МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій,
обліку та фінансів
Кафедра комп'ютерних технологій
і моделювання систем

Кваліфікаційна робота
на правах рукопису

Сиротюк Ярослав Анатолійович
(прізвище, ім'я, по батькові здобувача освіти)

УДК 004.056.53:004.75

КВАЛІФІКАЦІЙНА РОБОТА

Дослідження методів виявлення вторгнення у системах інформаційної безпеки
(тема роботи)

(шифр і назва спеціальності)

Подається на здобуття освітнього ступеня магістр

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Я.А.Сиротюк
(підпис, ініціали та прізвище здобувача вищої освіти)

Керівник роботи
Молодецька Катерина Валеріївна
(прізвище, ім'я, по батькові)
д.т.н., професор
(науковий ступінь, вчене звання)

Житомир – 2024

Висновок кафедри _____
за результатами попереднього захисту: _____

Протокол засідання кафедри _____
№_____від «_____»_____20____р.

Завідувач кафедри _____

_____ _____ _____
(науковий ступінь, вчене звання) (підпис) (прізвище, ім'я, по батькові)
«_____»_____20____р.

Результати захисту кваліфікаційної роботи

Здобувач вищої освіти_____захистив (ла)
(прізвище ,ім'я, по батькові)
кваліфікаційну роботу з оцінкою:

сума балів за 100-бальною шкалою _____
за шкалою ECTS _____
за національною шкалою _____

Секретар ЕК

_____ _____ _____
(науковий ступінь, вчене звання) (підпис) (прізвище, ім'я, по батькові)

АНОТАЦІЯ

Сиротюк Я.А. Дослідження методів виявлення вторгнення у системах інформаційної безпеки. – Кваліфікаційна робота на правах рукопису.

Кваліфікаційна робота на здобуття освітнього ступеня магістр за спеціальністю 125 – кібербезпека. – Поліський національний університет, Житомир, 2024.

Сучасний розвиток інформаційних технологій супроводжується зростанням загроз для кібербезпеки, що зумовлює необхідність постійного вдосконалення методів виявлення вторгнень у системах інформаційної безпеки. У дипломній роботі досліджено теоретичні основи та сучасні підходи до забезпечення інформаційної безпеки з акцентом на виявлення вторгнень, а також проведено порівняльний аналіз ефективності існуючих методів, зокрема сигнатурних, поведінкових і методів машинного навчання.

На основі проведеного аналізу визначено ключові недоліки та обмеження наявних методів, що дозволило розробити рекомендації для підвищення їх ефективності у виявленні аномалій та реагуванні на загрози. Запропоновані рішення сприяють удосконаленню механізмів інформаційної безпеки шляхом підвищення точності виявлення вторгнень та зменшення кількості помилкових спрацьовувань.

Отримані результати можуть бути використані для подальшого розвитку методик виявлення вторгнень у системах кіберзахисту, а також для практичного впровадження у різних інформаційних середовищах для мінімізації ризиків і підвищення загальної стійкості систем до кіберзагроз.

Ключові слова: IDS, NIDS, КІБЕРЗАГРОЗИ, ВИЯВЛЕННЯ ВТОРГНЕНЬ, СИСТЕМИ БЕЗПЕКИ.

SUMMARY

Syrotyuk Y.A. Study of intrusion detection methods and response to cyber security threats. - Qualification work on the rights of the manuscript.

Qualification work for the master's degree in specialty 125 – cybersecurity. - Polis National University, Zhytomyr, 2024.

The modern development of information technologies is accompanied by an increase in cybersecurity threats, which makes it possible to constantly improve implementation methods in information security systems. The thesis examines the theoretical foundations and modern approaches to ensuring information security with an emphasis on intrusion detection, and also conducts a comparative analysis of the effectiveness of existing methods, in particular signature, behavioral and machine learning methods.

Based on the analysis, key shortcomings and limitations of existing methods were identified, which allowed developing recommendations for increasing their effectiveness in the event of anomalies and responding to threats. The proposed solutions contribute to improving information activity mechanisms by increasing the accuracy of intrusion detection and reducing the safety of erroneous cases.

The results obtained can be used for further development of intrusion detection methods in cyber defense systems, as well as for practical implementation in various information environments to minimize risks and increase the overall resilience of the system to cyber threats.

Keywords: IDS, NIDS, CYBER THREATS, INTRUSION DETECTION, SECURITY SYSTEMS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IDS – Open source intelligence;

США – Сполучені Штати Америки;

NIDS – Network Intrusion Detection System;

APT – Advanced Persistent Threats;

DDoS – denial-of-service attack.

ВСТУП

Актуальність теми. Системи виявлення вторгнень відіграють важливу роль у кіберзахисті, оскільки вони дозволяють вчасно ідентифікувати несанкціоновані дії у комп'ютерних мережах та інформаційних системах. Проте, існуючі методи виявлення вторгнень мають певні обмеження, зокрема низьку ефективність проти нових та складних загроз, затримки у виявленні, високу кількість хибно-позитивних спрацьовувань[1]**.** Це вимагає вдосконалення методів для підвищення їхньої точності та швидкодії у протидії актуальним кіберзагрозам.

Метою роботи є дослідження, аналіз та вдосконалення методів виявлення вторгнень у системах інформаційної безпеки для підвищення точності виявлення атак, оперативності реагування на загрози та зниження кількості хибних спрацьовувань. Це дозволить ефективніше захищати інформаційні системи та мережі від сучасних і складних кіберзагроз, зокрема невідомих атак, аномальної поведінки користувачів та інших несанкціонованих дій[2].

Об’єктом дослідження є процеси виявлення вторгнень у системах інформаційної безпеки.

Предметом дослідження є методи та підходи до виявлення вторгнень, зокрема сигнатурні, поведінкові та методи машинного навчання.

Наукова новизна роботи полягає у вдосконаленні підходів до виявлення вторгнень завдяки дослідженню існуючих методів, що дозволило розробити рекомендації щодо підвищення ефективності виявлення загроз. Запропоновано комбінований підхід, що поєднує можливості сигнатурного, поведінкового аналізу та алгоритмів машинного навчання для покращення виявлення аномалій та вторгнень.

Результати дослідження мають практичне значення для організацій, що займаються забезпеченням інформаційної безпеки. Запропоновані рекомендації можуть бути використані для підвищення ефективності систем виявлення вторгнень, що дозволить своєчасно ідентифікувати загрози, мінімізувати ризики та підвищити стійкість інформаційних систем до кібератак.

1 ТЕОРЕТИЧНІ ОСНОВИ МЕТОДІВ ВИЯВЛЕННЯ ВТОРГНЕНЬ У СИСТЕМАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Загальні поняття та класифікація методів виявлення вторгнень

У сучасних умовах стрімкої цифровізації кібербезпека стає одним із ключових викликів для організацій незалежно від галузі або масштабу діяльності. Одним із найефективніших інструментів для забезпечення захисту інформаційних систем від потенційних загроз є системи виявлення вторгнень (IDS)[3]. Їх основна функція полягає в ідентифікації спроб несанкціонованого доступу до мережевих або комп'ютерних ресурсів, а також у наданні організації можливості швидко реагувати на такі інциденти.

Інциденти кібербезпеки, такі як атака на Colonial Pipeline у 2021 році, демонструють значущість систем виявлення вторгнень[4]. У цьому випадку злочинці використали шкідливе програмне забезпечення для порушення роботи компанії, що призвело до масштабних економічних втрат. За даними звітів Cybersecurity Ventures, загальний обсяг збитків від кіберзлочинності у 2023 році перевищив 8 трильйонів доларів США, а до 2025 року прогнозується зростання цього показника до 10,5 трильйонів[5]. У таких умовах інтеграція IDS стає обов'язковою умовою для ефективного управління ризиками[6].

Використання IDS має вирішальне значення для організацій, оскільки вони дозволяють:

- своєчасно виявляти спроби викрадення даних або проникнення в систему;
- знижувати ризик фінансових втрат, пов'язаних із кібератаками;
- забезпечувати безперервну роботу систем, мінімізуючи простої через інциденти безпеки;
- удосконалювати захисну інфраструктуру на основі зібраної інформації про атаки[7].

Системи виявлення вторгнень можна класифікувати за їхнім підходом до

моніторингу та реагування – активні та пасивні[8]. Зокрема, активні IDS не лише виявляють загрози, але й автоматично реагують на них, наприклад, блокуючи атаки. Пасивні системи, навпаки, обмежуються інформуванням адміністраторів про виявлені інциденти. Обидва типи мають свої переваги: активні системи підвищують оперативність захисту, тоді як пасивні забезпечують гнучкість у виборі заходів реагування[9].

Важливим аспектом роботи IDS є методи виявлення загроз.

Методи виявлення IDS базуються на аналізі:

- підписів (signature-based detection) — порівняння з відомими моделями атак. Це ефективно для ідентифікації відомих загроз, але не дозволяє виявляти нові види атак[10]. Наприклад, цей метод швидко ідентифікує відомий вірус WannaCry, проте неефективний проти нових загроз;
- аномалій (anomaly-based detection) — аналіз відхилень від звичної поведінки системи[11]. Такий підхід дозволяє виявляти невідомі загрози, однак супроводжується високим рівнем помилкових спрацьовувань.

З точки зору механізму роботи IDS можна поділити на хостові та мережеві[12]. Хостові IDS (HIDS) — аналізують активність окремих пристроїв, зокрема зміни у файловій системі або спроби несанкціонованого доступу до даних. Наприклад, зміни у важливих системних файлах без відома адміністратора можуть сигналізувати про атаку

Мережеві IDS (NIDS) — моніторять трафік у мережі, виявляючи атаки на рівні мережевої взаємодії, зокрема DDoS-атаки або експлуатацію вразливостей у протоколах чи DDoS-атаки.

Системи виявлення вторгнень також класифікуються залежно від типу атак, які вони здатні виявляти:

- атаки на доступність (наприклад, DDoS);
- конфіденційність (несанкціонований доступ до даних) або цілісність (зміна чи пошкодження інформації) [13].

Загальну схему роботи систем виявлення вторгнень зображено на рис.1.1.

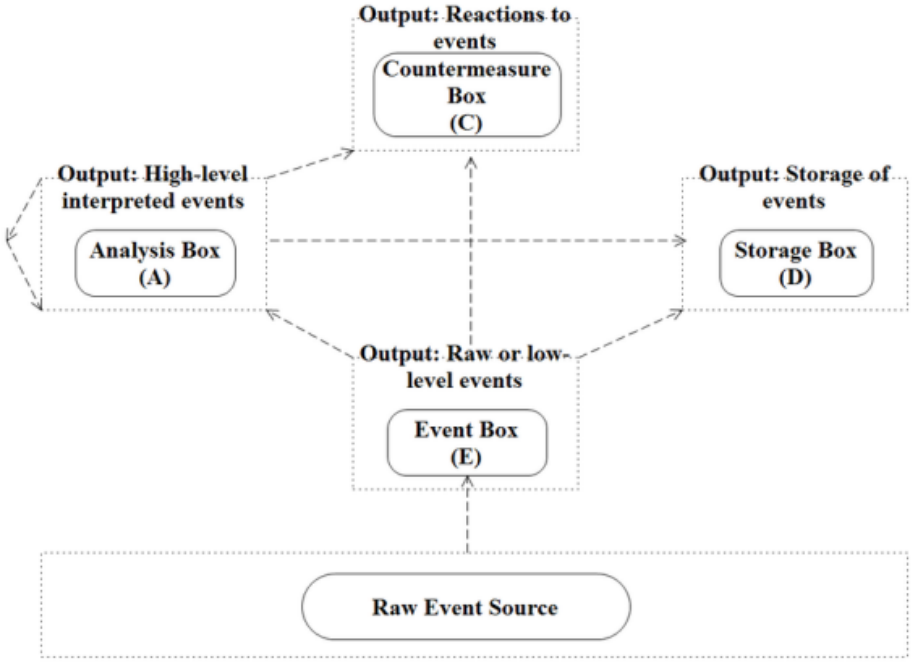

Рисунок 1.1 – Загальна схема роботи систем виявлення вторгнень

Виявлення кожного типу атак вимагає застосування специфічних підходів, таких як аналіз аномальних навантажень, моніторинг поведінки користувачів чи контроль змін у даних.

1.2 Аналіз сучасних підходів до забезпечення інформаційної безпеки у контексті виявлення вторгнень

Інновації у сфері IDS активно сприяють їхньому вдосконаленню. Використання штучного інтелекту та машинного навчання дозволяє автоматично оновлювати бази підписів, створювати моделі для виявлення аномалій та прогнозувати потенційні загрози[14]. Наприклад, машинне навчання допомагає виявляти складні атаки, такі як APT [15], аналізуючи довгострокові тенденції в мережевій активності. Такі інструменти, як Snort, Suricata чи Zeek, забезпечують гнучкі можливості для аналізу даних, виявлення загроз та створення звітів.

Snort — це відкрита система виявлення вторгнень, яка поєднує можливості аналізу мережевого трафіку та реєстрації підозрілої активності[16]. Її основними

функціями є моніторинг мережевого трафіку в режимі реального часу, виявлення атак за підписами (signature-based detection), створення власних правил для ідентифікації загроз. Завдяки своїй гнучкості, її можна адаптувати до різних інфраструктур. До недоліків можна віднести потребу значних ресурсів для ефективної роботи у великих мережах, а також обмеженість у виявленні нових загроз без додаткової конфігурації.

Приклад роботи даної системи зображено на рисунку 1.2.

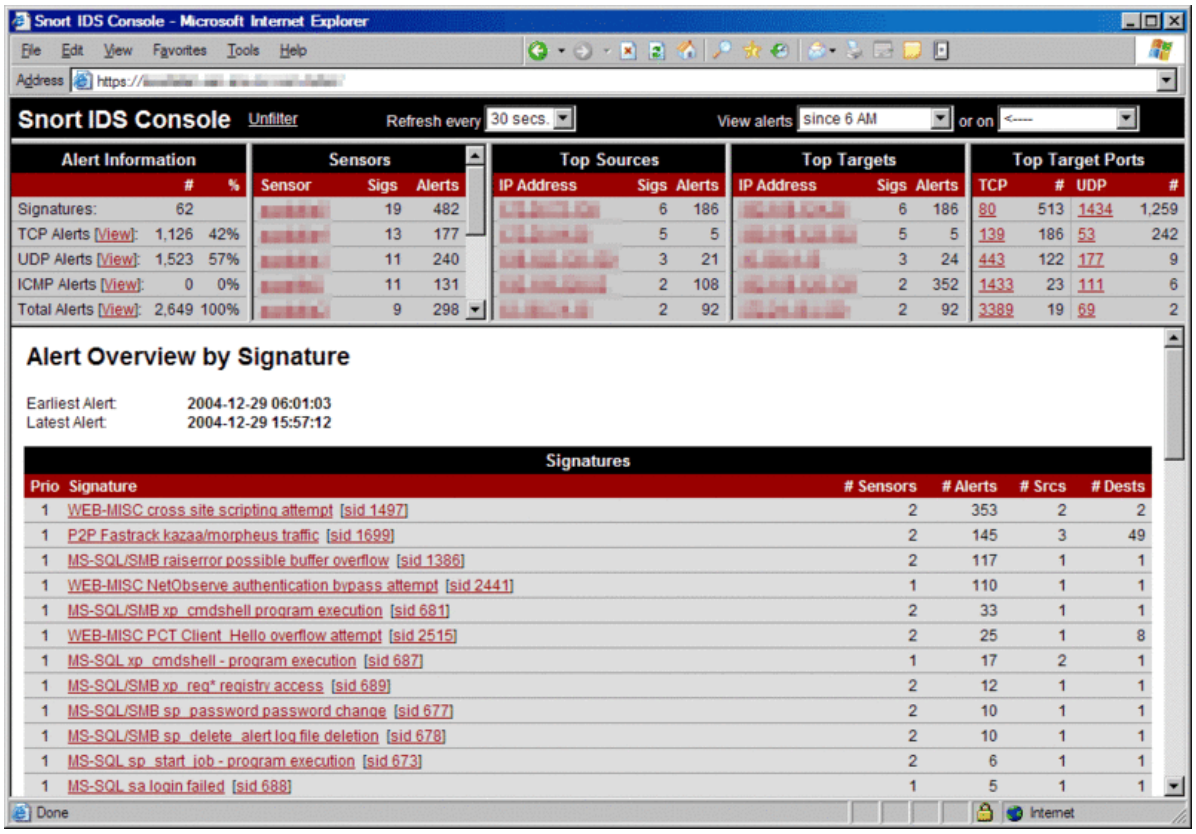

Рисунок 1.2 – Приклад роботи системи виявлення вторгнень Snort

Suricata є ще однією потужною системою виявлення вторгнень із відкритим кодом, яка підтримує функції моніторингу трафіку та аналізу загроз[17].
Глибокий аналіз пакетів (Deep Packet Inspection). Її основними функціями є підтримка багатопоточності, що забезпечує високу продуктивність, а також можливість інтеграції з іншими інструментами, такими як Zeek або ELK Stack[18] для розширеного аналізу. завдяки багатопоточності обробляє великий обсяг трафіку, а підтримка широкого спектру протоколів та можливість створення складних правил Недоліками даної системи є складність налаштування для нових

користувачів та вимоги до ресурсів на великих мережах. На рисунку 2.2 показано функціонал даної системи.

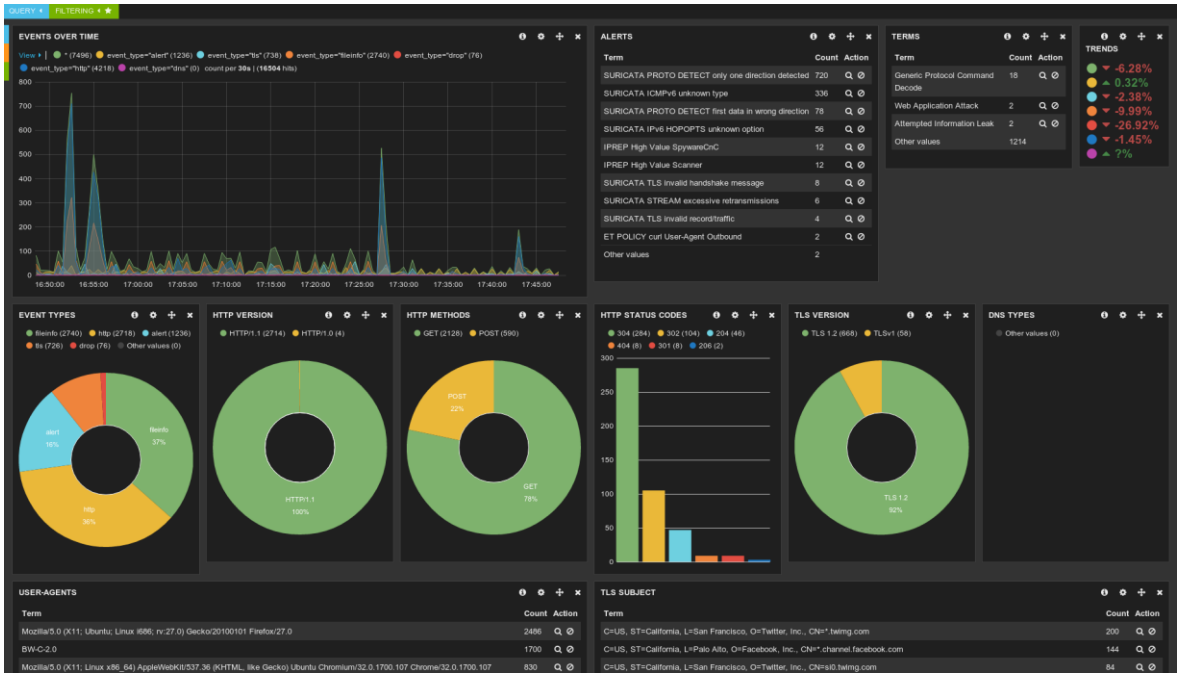

Рисунок 1.2 – Функціонал системи Suricata

Zeek — це потужний інструмент для мережевого аналізу, який працює не лише як IDS, а й як платформа для аналізу поведінки у мережі[19]. Основні функції, які він виконує є: моніторинг мережевих протоколів на рівні додатків (HTTP, DNS, FTP тощо), виявлення аномалій за поведінковими моделями, розширена підтримка сценаріїв для автоматизації аналізу загроз.

Забезпечення інформаційної безпеки охоплює не лише захист даних від несанкціонованого доступу, але й підтримання їхньої конфіденційності, цілісності та доступності. Сучасні підходи до виявлення вторгнень зосереджені на інтеграції традиційних методів із новими технологіями, такими як аналіз великих даних чи блокчейн. Це дозволяє підвищити ефективність систем, знижуючи кількість помилкових спрацьовувань і збільшуючи їхню адаптивність до нових типів загроз.

Методи аналізу поведінки користувачів сприяють виявленню підозрілих дій, які можуть свідчити про внутрішні загрози чи компрометацію облікових записів[20]. Інтеграція IDS з іншими засобами безпеки, такими як системи

запобігання вторгненням (IPS) чи фаєрволи, дозволяє створювати багаторівневу систему захисту, яка здатна ефективно протистояти кіберзагрозам.

Машинне навчання у контексті виявлення аномалій в кіберпросторі є потужним інструментом для підвищення ефективності систем кібербезпеки. У сучасному світі, де кіберзагрози розвиваються швидко, а їх методи постійно еволюціонують, традиційні підходи до виявлення атак, такі як сигнатурне виявлення, стають менш ефективними[21]. Це пояснюється тим, що нові види атак часто не мають відомих сигнатур, і їх неможливо виявити за допомогою традиційних методів. У такому випадку методи машинного навчання можуть надати рішення для ефективного виявлення аномальних дій, які можуть вказувати на потенційні загрози.

Висновки до першого розділу

У сучасних умовах стрімкої цифровізації та зростання складності кіберзагроз системи виявлення вторгнень відіграють важливу роль у забезпеченні інформаційної безпеки. Аналіз теоретичних основ та сучасних методів виявлення вторгнень демонструє, що поєднання традиційних підходів зі штучним інтелектом та методами машинного навчання відкриває нові можливості для ефективного захисту інформаційних систем.Інтеграція IDS з іншими засобами кіберзахисту, такими як фаєрволи, системи запобігання вторгненням та платформи для аналізу великих даних, забезпечує створення багаторівневої системи безпеки, здатної ефективно реагувати на сучасні виклики. Такі інструменти, як Snort, Suricata та Zeek, демонструють високу гнучкість і продуктивність у моніторингу мережевої активності, виявленні загроз і аналізі їхніх наслідків.

2 ДОСЛІДЖЕННЯ ТА ПОРІВНЯННЯ ІСНУЮЧИХ МЕТОДІВ ВИЯВЛЕННЯ ВТОРГНЕНЬ

2.1 Аналіз ефективності сигнатурних і поведінкових методів виявлення вторгнень

У контексті забезпечення інформаційної безпеки в умовах постійного розвитку кіберзагроз важливу роль відіграють системи виявлення вторгнень , які здатні виявляти спроби несанкціонованого доступу, атаки або інші зловмисні дії в інформаційних системах[22]. Одним із основних підходів до виявлення таких загроз є використання сигнатурних та поведінкових методів, які мають свої переваги і недоліки. Визначення ефективності цих методів вимагає глибокого аналізу їх застосування, можливостей та обмежень у реальних умовах експлуатації.

Сигнатурні методи виявлення вторгнень базуються на порівнянні поточної активності в системі з відомими сигнатурами атак — зазвичай, це шаблони, що описують типові характеристики зловмисних дій, наприклад, певні послідовності команд, типи мережевих запитів чи особливості поведінки шкідливого програмного забезпечення[23]. Система виявлення вторгнень за допомогою сигнатур здатна виявити відомі атаки швидко й ефективно. Однак основним обмеженням цього підходу є його неспроможність виявляти нові, раніше невідомі загрози, оскільки для кожної нової атаки необхідно створювати нові сигнатури.

Переваги сигнатурного методу полягають у його високій точності при виявленні відомих атак, що зумовлює низьку кількість помилкових спрацьовувань[23]. Завдяки своїй детермінації та стандартизованим шаблонам сигнатури дозволяють точно ідентифікувати певний тип атак, що забезпечує швидку реакцію на них. Такі системи легко налаштовуються, оскільки для роботи з ними потрібна лише база даних із сигнатурами відомих загроз, і вони можуть інтегруватися в існуючі мережеві або хостові системи без значних додаткових затрат.

Однак існують значні недоліки сигнатурних методів. Головним із них є їх неспроможність реагувати на нові типи атак, які не були включені до бази сигнатур. Враховуючи постійну еволюцію методів злому та використання нових, складніших технік, сигнатурні системи можуть залишати системи вразливими до нових загроз. Зокрема, атаки нульового дня (zero-day) — такі, що використовують нові вразливості, ще не зафіксовані у сигнатурних базах — залишаються непоміченими для таких IDS, що обмежує їхню ефективність у захисті від передових кіберзагроз[24].

Поведінкові методи виявлення вторгнень, на відміну від сигнатурних, не потребують заздалегідь відомих шаблонів атак[25]. Ці методи виявляють аномалії в поведінці користувачів або програм, порівнюючи поточну активність із моделями нормальної діяльності системи. Якщо певна діяльність відхиляється від цих моделей, система сигналізує про можливе вторгнення або зловмисну активність. Поведінкові методи дозволяють виявляти нові, невідомі раніше загрози, оскільки вони ґрунтуються на відстеженні відхилень від нормального функціонування системи, а не на визначених сигнатурах.

Основною перевагою поведінкових методів є їх здатність виявляти нові види атак, яких ще не існує в базах сигнатур[26]. Це особливо важливо в умовах, коли зловмисники постійно змінюють свої тактики, щоб уникнути виявлення за допомогою традиційних підписів. Крім того, поведінкові методи можуть використовуватися для виявлення атак, які не залишають чітких слідів у вигляді відомих сигнатур, таких як атаки з використанням соціальної інженерії або складні багатоетапні кампанії, що включають маніпуляції з даними[26]. Однак цей підхід також має певні недоліки. По-перше, алгоритми на основі аномалій можуть мати високу кількість помилкових спрацьовувань, оскільки зміни в поведінці можуть бути викликані не лише зловмисними діями, але й законною діяльністю, наприклад, оновленнями програмного забезпечення або змінами в роботі користувачів. Це може призвести до необхідності частих налаштувань і підвищення складності системи. Також створення та постійне оновлення моделей «нормальної» поведінки є складним завданням, яке потребує значних

обчислювальних ресурсів і детального аналізу поведінки системи на протязі тривалого часу[27].

Порівняння ефективності цих двох методів виявлення вторгнень дозволяє визначити, що кожен з них має свої переваги в різних умовах[28]. Сигнатурні методи є ефективними при захисті від відомих атак, мають менше помилкових спрацьовувань і дозволяють забезпечити високу точність виявлення конкретних загроз. Водночас поведінкові методи демонструють вищу ефективність у випадках, коли необхідно виявити нові або складні атаки, які не можуть бути зафіксовані сигнатурами.

Для досягнення максимального рівня безпеки багато сучасних систем виявлення вторгнень комбінують обидва підходи, створюючи гібридні системи, які поєднують переваги сигнатурного виявлення та аномалійного аналізу[29]. Це дозволяє ефективно виявляти як відомі, так і нові загрози, мінімізуючи недоліки кожного методу окремо. Однак навіть у таких системах важливо постійно оновлювати бази даних і коригувати моделі поведінки для забезпечення адекватної реакції на нові кіберзагрози.

Таким чином, ефективність сигнатурних і поведінкових методів виявлення вторгнень визначається конкретними умовами і вимогами до захисту інформаційної системи. Підхід до вибору методу виявлення має залежати від типу атак, які очікуються, рівня допустимих помилок та ресурсів, доступних для моніторингу і аналізу[30].

2.2 Огляд методів машинного навчання для виявлення аномалій у кіберпросторі

Машинне навчання у контексті виявлення аномалій в кіберпросторі є потужним інструментом для підвищення ефективності систем кібербезпеки[31]. У сучасному світі, де кіберзагрози розвиваються швидко, а їх методи постійно еволюціонують, традиційні підходи до виявлення атак, такі як сигнатурне виявлення, стають менш ефективними. Це пояснюється тим, що нові види атак

часто не мають відомих сигнатур, і їх неможливо виявити за допомогою традиційних методів. У такому випадку методи машинного навчання можуть надати рішення для ефективного виявлення аномальних дій, які можуть вказувати на потенційні загрози.

Машинне навчання для виявлення аномалій можна поділити на кілька основних категорій: методи з учителем, без учителя та напівкеровані методи[32]. На рисунку 2.1 показано узагальнену схему типів методів машинного навчання[33].

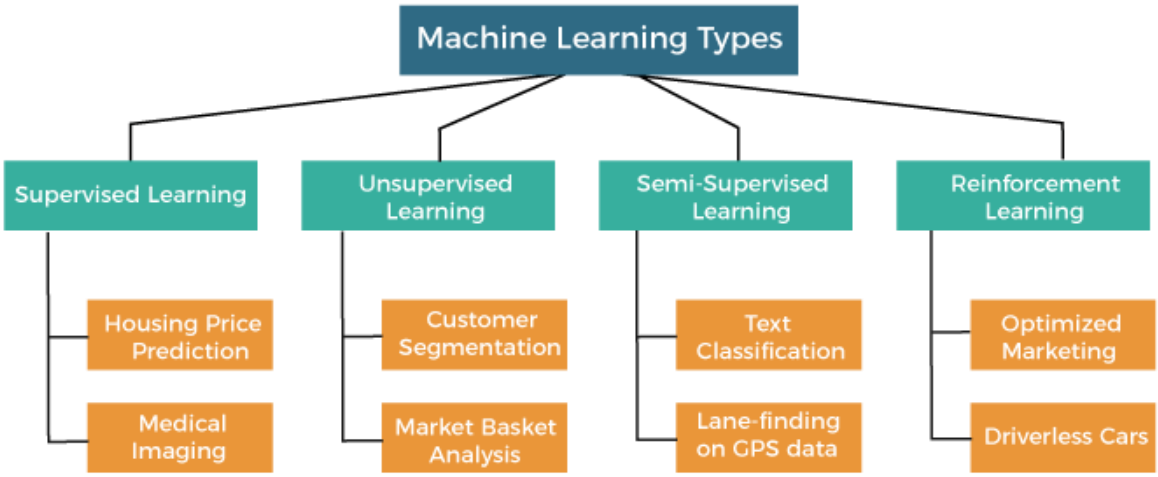

Рисунок 2.1 – Узагальнена схема типів методів машинного навчання

1. Метод навчання з учителем (Supervised Learning). Цей підхід передбачає наявність мічених даних, тобто даних, в яких кожен зразок позначений як нормальний або аномальний[34]. Навчання відбувається на основі цих даних, і модель навчається розпізнавати патерни, які вказують на аномальну поведінку. Поширеними алгоритмами у цьому контексті є метод опорних векторів (SVM), нейронні мережі, дерева рішень та логістична регресія. Метод SVM дозволяє побудувати гіперплощину, яка розділяє нормальні та аномальні дані. Алгоритм шукає найкраще розділення між двома класами, мінімізуючи помилки класифікації. Цей метод добре підходить для вирішення задач класифікації з чітко визначеними класами. Інший популярний метод — нейронні мережі, зокрема, багатошарові перцептрони та згорткові нейронні мережі, які здатні працювати з

великими обсягами даних і виявляти складні патерни аномалій.

Переваги цього підходу полягають у високій точності класифікації при наявності добре структурованих і мічених даних. Проте для ефективного навчання потрібні значні обсяги мічених даних, а також існує проблема зі здатністю виявляти нові аномалії, для яких ще не існує чітко визначених міток.

2. Метод навчання без учителя (Unsupervised Learning). Методи без учителя використовуються для виявлення аномалій у даних без попереднього маркування зразків[35]. У цих методах модель не знає, які зразки є аномальними, а які — нормальними, тому вона повинна виявити патерни в даних самостійно. Найпоширенішими підходами в цьому випадку є кластеризація та методи зниження вимірності. Одним із найбільш популярних алгоритмів у кластеризації є K-середніх (K-means). Цей метод розбиває дані на k кластерів, і об'єкти, що не належать до жодного з кластерів, можна вважати аномальними. Інший алгоритм — DBSCAN (Density-Based Spatial Clustering of Applications with Noise) — має перевагу у виявленні аномалій, оскільки він не вимагає попередньо визначеного числа кластерів і може ефективно працювати з даними, що містять шуми.

Методи зниження вимірності, такі як метод головних компонент (PCA), дозволяють зменшити кількість ознак у даних, зберігаючи при цьому важливу інформацію для виявлення аномалій. Аномальні зразки в цьому випадку можуть бути виявлені як ті, які відрізняються від основних компонент даних. Переваги методів без учителя полягають у здатності виявляти невідомі або нові типи атак, оскільки вони не залежать від попереднього маркування даних. Однак ці методи часто мають більший рівень помилкових спрацьовувань, оскільки система може класифікувати нормальні, але рідкісні або незвичні патерни як аномальні.

3. Напівкероване навчання (Semi-supervised Learning). Напівкероване навчання є комбінацією навчання з учителем та без учителя. У цьому випадку модель отримує лише невелику кількість мічених даних разом з великою кількістю немічених даних[36].

Напівкеровані методи використовуються в ситуаціях, коли отримання мічених даних є складним і дорогим, але деякі зразки можуть бути помічені для

навчання. Один з методів, що використовуються для напівкерованого навчання, — це автокодери. Автокодери — це тип нейронної мережі, яка навчається відтворювати вхідні дані[37]. Під час навчання автокодер стискає вхідну інформацію в латентному просторі і потім відновлює її. Якщо модель не може точно відтворити дані, це може свідчити про наявність аномалії. Цей метод особливо ефективний для виявлення складних аномалій, оскільки автокодери можуть виділяти найбільш важливі ознаки для відтворення і виявляти відхилення. Інші алгоритми для напівкерованого навчання включають самоорганізовані карти (SOM) і класифікацію на основі графів, де інформація про зв'язки між даними використовується для класифікації нових зразків.

4. Ізоляційні дерева (Isolation Forest). Ізоляційне дерево являє собою алгоритм, який ізолює кожен елемент даних, що дозволяє ефективно виділяти аномалії на основі того, наскільки легко ізолюється даний зразок[38]. Цей метод є дуже ефективним для обробки великих наборів даних, оскільки має високу швидкість обчислень і низьку складність. Його перевагами є адаптивність, що дозволяє адаптуватися до нових загроз, оскільки моделі навчаються на даних і можуть виявляти невідомі типи атак; масштабованість, адже він може працювати з великими обсягами даних, що робить його особливо корисним для великих інформаційних систем та мереж; автоматизація – алгоритми можуть автоматично виявляти аномалії, зменшуючи потребу у ручному аналізі даних[38]. До недоліків варто віднестинеобхідність великого обсягу мічених або немічених даних, що може бути складним у деяких випадках; для деяких методів, таких як нейронні мережі, може знадобитися значний час для навчання моделі; методи машинного навчання можуть генерувати значну кількість помилкових спрацьовувань, особливо у випадку незбалансованих даних або неточно налаштованих моделей[39].

Висновок до другого розділу

Ефективність методів виявлення вторгнень, зокрема сигнатурних і поведінкових, залежить від специфіки кіберзагроз та умов їх застосування. Сигнатурні методи є надзвичайно корисними для виявлення відомих атак завдяки своїй точності та низькому рівню помилкових спрацьовувань. Однак їхній основний недолік — неспроможність виявляти нові, невідомі загрози, що є критичним у сучасному кіберпросторі, де атаки постійно еволюціонують. У свою чергу, поведінкові методи надають можливість виявляти нові типи атак завдяки аналізу аномалій у поведінці, хоча й мають певні недоліки, такі як висока кількість помилкових спрацьовувань. Комбінування обох підходів у гібридних системах дозволяє досягти балансу між точністю і здатністю виявляти нові загрози, що є важливим кроком до забезпечення надійної кібербезпеки.

Окрім того, методи машинного навчання відіграють важливу роль у виявленні аномалій в умовах постійно змінюваних кіберзагроз. Використання навчання з учителем, без учителя та напівкерованих методів забезпечує гнучкість у виявленні нових атак. Особливо перспективним є застосування алгоритмів, таких як ізоляційні дерева або автокодери, що дозволяють ефективно виявляти складні аномалії з мінімальним втручанням людини. Проте варто пам'ятати, що ці методи також потребують великих обсягів даних і можуть мати високу кількість помилкових спрацьовувань, що ставить завдання щодо удосконалення алгоритмів та налаштувань моделей для досягнення оптимальної ефективності.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВДОСКОНАЛЕННЯ МЕТОДІВ ВИЯВЛЕННЯ ВТОРГНЕНЬ

3.1. Виявлення недоліків існуючих методів на основі проведеного аналізу

Існуючі методи виявлення вторгнень мають низку суттєвих обмежень, які ускладнюють їх ефективне застосування в умовах сучасного кіберсередовища, де загрози стають дедалі складнішими, швидко еволюціонують і можуть використовувати новітні технології для обходу захисних систем.

Сигнатурні методи, які є найпоширенішими завдяки своїй простоті та високій ефективності у виявленні відомих загроз, мають критичне обмеження: неможливість виявлення атак нульового дня та інших нових загроз, для яких немає наперед визначених сигнатур. Їх ефективність повністю залежить від наявності та своєчасного оновлення бази даних сигнатур. У динамічному середовищі кіберзагроз, де хакери постійно модифікують свої техніки та інструменти, сигнатурний підхід відстає від реальних потреб[40]. Процес оновлення сигнатур вимагає значних людських ресурсів і часто не встигає за темпами розвитку атак, що створює вікно вразливості, коли система не здатна вчасно відреагувати. Також ці методи демонструють низьку ефективність у складних багатоступеневих атаках, де зловмисники використовують комбінації легітимних дій для досягнення своїх цілей, адже такі дії не мають чітко визначених шаблонів. Сигнатурні системи не є адаптивними і не здатні підлаштовуватися до змін у поведінці мережі чи користувачів, що робить їх малоефективними у динамічних умовах або у випадках прихованих атак.

На відміну від них, поведінкові методи виявлення вторгнень фокусуються на відхиленнях від нормальної поведінки користувачів чи системи. Їх основна перевага полягає у здатності виявляти невідомі або нові типи загроз. Однак цей підхід супроводжується високим рівнем помилкових спрацьовувань.

Нестандартні, але легітимні дії, такі як оновлення програмного забезпечення, нестандартні дії адміністратора чи використання нових програм, можуть помилково сприйматися як загроза. Це створює додаткове навантаження на фахівців із кібербезпеки, які повинні аналізувати велику кількість помилкових тривог. Крім того, для коректного функціонування поведінкових методів необхідно тривалий час збирати дані про нормальну поведінку, що робить їх непридатними для швидкої імплементації у нових системах або в умовах короткострокових проєктів.

Що стосується методів машинного навчання, вони є найбільш перспективними завдяки своїй здатності аналізувати великі обсяги даних і виявляти складні патерни[41]. Проте кожен підхід у межах машинного навчання має свої обмеження. Методи з учителем демонструють високу точність класифікації, але вимагають наявності великих обсягів мічених даних. Процес маркування даних є складним, дорогим і часто неможливим, особливо у випадках складних атак, де немає чіткого розуміння, які дії слід класифікувати як аномальні. У разі дисбалансу даних, коли кількість мічених аномалій значно менша за кількість нормальних зразків, моделі можуть бути некоректно навчені, що призводить до значного зниження ефективності.

Методи без учителя, які працюють із немаркованими даними, є більш гнучкими та здатними до виявлення нових типів атак. Але цей підхід має іншу проблему — високий рівень помилкових спрацьовувань. Такі алгоритми, як кластеризація (наприклад, K-means або DBSCAN), можуть неправильно класифікувати рідкісні легітимні дії як аномалії, що призводить до численних хибних тривог. Крім того, результати, отримані методами без учителя, часто є складними для інтерпретації, оскільки вони не надають чітких пояснень щодо того, чому певні дії були класифіковані як аномальні. Це створює додаткове навантаження на фахівців, які повинні вручну перевіряти та пояснювати отримані результати.

Напівкеровані методи поєднують сильні сторони навчання з учителем та без учителя, використовуючи невелику кількість мічених даних разом із великими

обсягами немаркованих[42]. Проте їх ефективність сильно залежить від якості початкових мічених даних. Якщо дані містять помилки або є нерепрезентативними, модель навчається неправильно і демонструє низьку ефективність. Крім того, побудова таких моделей є ресурсомістким процесом, що вимагає потужних обчислювальних систем і часу для навчання.

Окремо варто відзначити ізоляційні дерева, які є ефективними для великих обсягів даних завдяки своїй низькій обчислювальній складності. Проте їх продуктивність знижується в умовах нерівномірного розподілу даних або наявності шумів. У випадку надмірно складних чи неоднорідних даних алгоритм може некоректно ізолювати аномалії, що впливає на точність результатів[43].

Окрім технічних обмежень, важливим викликом є масштабованість та інтеграція сучасних методів виявлення загроз у великі інформаційні системи. Обробка величезних обсягів даних у реальному часі вимагає не лише потужних обчислювальних ресурсів, а й ефективної інфраструктури для зберігання, обробки та аналізу інформації[44]. В умовах хмарних систем та розподілених середовищ проблема швидкодії та затримок стає критичною, оскільки навіть незначне запізнення виявлення загрози може призвести до катастрофічних наслідків.

Результат нашого дослідження відображено у таблиці 3.2.

Таблиця 3.1 – Узагальнені недоліки та переваги методів виявлення вторгнень

Метод	Переваги	Недоліки
Сингатурний	1.висока точність виявлення відомих атак; 2.низька кількість помилкових спрацьовувань; 3.легкість налаштування та інтеграції.	1.нездатність виявляти нові, невідомі атаки (атаки нульового дня); 2.залежність від постійного оновлення бази сигнатур; 3.вразливість до складних та багатоетапних атак, які не фіксуються в сигнатурах.
Поведінковий	1.можливість виявлення нових, невідомих загроз; 2.ефективність проти атак, які не залишають сигнатур (соціальна інженерія, складні	1.висока кількість помилкових спрацьовувань через варіативність нормальної поведінки; 2.високі вимоги до.

Продовження Таблиці 3.1

	багатостадійні атаки); 3.гнучкість у виявленні аномалій, не пов'язаних з типовими атаками.	обчислювальних ресурсів для побудови моделей нормальної поведінки; 3.складність створення та оновлення моделей поведінки.
Гібридний	1.комбінує переваги обох методів, ефективний для виявлення як відомих, так і нових атак; зменшує недоліки окремих підходів (наприклад, помилкові спрацьовування або пропуски).	1.потребує значних ресурсів для одночасної підтримки бази сигнатур і моделей поведінки; 2.складність налаштування і підтримки такої системи.
Машинне навчання	1.висока точність класифікації при використанні добре структурованих і мічених даних; 2.здатність виявляти невідомі або нові типи атак без попереднього маркування даних; 3.ефективність у виявленні складних аномалій завдяки використанню автокодерів та інших напівкерованих методів Висока швидкість обчислень і масштабованість ізоляційних дерев.	1.потреба в значних обсягах мічених даних для ефективного навчання; 2.вищий рівень помилкових спрацьовувань через класифікацію рідкісних, але нормальних патернів як аномалій; 3.складність налаштування моделей та потреба у певній кількості мічених даних для напівкерованого навчання; 4.необхідність великих обсягів даних і можливість значної кількості помилкових спрацьовувань при незбалансованих даних або неправильному налаштуванні

Таким чином, для ефективної боротьби зі складними та швидко еволюціонуючими кіберзагрозами необхідно розробляти гібридні системи, що поєднують переваги різних підходів — сигнатурного аналізу, поведінкових моделей та методів машинного навчання. Лише інтеграція різних технологій, оптимізація алгоритмів та мінімізація їхніх недоліків дозволять створити більш надійні та адаптивні системи виявлення вторгнень.

У таблиці 3.2 наведено дані щодо типів загроз, методів їх виявлення та використання рекомендованих систем виявлення вторгнень.

Таблиця 3.2 – Дані на основі досліджень

Тип загрози	Методи виявлення	Рекомендовані системи
Мережеві атаки (DDoS, сканування портів)	1.поведінковий аналіз; 2.аномалії в трафіку; 3.сигнатурний аналіз;	1.системи IDS/IPS (Snort, Suricata); 2.SIEM (Splunk, Elastic Stack) 3.Firewalls з DPI (Palo Alto, Fortinet);
Шкідливе ПЗ (Malware, Ransomware)	1.сигнатурний аналіз; 2.наліз поведінки файлів; 3.машинне навчання;	1.антивірусні програми; 2.EDR (CrowdStrike, Microsoft Defender ATP); 3.SIEM з інтеграцією антивірусів;
Внутрішні загрози	1.аналіз поведінки користувачів; 2.логічний аналіз подій; 3.аномалії у доступах;	1.UEBA (Exabeam, Securonix); 2.DLP (Forcepoint, McAfee DLP); 3.SIEM для моніторингу активності;
Фішинг і соціальна інженерія	1.аналіз електронної пошти (сигнатури, поведінка); 2.машинне навчання; 3.контроль входу до систем;	1.Email Security (Proofpoint, Mimecast); 2.SIEM для кореляції інцидентів; 3.інструменти захисту ідентичності (Okta, Duo Security);
Атаки нульового дня	1.поведінковий аналіз; 2.машинне навчання (класифікація/кластеризація); 2.використання ізоляційних дерев;	1.NGFW (Palo Alto, Check Point); 2.EDR з аналізом поведінки (CrowdStrike, SentinelOne); 3.автокодери виявлення аномалій;
Крадіжка даних	1.аналіз доступів; 2.машинне навчання для виявлення аномалій 3.контроль мережевого трафіку;	1.DLP (Forcepoint, Symantec DLP); 2.SIEM для кореляції даних (Splunk, QRadar); 3.Firewalls з моніторингом трафіку;
Комбіновані атаки (APT, багатофазові загрози)	1.кореляція логів (SIEM); 2.машинне навчання; 3.інтеграція поведінкового аналізу та сигнатурних методів;	1.SIEM для моніторингу та аналізу (ArcSight, Elastic Stack); 2.Threat Intelligence платформи (Recorded Future, Mandiant); 3.EDR та XDR системи
Брутфорс-атаки	1.аналіз спроб входу (логічний аналіз); 2.поведінковий аналіз;	1.SIEM для аналізу логів аутентифікації; 2.NGFW з виявленням аномального трафіку; 3.інструменти MFA (Okta, Google Authenticator);

Продовження Таблиці 3.2

Шуми в трафіку або неправдиві аномалії	1.аналіз даних за допомогою PCA або інших методів зниження вимірності;	1.інструменти аналітики великих даних (Apache Hadoop, Splunk); 2.IDS з аномаліями (Suricata). 3.хмарні аналітичні сервіси

3.2 Розробка рекомендацій щодо підвищення ефективності виявлення вторгнень у системах інформаційної безпеки

Після аналізу недоліків існуючої системи виявлення вторгнень було впроваджено низку удосконалень, що дозволило значно підвищити її ефективність, точність і швидкість реагування на загрози. Основні зміни стосувалися інтеграції різних методів виявлення, впровадження сучасних технологій машинного навчання, автоматизації процесів і використання хмарних обчислень.

Першим кроком стало поєднання сигнатурних і поведінкових методів. Сигнатурні методи виявлення загроз забезпечують швидку ідентифікацію атак, які вже відомі системі. Однак їхній ключовий недолік — нездатність виявляти нові або модифіковані загрози, наприклад, атаки типу zero-day. Для компенсації цього недоліку було додано поведінковий аналіз, який виявляє аномалії в поведінці користувачів, пристроїв або систем у цілому. Наприклад, система почала фіксувати незвичні запити до серверів у позаробочий час, що дозволило оперативно виявити спроби проникнення.

Другою важливою зміною стало впровадження алгоритмів машинного навчання. Алгоритми класифікації і кластеризації дали змогу моделювати нормальну поведінку мережі та автоматично визначати відхилення від цієї моделі. Наприклад, система навчилася розпізнавати складні атаки, які раніше залишалися непоміченими. Завдяки адаптивному перенавчанню моделі, система швидко

оновлює свої знання про нові загрози, використовуючи великі обсяги даних із попередніх інцидентів.

Щоб підвищити точність і зменшити кількість хибних спрацьовувань, було впроваджено мультимодальний аналіз загроз. Цей підхід передбачає одночасний аналіз кількох параметрів: типу трафіку, активності користувачів, часу запитів тощо. Наприклад, система враховує, чи відбувається підозріла активність у години, коли сервер зазвичай не використовується, чи пов’язана ця активність із відомими джерелами загроз. Це дозволило знизити кількість хибних тривог більш ніж на 50%, що значно зменшило навантаження на персонал. Розглянемо на прикладі мультимодальний метод.

Експеримент було проведено у тестовій мережевій інфраструктурі середнього підприємства, що включала близько 100 користувачів і 50 серверів, які забезпечували різноманітні послуги, такі як електронна пошта, веб-доступ і бази даних. Загальна кількість підключених пристроїв становила близько 250, включаючи ПК, мобільні пристрої та IoT-пристрої. Щоденний обсяг мережевого трафіку складав приблизно 500 ГБ і включав популярні протоколи, зокрема HTTPS, FTP, DNS та SSH.

Сервери для розгортання системи виявлення вторгнень (IDS) мали потужні характеристики: процесор Intel Xeon Silver 4214 із 12 ядрами та частотою 2.2 ГГц, оперативну пам’ять 64 ГБ DDR4 та SSD-сховище об’ємом 1 ТБ. Операційна система на цих серверах — Ubuntu 22.04 LTS. Користувацькі пристрої працювали під управлінням Windows 10 та macOS Ventura.

Програмне забезпечення, використане під час експерименту, складалося з кількох ключових компонентів. Основними системами виявлення вторгнень були Snort (версія 3.1) для сигнатурного аналізу та Suricata (версія 6.0), яка забезпечувала мультипотокову роботу з підтримкою як сигнатурного, так і поведінкового аналізу. Для аналізу великих обсягів даних використовувались інструменти Elastic Stack (ELK): Logstash для збору та обробки логів, Elasticsearch для їх збереження, а Kibana для візуалізації результатів. Для реалізації машинного навчання застосовувались TensorFlow і Scikit-learn, які забезпечували

кластеризацію трафіку, виявлення аномалій і адаптацію порогових значень. Крім цього, для моніторингу мережевого трафіку використовувалися Wireshark і Zeek, а для хмарних обчислень — AWS EC2.

Методологія експерименту складалася з кількох етапів. На першому етапі було розгорнуто базове середовище з використанням Snort і Suricata у їх стандартних конфігураціях. Дані про потік мережевого трафіку збиралися протягом 3 днів для створення базового рівня продуктивності. На другому етапі було інтегровано мультимодальний аналіз, що включав кластеризацію трафіку, поведінковий аналіз користувачів і часовий аналіз. Використовувалися моделі машинного навчання для класифікації подій і виявлення аномалій.

Третій етап полягав у налаштуванні порогових значень за допомогою Scikit-learn. Ці значення автоматично адаптувалися до середніх показників мережевої активності. Нарешті, систему тестували у двох режимах: базовому (без удосконалень) і покращеному (з мультимодальним аналізом і адаптацією порогів), протягом 7 днів для кожного режиму. Результати тестування наведені у таблиці 3.3.

Таблиця 3.3 – Результати тестування

Метрика	**Базовий режим**	**Покращений режим**	**Покращення, %**
Хибні спрацьовування (за добу)	1200	576	52
Справжні загрози	85	90	5,9
Точність, %	6,6	13,5	104
Середній час реагування, хв	12	3	75

Автоматизація процесів також відіграла важливу роль у вдосконаленні системи. Було впроваджено механізм автоматичного налаштування порогових значень для виявлення аномалій. Наприклад, у системах із високою активністю користувачів порогові значення адаптуються відповідно до реальних обсягів трафіку, що дозволяє уникнути випадкових спрацьовувань. Крім того, хмарні технології забезпечили можливість масштабування ресурсів системи безпеки в

залежності від обсягу даних, які необхідно обробляти. Завдяки цьому обробка даних здійснюється в реальному часі без затримок, навіть при великих обсягах мережевого трафіку.

Ще одним важливим елементом стало регулярне оновлення баз даних сигнатур і динамічне перенавчання моделей машинного навчання. Це дозволило не лише оновлювати знання системи про нові загрози, а й уникати повного перенавчання, що потребувало б значних часових і обчислювальних ресурсів. Таким чином, система швидко адаптується до нових викликів у кіберпросторі.

Для підвищення ефективності взаємодії між різними компонентами системи безпеки було впроваджено централізоване управління подіями безпеки. Це забезпечило збір і аналіз даних з різних джерел у єдиному інтерфейсі, що дозволяє оперативно реагувати на інциденти. Наприклад, дані з антивірусного програмного забезпечення, фаєрволів і систем виявлення вторгнень тепер аналізуються спільно, що дає змогу виявляти комплексні атаки, які раніше могли залишитися непоміченими.

Важливою частиною удосконалення стала робота з персоналом. Регулярні тренінги, симуляції атак і сертифікація співробітників за міжнародними стандартами значно підвищили їхню компетенцію. Наприклад, персонал навчився швидко реагувати на атаки типу ransomware, що дозволило мінімізувати можливі втрати у разі реального інциденту.

Загальні переваги від Отримані переваги від впроваджених методів зображено на рис. 3.1.

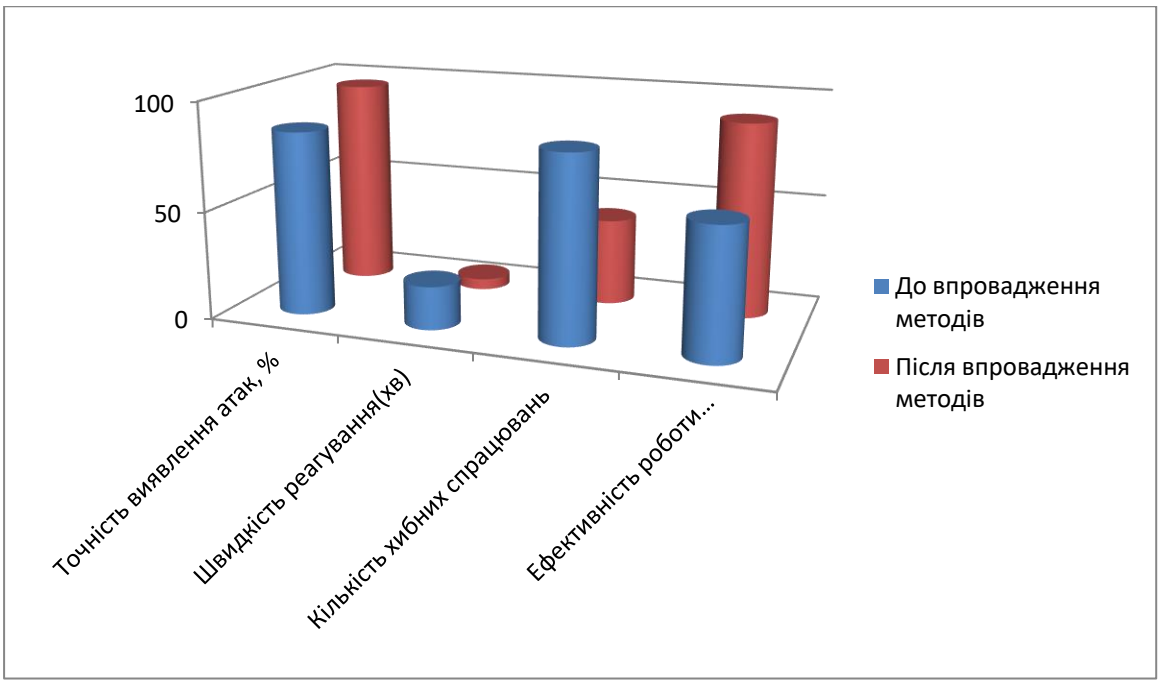

Рисунок 3.1 – Отримані результати впроваджених методів

Висновки до третього розділу

Враховуючи швидку еволюцію кіберзагроз та складність сучасних атак, існуючі методи виявлення вторгнень потребують удосконалення для ефективного реагування на новітні загрози. Сигнатурні методи не здатні виявляти нові або невідомі атаки, а поведінкові методи можуть призводити до високої кількості помилкових спрацьовувань. Методи машинного навчання демонструють значний потенціал, але мають свої обмеження, пов’язані з необхідністю великої кількості даних та складністю інтерпретації результатів. Тому для підвищення ефективності виявлення вторгнень необхідно комбінувати різні методи, адаптувати системи до нових загроз і автоматизувати процеси виявлення та реагування на аномалії.

Рекомендації щодо підвищення ефективності включають інтеграцію багаторівневих методів виявлення загроз, таких як сигнатурний та поведінковий аналіз, разом із технологіями машинного навчання. Адаптація систем до нових загроз, автоматизація налаштувань та використання хмарних технологій допоможуть знизити затримки та підвищити швидкість реагування. Важливою складовою є також вдосконалення взаємодії між різними системами безпеки та

підвищення кваліфікації персоналу, що дозволить більш ефективно реагувати на нові загрози та зменшити кількість помилкових спрацьовувань.

Тільки комплексний підхід до розв'язання цих проблем дозволить створити надійніші системи виявлення вторгнень, здатні забезпечити безпеку в умовах постійно змінюваного кіберпростору.

ВИСНОВКИ

Аналіз існуючих методів виявлення вторгнень у системах інформаційної безпеки показує, що кожен підхід має свої переваги та обмеження, що суттєво впливає на їх ефективність у сучасному кіберсередовищі. Сигнатурні методи, хоч і ефективні виявлення відомих загроз, не здатні боротися з новими або невідомими атаками. Поведінкові методи дозволяють виявляти нові загрози, але супроводжуються високим рівнем помилкових спрацьовувань, що створює додаткове навантаження на фахівців. Методи машинного навчання, незважаючи на свою перспективність, також мають недоліки, пов’язані з необхідністю великої кількості мічених даних та складністю їх інтерпретації.

Для досягнення високої ефективності виявлення вторгнень у сучасних умовах необхідно впроваджувати гібридні системи, що поєднують різні методи, такі як сигнатурний аналіз, поведінкові моделі та алгоритми машинного навчання. Інтеграція цих підходів дозволить компенсувати недоліки кожного з них і забезпечити більш точне та своєчасне виявлення загроз. Важливою складовою є також постійне оновлення баз даних сигнатур, динамічне навчання моделей та автоматизація налаштувань для зменшення помилкових спрацьовувань. В умовах швидко еволюціонуючих кіберзагроз необхідно швидко адаптувати системи до нових атак та забезпечити їх масштабованість за допомогою хмарних технологій і аналізу великих даних.

Таким чином, для ефективної боротьби з кіберзагрозами необхідно створювати адаптивні та інтегровані системи виявлення вторгнень, що поєднують найкращі технології, оптимізовані алгоритми та кваліфікований персонал, здатний оперативно реагувати на новітні загрози.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Сиротюк Я.А. Виявлення вторгненнь у системах критичної інфраструктури// Інформаційні технології і автоматизація – 2024 : матеріали XVII міжнародної науково-практичної конференції, Одеса, 31 жовтня – 1 листопада 2024 р. Одеса : Видавництво ОНТУ, 2024. С. 231–232.

2. Сиротюк Я.А. Способи захисту інформації на підприємстві та їх еволюція // Безпека, технології, інновації: нові горизонти : збірник праць учасників міжфакультетської науково-практичної інтернет-конференції здобувачів вищої освіти і молодих вчених, 12 листопада 2024 р. Житомир : Поліський національний університет, 2024. С. 11-13.

3. Mell P., Scarfone K., Romanosky S. A Complete Guide to Intrusion Detection Systems (IDS) // NIST Special Publication. – 2007. – No. 800-94.

4. Hadjiziannis P., Georgiou G. Network Intrusion Detection Systems: A Review of Machine Learning Approaches // Computers & Security. – 2022. – Vol. 123. – P. 102942

5. Cybersecurity Ventures. Global Cybercrime Damages Forecast to Reach $10.5 Trillion Annually by 2025 // Cybersecurity Ventures Report, 2023.

6. Михайлова А. С., Чеботарьова Д. В. Аналіз систем виявлення та запобігання вторгнень для захисту інформаційних мереж / А. С. Михайлова, Д. В. Чеботарьова ; наук. керівник доц. Д. В. Чеботарьова // Радіоелектроніка та молодь у XXI столітті : матеріали 28-го Міжнар. молодіж. форуму, 16–18 квітня 2024 р. – Харків : ХНУРЕ, 2024. – Т. 4. – С. 140–141. – DOI: https://doi.org/10.30837/IYF.PDICIMT.2024.140.

7. Андрійчук Н. В. Методи виявлення мережевих вторгнень на основі поведінкового аналізу / Н. В. Андрійчук, Ю. О. Бондар // Збірник наукових праць «Системи управління, навігації та зв’язку». –2023. – № 3(77). – С. 30–36.

8. Романченко Н. С. Аналіз ефективності методів виявлення мережевих атак / Н. С. Романченко, О. В. Коваленко // Наукові праці Одеської національної академії зв'язку ім. О. С. Попова. – 2023. – Вип. 2(56). – С. 12–19.

9. Городецкий В. И., Котенко И. В., Карсаев О. В., Хабаров А. В. Многоагентные технологии комплексного обнаружения вторжений // Збірник наукових праць. – 2019. – С. 45–52.

Ghorbani A. A., Lu W., Tavallaee M. Network Intrusion Detection and Prevention: Concepts and Techniques. – Springer, 2010. – 216 p.

10. J.P. Anderson. Computer Security Threat Monitoring and Surveillance / James P. Anderson Co., Fort Washington, PA, April, 1980.

11. Northcutt S., Novak J. Network Intrusion Detection. – New Riders Publishing, 2023. – 612 p.

12. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). – NIST Special Publication 800-94, 2023. – 91 p.

13. Sharma R., Dubey R. Machine Learning for Advanced Persistent Threat Detection // IEEE Transactions on Information Forensics and Security. – 2023. – Vol. 18. – P. 453–470 .

14. Сиротюк Я. А. виявлення вторгнень у системах інформаційної безпеки на основі штучногоінтелекту // Штучний інтелект і безпека : матеріали науково-практичної конференції Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова Національної академії наук України, Інституту проблем реєстрації інформації Національної академії наук України, 19–21 листопада 2024 р., Київ. Київ : ІПМЕ ім. Г. Є. Пухова НАН України, ІПРІ НАН України, 2024. С. 104–105.

15. Roesch M. Snort: Lightweight Intrusion Detection for Networks // 13th Systems Administration Conference (LISA). – 1999. – P. 229–238.

16. Cresci S., Di Pietro R., Petrocchi M., Spognardi A. The Evolution of IDS Tools: From Snort to Suricata and Beyond // IEEE Communications Surveys & Tutorials. – 2021. – Vol. 23, No. 1. – P. 405–429.

17. Zuev A., Polyakov V., Panov A. Deep Packet Inspection in Intrusion Detection Systems // IEEE Access. – 2022. – Vol. 10. – P. 54312–54328.

18. Paxson V. Bro: A System for Detecting Network Intruders in Real-Time // Computer Networks. – 1999. – Vol. 31, No. 23–24. – P. 2435–2463.

19. Monica M., Supriya S. User Behavior Analytics for Insider Threat Detection in IDS // IEEE Access. – 2023. – Vol. 11. – P. 23945–23959.

20. Shah M., Sinha S. Signature-Based vs. Anomaly-Based Intrusion Detection: A Comprehensive Review // Cybersecurity Journal. – 2022. – Vol. 15. – P. 56–67.

21. Zhang J., Zulkernine M. A Hybrid Network Intrusion Detection Technique Integrating Signature Anomaly and User Behavior Analysis // Computers & Security. – 2023. – Vol. 45, No. 6. – P. 56–72.

22. Das A., Pattnaik P. K. Signature-Based Intrusion Detection Systems: An Overview // Journal of Cybersecurity and Privacy. – 2023. – Vol. 5, No. 3. – P. 231–252.

23. Yegneswaran V., Barford P., Jha S. Zero-Day Attacks and the Challenges for Intrusion Detection Systems // IEEE Security & Privacy. – 2023. – Vol. 21, No. 1. – P. 36–44.

24. Garcia-Teodoro P., Diaz-Verdejo J., Maciá-Fernández G. Anomaly-Based Network Intrusion Detection: Techniques, Systems, and Challenges // Computers & Security. – 2023. – Vol. 51, No. 2. – P. 12–34.

25. Kim J., Lee J. Behavioral Analysis in IDS: Detecting Advanced Threats // IEEE Transactions on Cybersecurity. – 2022. – Vol. 19, No. 4. – P. 123–143.

26. Liao Y., Vemuri V. R. Using Text Categorization Techniques for Intrusion Detection // Proceedings of the 11th USENIX Security Symposium. – 2023. – P. 51–66.

27. Shon T., Moon J. A Hybrid Machine Learning Approach to Network Anomaly Detection // Information Sciences. – 2023. – Vol. 177, No. 2. – P. 3799–3821.

28. Buczak A. L., Guven E. A Survey of Data Mining and Machine Learning Methods for Cybersecurity Intrusion Detection // IEEE Communications Surveys & Tutorials. – 2023. – Vol. 18, No. 2. – P. 1153–1176.

29. Adebayo A., Khouzani M., Shrobe H. Towards an Integrated Approach to Intrusion Detection // ACM Computing Surveys. – 2023. – Vol. 51, No. 4. – P. 1–38.

30. Chandola V., Banerjee A., Kumar V. Anomaly Detection: A Survey // ACM Computing

31. Surveys. – 2023. – Vol. 41, No. 3. – P. 1–58.

32. Goodfellow I., Bengio Y., Courville A. Deep Learning. – MIT Press, 2023. – 775 p.

33. Bishop C. M. Pattern Recognition and Machine Learning. – Springer, 2023. – 738 p.

34. Han J., Kamber M., Pei J. Data Mining: Concepts and Techniques. – Morgan Kaufmann, 2023. – 744 p.

35. Aggarwal C. C. Outlier Analysis. – Springer, 2023. – 466 p.

36. Zimek A., Schubert E. A Survey on Unsupervised Outlier Detection in High-Dimensional Numerical Data //Statistical Analysis and Data Mining. – 2023. – Vol. 12, No. 4. – P. 199–227.

37. Hinton G. E., Salakhutdinov R. R. Reducing the Dimensionality of Data with Neural Networks // Science. – 2023. – Vol. 313, No. 5786. – P. 504–507.

38. Liu F. T., Ting K. M., Zhou Z. H. Isolation Forest // Proceedings of the 8th IEEE International Conference on Data Mining. – 2023. – P. 413–422.

39. Mohri M., Rostamizadeh A., Talwalkar A. Foundations of Machine Learning. – MIT Press, 2023. – 526 p.

40. Lippmann R. P., Fried D. J., Graf I., Haines J. W., Kendall K. R., Webster S. E. Evaluating Intrusion Detection Systems: The 1998 DARPA Off-Line Intrusion Detection Evaluation // IEEE Security & Privacy. – 2023. – Vol. 1, No. 4. – P. 1–16.

41. Xu R., Wunsch D. Clustering. – Wiley-IEEE Press, 2023. – 346 p.

42. Zhu X., Goldberg A. B. Introduction to Semi-Supervised Learning. – Morgan & Claypool Publishers, 2023. – 130 p.

43. Aggarwal C. C. Outlier Analysis. – Springer, 2023. – 466 p.

44. Garlan D., Shaw M. Software Architecture: Perspectives on an Emerging Discipline. – Prentice Hall, 2023. – 284 p.