забезпечує якісну підготовку для подальшого аналізу та підвищує ефективність роботи системи в цілому.

Наступним кроком є аналіз даних за допомогою першої нейронної мережі. Цей етап передбачає подачу нормалізованого вектора даних на обробку нейронній мережі, яка навчена виявляти аномалії у мережевому трафіку. Якщо нейромережа не виявляє ознак аномалій, система повертається до початкового етапу збору даних. У випадку виявлення аномалій, система переходить до наступного етапу аналізу.

Паралельно з нейромережевим аналізом проводиться сигнатурний аналіз, який передбачає порівняння вхідних даних з базою відомих сигнатур атак. Цей етап дозволяє швидко виявляти відомі загрози, що є особливо важливим для захисту від поширених типів атак.

У разі виявлення потенційної загрози, система генерує набір спеціалізованих детекторів з різними параметрами та структурою. Ці детектори навчаються розпізнавати специфічні ознаки мережевої атаки, що дозволяє більш точно ідентифікувати характер загрози. Вектор вхідних даних досліджується цими детекторами для підтвердження наявності вторгнення.

Ключовою особливістю запропонованого методу є застосування алгоритмів машинного навчання, зокрема, методів класифікації, таких як Random Forest, у поєднанні з нейронними мережами. Модель машинного навчання тренується на історичних даних про атаки та нормальний трафік, що дозволяє їй ефективно розрізняти легітимну та зловмисну активність. Використання машинного навчання значно підвищує адаптивність системи до змін у мережевому середовищі та покращує її здатність виявляти складні та раніше невідомі типи атак.

Після проведення всіх етапів аналізу відбувається агрегація результатів. На цьому етапі комбінуються результати сигнатурного аналізу, виявлення аномалій та машинного навчання. На основі цієї агрегованої інформації приймається остаточне рішення про наявність або відсутність вторгнення. У разі підтвердження вторгнення, система генерує сигнал тривоги [3].

Важливою складовою методу є постійне оновлення та адаптація. Це включає регулярне оновлення бази сигнатур для виявлення нових відомих атак, а також періодичне перенавчання моделей машинного навчання та нейронних мереж на нових даних. Крім того, система має механізм "мутації" детекторів, які поглинають інформацію про виявлене втручання, що дозволяє системі постійно вдосконалюватися та адаптуватися до нових загроз.

Запропонований метод демонструє високу ефективність у виявленні широкого спектру атак, від добре відомих до нових та складних. Його гнучкість та адаптивність роблять його придатним для застосування в різноманітних мережевих середовищах, від невеликих локальних мереж до великих корпоративних інфраструктур. Крім того, інтеграція машинного навчання та нейронних мереж дозволяє системі постійно вдосконалюватися, покращуючи свою точність та ефективність з часом.

**Література**

1. Аналіз та класифікація методів виявлення вторгнень в інформаційну систему | Системи управління, навігації та зв’язку. Збірник наукових праць. *Open Journal Systems*. URL: <https://journals.nupp.edu.ua/sunz/article/view/323> (дата звернення: 29.09.2024).
2. Учасники проектів Вікімедіа. Система виявлення вторгнень – Вікіпедія. *Вікіпедія*. URL: [https://uk.wikipedia.org/wiki/Система\_виявлення\_вторгнень](https://uk.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D0%B2%D0%B8%D1%8F%D0%B2%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F_%D0%B2%D1%82%D0%BE%D1%80%D0%B3%D0%BD%D0%B5%D0%BD%D1%8C) (дата звернення: 29.09.2024).
3. Лукова-Чуйко Н. Методи виявлення вторгнень у сучасних системах ids. *Інформаційна та кібернетична безпека*. С. 19–26. URL: <https://moodle.znu.edu.ua/pluginfile.php/598874/mod_folder/content/0/03-BIST_No+1(5)_2021+Lukova+19-26.pdf?forcedownload=1>.