МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЕКОНОМІЦІ

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

Галузь знань: 12 «Інформаційні технології»
Спеціальність 125 «Кібербезпека»

Форма здобуття освіти: очна (денна)

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему **«РОЗРОБКА АДАПТИВНИХ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ ГІБРИДНИМИ МЕТОДАМИ»**

здобувача Параніна Ігоря Едуардовича _____

Науковий керівник: к.т.н., доц. Кулініч О.М._____

Робота допущена до захисту перед екзаменаційною комісією з атестації здобувачів вищої освіти (ЕК)

Завідувач кафедри: д.ф.-м.н., професор Джалладова І.А.
_____

Київ 2026

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАДИМА ГЕТЬМАНА

ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЕКОНОМІЦІ

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

Галузь знань: 12 «Інформаційні технології»

Спеціальність 125 «Кібербезпека»

ПОГОДЖЕНО
Керівник проєктної групи (гарант)
освітньо-професійної програми

А.В. Бегун

2026 р.

ЗАТВЕРДЖУЮ
Завідувач кафедри

Джалладова І.А.

2026 р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

здобувача вищої освіти Параніна Ігоря Едуардовича

очної (денної) форми здобуття освіти

на підготовку кваліфікаційної бакалаврської роботи

на тему **«РОЗРОБКА АДАПТИВНИХ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ ГІБРИДНИМИ МЕТОДАМИ»**

Тему затверджено наказом ректора Університету від «___» _____ 2026 р .№ ___-ст

Кваліфікаційна бакалаврська робота виконується на матеріалах

План кваліфікаційної бакалаврської роботи

Розділ 1	**ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ СИСТЕМ ВИЯВЛЕННЯ**
(назва розділу)	
Розділ 2	**МОДЕЛЮВАННЯ АДАПТИВНОЇ IDS НА ОСНОВІ ГІБРИДНИХ МЕТОДІВ**
(назва розділу)	
Розділ 3	**РОЗРОБКА ТА РЕАЛІЗАЦІЯ АДАПТИВНОЇ ГІБРИДНОЇ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ**
(назва розділу)	

Об'єкт дослідження:	процес виявлення вторгнень у комп'ютерних мережах на основі аналізу мережевого трафіку
Предмет дослідження:	методи, моделі та алгоритми побудови адаптивних систем виявлення вторгнень на основі гібридних методів
Мета кваліфікаційної бакалаврської роботи:	розробка адаптивної системи виявлення вторгнень на основі гібридних методів з метою підвищення ефективності виявлення кіберзагроз, зменшення кількості хибних спрацювань і забезпечення своєчасного реагування на сучасні атаки

Конкретні завдання, які здобувач повинен виконати для досягнення поставленої мети:

У розділі 1	**ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ**
Дослідити історію виникнення та еволюцію систем виявлення вторгнень; визначити поняття, сутність та місце систем виявлення вторгнень у системі кібербезпеки; дослідити класифікацію систем виявлення вторгнень та їх архітектуру.	

У розділі 2	**МОДЕЛЮВАННЯ АДАПТИВНОЇ IDS НА ОСНОВІ ГІБРИДНИХ МЕТОДІВ**
Дослідити принципи адаптивності в IDS; розглянути можливості застосування гібридних методів у кібербезпеці; формалізувати задачу виявлення вторгнень як задачу класифікації та виявлення аномалій; розробити гібридну модель адаптивної IDS.	

У розділі 3	**РОЗРОБКА ТА РЕАЛІЗАЦІЯ АДАПТИВНОЇ ГІБРИДНОЇ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ**
Реалізувати алгоритм функціонування розробленої адаптивної гібридної системи виявлення вторгнень; сформувати експериментальне середовище та підготовку даних мережевого трафіку для задачі виявлення вторгнень.	

Завдання підготував науковий керівник _____ _____

(підпис) *(ініціали, прізвище)*

«_____» _____ 2026 р.

Завдання одержав здобувач _____

(підпис) *(ініціали, прізвище)*

«_____» _____ 2026 р.

Реферат

Кваліфікаційна бакалаврська робота містить **103 сторінки**, **4 таблиці**, **34 рисунки**, список використаних джерел з **92 найменування**.

Тема: «Розробка адаптивних систем виявлення вторгнень гібридними методами»

Об'єктом дослідження є процес виявлення вторгнень у комп'ютерних мережах на основі аналізу мережевого трафіку.

Предмет дослідження – методи, моделі та алгоритми побудови адаптивних систем виявлення вторгнень на основі гібридних методів.

Мета кваліфікаційної бакалаврської роботи – розробка адаптивної системи виявлення вторгнень на основі гібридних методів з метою підвищення ефективності виявлення кіберзагроз, зменшення кількості хибних спрацювань і забезпечення своєчасного реагування на сучасні атаки. Для досягнення поставленої мети визначено такі **завдання**:

- дослідити історію виникнення та еволюцію систем виявлення вторгнень;
- визначити поняття, сутність та місце систем виявлення вторгнень у системі кібербезпеки;
- дослідити класифікацію систем виявлення вторгнень та їх архітектуру;
- дослідити принципи адаптивності в IDS;
- розглянути можливості застосування гібридних методів у кібербезпеці;
- формалізувати задачу виявлення вторгнень як задачу класифікації та виявлення аномалій;
- розробити гібридну модель адаптивної IDS;
- реалізувати алгоритм функціонування розробленої адаптивної гібридної системи виявлення вторгнень;
- сформувати експериментальне середовище та підготовку даних мережевого трафіку для задачі виявлення вторгнень.

У процесі виконання роботи використано загальнонаукові **методи** (аналіз, синтез, порівняння, узагальнення), методи математичного та алгоритмічного моделювання, методи кластерного аналізу і класифікації, а також методи статистичної обробки результатів обчислювального експерименту.

Теоретична і методична значущість отриманих результатів полягає у розвитку підходів до побудови адаптивних гібридних систем виявлення вторгнень на основі поєднання сигнатурного аналізу, методів машинного навчання та поведінкового аналізу мережевого трафіку. У роботі узагальнено сучасні підходи до виявлення кіберзагроз, обґрунтовано доцільність використання гібридної архітектури та запропоновано методику аналізу й обробки мережевих даних для підвищення точності виявлення атак. Отримані результати можуть бути

використані як теоретична та методична основа для подальших досліджень у сфері інтелектуальних систем кібербезпеки, а також для вдосконалення методів аналізу та класифікації мережевого трафіку.

Практичне значення отриманих результатів полягає у розробці прототипу адаптивної гібридної системи виявлення вторгнень, яка може застосовуватися для підвищення рівня кіберстійкості інформаційних систем підприємств і державних установ. Запропонована модель також може використовуватися для дослідження та тестування нових методів виявлення вторгнень, а також для зменшення кількості хибних спрацювань у процесі аналізу мережевого трафіку. Крім того, результати роботи створюють основу для подальших наукових досліджень у сфері адаптивних і гібридних систем кібербезпеки.

Ключові слова: кібербезпека, кіберзагрози, кіберзахист, мережевий трафік, системи виявлення вторгнень, методи кластерного аналізу, сигнатурний аналіз, аномалії, адаптивна гібридна система, гібридні системи виявлення вторгнень

Рік виконання кваліфікаційної бакалаврської роботи – 2026.

Рік захисту роботи – 2026

ВІДГУК

на кваліфікаційну бакалаврську роботу

студента Параніна Ігоря Едуардовича гр. ІК-402

на тему: **«РОЗРОБКА АДАПТИВНИХ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ ГІБРИДНИМИ МЕТОДАМИ»**

Актуальність теми. Актуальність теми кваліфікаційної бакалаврської роботи обумовлена стрімким розвитком інформаційно-комунікаційних технологій, постійним зростанням обсягів мережевого трафіку та ускладненням сучасних кіберзагроз. Особливого значення питання забезпечення кібербезпеки набули в умовах воєнної агресії проти України, коли об'єктами кібератак дедалі частіше стають державні інформаційні ресурси, об'єкти критичної інфраструктури та корпоративні мережі.

Сучасні системи виявлення вторгнень не завжди здатні ефективно протидіяти новим і модифікованим типам атак, що зумовлює необхідність пошуку нових підходів до забезпечення кіберзахисту. У цьому контексті особливий науковий і практичний інтерес становлять адаптивні системи виявлення вторгнень, побудовані на основі гібридних методів, які поєднують сигнатурний аналіз, методи машинного навчання та поведінковий аналіз мережевого трафіку. Саме тому обрана тема є актуальною, своєчасною та має важливе практичне значення для розвитку сучасних засобів кібербезпеки.

Повнота розкриття теми. Тема кваліфікаційної бакалаврської роботи розкрита повною мірою. У роботі досліджено теоретичні основи систем виявлення вторгнень, проаналізовано адаптивні та гібридні підходи до виявлення кіберзагроз, виконано формалізацію задачі виявлення вторгнень, розроблено гібридну модель адаптивної IDS та алгоритм її функціонування. Особливу увагу приділено реалізації та налаштуванню системи, а також формуванню експериментального середовища і підготовці даних мережевого трафіку для задачі виявлення вторгнень. Поставлені мета та завдання дослідження виконані в повному обсязі, а отримані результати відповідають темі та змісту роботи.

Теоретичний рівень. Теоретична значущість отриманих результатів полягає в удосконаленні підходів до побудови адаптивних систем виявлення вторгнень на основі гібридних методів. У роботі обґрунтовано доцільність поєднання сигнатурного аналізу, машинного навчання та поведінкового аналізу мережевого трафіку, а також запропоновано підхід до обробки й аналізу мережевих даних для підвищення ефективності виявлення атак. Отримані результати можуть бути використані в подальших дослідженнях та при вдосконаленні сучасних систем кібербезпеки.

Практична значущість отриманих результатів полягає у розробці прототипу адаптивної гібридної системи виявлення вторгнень для підвищення

рівня кіберзахисту інформаційних систем. Запропонована модель може використовуватися для виявлення кіберзагроз, тестування нових методів аналізу мережевого трафіку та зменшення кількості хибних спрацювань. Результати роботи також можуть бути використані як основа для подальших досліджень і вдосконалення сучасних систем кібербезпеки.

Самостійність виконання роботи. Робота виконана самостійно. Автор продемонстрував уміння працювати з науковими джерелами, аналізувати інформацію, формулювати висновки та розв'язувати поставлені завдання дослідження. Отримані результати мають самостійний характер і відповідають визначеній темі роботи.

Якість оформлення, загальна та спеціальна грамотність. Кваліфікаційна бакалаврська робота оформлена відповідно до встановлених вимог. Матеріал викладено логічно, послідовно та зрозуміло. Автор коректно використовує загальнонаукову та спеціальну термінологію у сфері кібербезпеки, систем виявлення вторгнень і машинного навчання. Робота характеризується належним рівнем загальної та фахової грамотності, а виявлені окремі стилістичні чи технічні неточності не впливають на загальне позитивне враження від роботи.

Переваги та недоліки роботи. До основних переваг роботи належать актуальність обраної теми, комплексний підхід до дослідження систем виявлення вторгнень, поєднання теоретичного аналізу та практичної реалізації гібридної моделі IDS. Позитивним є також розроблення алгоритму функціонування системи, формування експериментального середовища та використання сучасних підходів, зокрема методів машинного навчання й кластеризації для виявлення кіберзагроз.

Недоліки роботи. Окремі результати дослідження могли б бути підсилені більш широким експериментальним тестуванням на сучасних наборах мережевого трафіку та детальнішим порівнянням запропонованої моделі з існуючими системами виявлення вторгнень. Водночас зазначені зауваження мають рекомендаційний характер і не впливають на загальну позитивну оцінку роботи.

Загальна оцінка роботи та висновок щодо рекомендації до захисту в ЕК. Загалом кваліфікаційна бакалаврська робота виконана на високому науковому та методичному рівні, відповідає вимогам до бакалаврських робіт. Зазначене дозволяє допустити кваліфікаційну бакалаврську роботу до захисту перед Екзаменаційною комісією та оцінити високою позитивною оцінкою.

Науковий керівник к.т.н., доц. Кулініч О.М.

«____»_____2026 р.

РЕЦЕНЗІЯ

на кваліфікаційну бакалаврську роботу
здобувача вищої освіти Параніна Ігоря Едуардовича
на тему: **«Розробка адаптивних систем виявлення вторгнень гібридними методами»**

У сучасних умовах стрімкого розвитку інформаційних технологій та постійного зростання кількості кіберзагроз питання забезпечення кібербезпеки інформаційних систем набуває особливої актуальності. Тому тема кваліфікаційної бакалаврської роботи, присвячена розробці адаптивних систем виявлення вторгнень із використанням гібридних методів, є своєчасною, актуальною та має практичне значення для розвитку сучасних засобів захисту інформації.

Наукова новизна роботи полягає в удосконаленні підходу до побудови адаптивної системи виявлення вторгнень шляхом інтеграції сигнатурного аналізу та методів машинного навчання в єдину гібридну архітектуру з механізмом адаптивного оновлення моделі.

Робота відзначається логічністю структури, послідовністю викладення матеріалу, належним рівнем теоретичного опрацювання наукових джерел та достатнім рівнем практичної реалізації поставлених завдань. Матеріал викладено грамотно, з використанням сучасної термінології у сфері кібербезпеки.

Автор продемонстрував належний рівень роботи з науковою, навчальною та фаховою літературою з питань кібербезпеки, систем виявлення вторгнень, машинного навчання та гібридних методів аналізу даних. У роботі використано сучасні вітчизняні та зарубіжні джерела, наукові публікації, монографії, матеріали міжнародних організацій. Проведений аналіз літературних джерел свідчить про здатність автора критично опрацьовувати наукову інформацію, узагальнювати існуючі підходи та використовувати їх для обґрунтування власних рішень і висновків. Бібліографічний апарат роботи оформлено відповідно до встановлених вимог, а використані джерела є релевантними тематиці дослідження та достатніми для досягнення поставленої мети.

Теоретична значущість дослідження полягає в узагальненні сучасних підходів до побудови адаптивних IDS та розвитку методичних засад використання гібридних методів для виявлення кіберзагроз.

Практичну цінність роботи становить створення експериментального середовища для тестування системи виявлення вторгнень, яке включає мережеву інфраструктуру, генератори легітимного та шкідливого трафіку, IDS/IPS-компоненти, систему централізованого моніторингу та модулі аналізу даних. Запропонований підхід може бути використаний для підвищення рівня захисту інформаційних систем підприємств і організацій, а також для подальших досліджень у сфері адаптивних систем кібербезпеки.

Разом із позитивними сторонами роботи доцільно зазначити окремі зауваження. Зокрема, результати дослідження могли б бути підсилені проведенням ширшого експериментального оцінювання із використанням сучасних відкритих наборів даних та порівнянням ефективності запропонованої моделі з існуючими системами виявлення вторгнень. Проте наведені зауваження мають рекомендаційний характер і не впливають на загальну позитивну оцінку роботи.

Кваліфікаційна бакалаврська робота на тему «Розробка адаптивних систем виявлення вторгнень гібридними методами» є завершеним самостійним дослідженням, відповідає вимогам, що висуваються до кваліфікаційних робіт бакалаврського рівня вищої освіти.

Рецензент:
к.т.н., доц., професор кафедри Інтелектуальних програмних систем ФКНК КНУ імені ТАРАСА ШЕВЧЕНКА

_____ Гізун А.І.
підпис *прізвище, ініціали*

Печатка

Підпис Гізуна А.І. засвідчую
«___» _____ 20 26 р.
Заст. декана Дмитро ЗАТУЛА

«05» 06 2026 р.

ЗМІСТ

ВСТУП.....3

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ 6

1.1. Історія виникнення та еволюція систем виявлення вторгнень 6

1.2. Поняття, сутність та місце систем виявлення вторгнень у системі кібербезпеки 13

1.3. Класифікація систем виявлення вторгнень 15

1.4. Архітектура та компоненти систем виявлення вторгнень 21

Висновки до першого розділу 26

РОЗДІЛ 2. МОДЕЛЮВАННЯ АДАПТИВНОЇ IDS НА ОСНОВІ ГІБРИДНИХ МЕТОДІВ 28

2.1. Адаптивні системи виявлення вторгнень 28

2.2. Гібридні методи в задачах кібербезпеки 33

2.3. Формалізація задачі виявлення вторгнень 36

Висновки до другого розділу 41

РОЗДІЛ 3. РОЗРОБКА ТА РЕАЛІЗАЦІЯ АДАПТИВНОЇ ГІБРИДНОЇ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ 43

3.1. Розробка гібридної моделі адаптивної IDS 43

3.2. Алгоритм функціонування розробленої адаптивної гібридної системи виявлення вторгнень 56

3.3. Реалізація та налаштування гібридної моделі IDS 59

3.4. Формування експериментального середовища та підготовка даних мережевого трафіку для задачі виявлення вторгнень 69

Висновки до третього розділу 89

ВИСНОВКИ 92

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 98

ВСТУП

Актуальність теми. Стрімкий розвиток інформаційних технологій, зростання обсягів мережевого трафіку та ускладнення кібератак зумовлюють необхідність удосконалення систем захисту комп’ютерних мереж. В умовах сучасних геополітичних конфліктів, зокрема війни в Україні, інформаційна безпека стає критично важливою складовою захисту національних інтересів. Війна стала своєрідним випробувальним майданчиком для нових підходів і технологій у галузі кіберзахисту, особливо у виявленні та протидії кібератакам.

Традиційні системи виявлення вторгнень (IDS), які базуються переважно на сигнатурному аналізі, ефективні щодо відомих атак, проте малоефективні при виявленні нових, модифікованих або нульових (zero-day) загроз. Аномалійні методи дозволяють виявляти невідомі атаки, але характеризуються високим рівнем хибних спрацювань.

У цьому контексті особливої актуальності набуває розробка адаптивних гібридних систем IDS, які поєднують переваги сигнатурного та аномалійного підходів, підвищуючи точність і швидкість реагування на кіберзагрози. Сучасні атаки відзначаються високою динамічністю, що потребує впровадження адаптивних механізмів оновлення моделей виявлення вторгнень. Таким чином, розробка адаптивної гібридної IDS є актуальним і перспективним завданням у сфері кібербезпеки.

В сучасних дослідженнях спостерігаються два підходи до створення систем захисту інформації. Перший підхід передбачає реалізацію заходів, спрямованих на запобігання несанкціонованим впливам порушника на інформаційну сферу комп'ютерної мережі. При цьому підході до структури системи включаються міжмережеві екрани, засоби контролю доступу та аналізу захищеності.

Другий підхід ґрунтується на виявлення факту несанкціонованого проникнення порушника, а також на локалізації місця та встановлення джерела впливу. Основу структури системи складають засоби виявлення несанкціонованих впливів, здатних фіксувати спроби порушення інформаційної безпеки на початковому етапі їх розвитку [1].

Мета і завдання дослідження. Метою кваліфікаційної бакалаврської роботи є розробка адаптивної системи виявлення вторгнень на основі гібридних методів з метою підвищення ефективності виявлення кіберзагроз, зменшення кількості хибних спрацювань і забезпечення своєчасного реагування на сучасні атаки. Для досягнення поставленої мети визначено такі **завдання**:

- дослідити історію виникнення та еволюцію систем виявлення вторгнень;
- визначити поняття, сутність та місце систем виявлення вторгнень у системі кібербезпеки;
- дослідити класифікацію систем виявлення вторгнень та їх архітектуру;
- дослідити принципи адаптивності в IDS;
- розглянути можливості застосування гібридних методів у кібербезпеці;
- формалізувати задачу виявлення вторгнень як задачу класифікації та виявлення аномалій;
- розробити гібридну модель адаптивної IDS;
- реалізувати алгоритм функціонування розробленої адаптивної гібридної системи виявлення вторгнень;
- сформувати експериментальне середовище та підготовку даних мережевого трафіку для задачі виявлення вторгнень.

Об’єктом дослідження є процес виявлення вторгнень у комп’ютерних мережах на основі аналізу мережевого трафіку.

Предмет дослідження – методи, моделі та алгоритми побудови адаптивних систем виявлення вторгнень на основі гібридних методів.

Методи дослідження. У процесі виконання роботи використано загальнонаукові методи (аналіз, синтез, порівняння, узагальнення), методи математичного та алгоритмічного моделювання, методи кластерного аналізу і класифікації, а також методи статистичної обробки результатів обчислювального експерименту.

Теоретична і методична значущість отриманих результатів полягає у розвитку підходів до побудови адаптивних гібридних систем виявлення вторгнень на основі поєднання сигнатурного аналізу, методів машинного навчання та поведінкового аналізу мережевого трафіку. У роботі узагальнено

сучасні підходи до виявлення кіберзагроз, обґрунтовано доцільність використання гібридної архітектури та запропоновано методику аналізу й обробки мережевих даних для підвищення точності виявлення атак. Отримані результати можуть бути використані як теоретична та методична основа для подальших досліджень у сфері інтелектуальних систем кібербезпеки, а також для вдосконалення методів аналізу та класифікації мережевого трафіку.

Практичне значення отриманих результатів полягає у розробці прототипу адаптивної гібридної системи виявлення вторгнень, яка може застосовуватися для підвищення рівня кіберстійкості інформаційних систем підприємств і державних установ. Запропонована модель також може використовуватися для дослідження та тестування нових методів виявлення вторгнень, а також для зменшення кількості хибних спрацювань у процесі аналізу мережевого трафіку. Крім того, результати роботи створюють основу для подальших наукових досліджень у сфері адаптивних і гібридних систем кібербезпеки.

Інформаційну базу дослідження становлять наукові публікації вітчизняних і зарубіжних авторів, матеріали міжнародних конференцій та фахових журналів з кібербезпеки, нормативні документи у сфері захисту інформації, відкриті датасети мережевого трафіку для задач виявлення вторгнень, а також результати власного експериментального моделювання.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

1.1. Історія виникнення та еволюція систем виявлення вторгнень

На початкових етапах розвитку комп'ютерів і комп'ютерних мереж основним засобом виявлення вторгнень були самі системні адміністратори. Вони вручну, через консоль, аналізували дії користувачів і відстежували підозрілу активність. До таких дій належали, наприклад, нетипова активність принтера, який зазвичай використовувався рідко, або локальний вхід користувача в систему під час його офіційної відпустки.

Попри певну ефективність, такий підхід з часом втратив актуальність. Його недоліками були орієнтація лише на заздалегідь визначені ситуації, суб'єктивність оцінювання та неможливість масштабування в умовах великих і розгалужених мереж. Це зумовило потребу в розробленні автоматизованих систем виявлення вторгнень, здатних аналізувати значні обсяги даних у реальному часі.

Стрімкий розвиток інформаційних технологій та глобальних мереж спричинив зростання кількості кіберзагроз. Несанкціонований доступ до інформаційних ресурсів, мережеві атаки та шкідливе програмне забезпечення стали серйозною проблемою як для державних установ, так і для приватних компаній. Класичні методи захисту вже не можуть впоратися з високою швидкістю змін у поведінці атак і новими техніками проникнення. Тому важливо розуміти історію створення та еволюцію систем виявлення вторгнень (Intrusion Detection Systems, IDS) як ключового елементу сучасних рішень з кібербезпеки.

Розглянемо еволюцію систем виявлення вторгнень (рис. 1.1)

1. Початок. 1970–1980-ті роки: Перші концепції James P. Anderson

Перші дослідження у сфері автоматизованого контролю безпеки комп'ютерних систем розпочалися ще у 1970-х роках. Перша концепція СВВ

з'явилася завдяки Джеймсу Андерсону і його статті з назвою «Моніторинг та спостереження загроз комп'ютерної безпеки» [2].



Рисунок 1.1 – Еволюція систем виявлення вторгнень (IDS): від ручного аналізу до AI

Джерело: розроблено автором на основі [2-14] за допомогою ChatGPT

У цій роботі він запропонував концепцію аналізу журналів подій (log-файлів) з метою виявлення підозрілої активності користувачів. Основна ідея полягала у створенні профілів нормальної поведінки та порівнянні їх із фактичними діями в системі. Цей підхід став теоретичною основою для подальших досліджень та розвитку сучасних систем виявлення вторгнень (IDS).

2. 1980-ті. Перші дослідницькі системи 1987 році Dorothy Denning

У 1984 Фред Коен зробив заяву про те, що кожне вторгнення виявити неможливо і ресурси, необхідні для виявлення вторгнень, будуть рости пропорційно використанню комп'ютерних технологій.

Значний внесок у розвиток систем виявлення вторгнень зробила Dorothy Denning, яка в 1986 році за сприяння Пітера Неймана опублікувала статтю з

назвою «Модель виявлення вторгнень», де представила власну систему виявлення вторгнень (далі – СВВ) – Denning's Intrusion Detection Model і ця робота лягла в основу більшості сучасних систем [3, с. 119-131]. Ця модель передбачала:

– використання статистичного аналізу;

– застосування сигнатурного підходу;

– формування профілів поведінки користувачів для виявлення аномалій.

MIDAS (Multics intrusion detection and alerting system), експертна система, написана з використанням мови програмування LISP, була розроблена в 1988 році на основі роботи Деннінга і Неймана [4].

У цей період з'явилися перші експериментальні системи, зокрема IDES (Intrusion Detection Expert System) та Haystack. Вони переважно були орієнтовані на захист окремих комп'ютерів і належали до класу Host-based Intrusion Detection Systems (HIDS), що функціонували безпосередньо на захищуваному хості та аналізували події операційної системи й журнали активності користувачів. Система працювала на робочих станціях Sun і перевіряла як мережевий трафік, так і дані користувачів додатків [5].

W & S (Wisdom & Sense «мудрість і почуття») – це система виявлення аномалій, розроблена у 1989 році в Національній лабораторії Лос-Аламосу (Los Alamos National Laboratory) [6]. W&S ґрунтувався на статистичних методах і дозволяв автоматично створювати правила на основі аналізу нормальної поведінки системи.

Після формування правил система застосовувала їх для виявлення аномалій у поведінці користувачів або системних процесів, що дозволяло визначати потенційні інциденти безпеки. Такий підхід став одним із перших практичних прикладів використання статистичних методів у IDS і заклав основу для подальшого розвитку аномалійних систем виявлення вторгнень.

Система IDES для виявлення вторгнень використовувала два основні методи.

Першим компонентом була експертна система, що спиралася на базу знань із уже відомими типами вторгнень (сигнатурний підхід). Другим — модуль

моніторингу, який здійснював аналіз стану системи за допомогою статистичних методів, використовуючи дані про поведінку користувачів і параметри захищуваної системи (аномалійний підхід).

Наступним етапом розвитку систем виявлення вторгнень стало впровадження штучних нейронних мереж як третього компонента аналізу. Це нововведення було запропоноване Teresa Lunt. У результаті в 1993 році було розроблено систему NIDES (Next-generation Intrusion Detection Expert System – експертна система виявлення вторгнень нового покоління), яка базувалася на її ідеях і поєднувала експертні правила, статистичний аналіз та елементи інтелектуальної обробки даних [7].

3. 1990-ті. Комерціалізація та розвиток мережевих IDS. Поява NIDS

У 1990 роках із розвитком Інтернету та корпоративних мереж виникла потреба у контролі мережевого трафіку. Це сприяло появі мережевих систем виявлення вторгнень (Network-based IDS, NIDS). Однією з найвідоміших систем цього періоду стала Snort.

У 1990 році була розроблена система TIM (Time-based Inductive Machine), яка реалізувала виявлення аномалій за допомогою індуктивного навчання. Система аналізувала послідовні патерни поведінки користувачів, використовуючи мову Common LISP, і працювала на комп’ютері VAX 3500. Принципи роботи TIM описані в статті «Адаптивне виявлення аномалій в режимі реального часу з використанням індуктивно сформованих послідовних шаблонів» [8].

Приблизно в той же період був розроблений NSM (Network Security Monitor) – мережевий монітор безпеки, який здійснював порівняння матриць доступу для виявлення аномалій на робочих станціях Sun-3/50 [9].

У тому ж 1990 році з’явилася система ISOA (Information Security Officer's Assistant), яка інтегрувала статистичні методи, перевірку профілю користувачів та експертну систему для підвищення ефективності виявлення вторгнень.

Крім того, система ComputerWatch, розроблена в AT&T Bell Labs, поєднувала статистичний аналіз та сигнатурні методи, що дозволяло скоротити обсяг даних аудиту та підвищити швидкість виявлення атак.

Таким чином, на початку 1990-х років спостерігався активний розвиток систем IDS із використанням статистичних методів, індуктивного навчання та комбінації сигнатур і аномалійного аналізу, що заклало основу сучасних систем виявлення вторгнень.

У 1998 році програміст Мартін Роеш (Martin Roesch) створив Snort як невеликий «вихідний проєкт» для власного задоволення. Спочатку програма називалася APE і була звичайним інструментом для прослуховування мережевого трафіку (сніффером). Через місяць після розробки автор перейменував її на Snort (від англ. snort – «хрюкання», що відображено в логотипі з поросям) і випустив як вільне програмне забезпечення з відкритим кодом. Вона швидко здобула популярність завдяки відкритому коду та можливості аналізу трафіку в реальному часі.

У 2001 році, побачивши великий успіх проєкту у спільноті, Роеш заснував компанію Sourcefire для розвитку комерційних рішень на базі Snort для великих підприємств. У 2009 році Snort було включено до Open Source Hall of Fame журналу InfoWorld як одну з найкращих програм в історії вільного програмного забезпечення. З 2013 року і дотепер Snort є частиною безпекової екосистеми Cisco Systems, яка викупила Sourcefire, і продовжує розвиватися як відкритий проєкт. У 1990-х роках IDS почали активно впроваджуватися у корпоративному секторі, що стало початком їх комерціалізації [1].

4. 2000-ті. Інтеграція IDS та IPS у широку екосистему безпеки

На початку 2000-х років системи виявлення вторгнень (IDS) стали досить популярними. У той час фаєрволи обробляли мережевий трафік відносно швидко, оскільки вони не здійснювали глибокої інспекції пакетів. Іншими словами, фаєрволи реагували лише на визначені в правилах протоколи та мережеві адреси, не аналізуючи сам зміст трафіку.

У той же період почали масово з’являтися нові типи атак, наприклад, SQL-ін’єкції та інші складні експлойти, які швидко поширювалися. Саме для захисту від таких загроз системи IDS виявилися надзвичайно корисними, оскільки вони

[1] https://chatgpt.com/c/699b2d76-1ce0-838e-97c5-7f9e92b8e44d

могли виявляти аномалії й підозрілу активність, що виходила за межі стандартних правил фаєрволів.

Що стосується систем IPS (Intrusion Prevention Systems), то їх впровадження було менш масовим. Деякі організації уникали використання IPS через ризик блокування легітимного трафіку, що могло негативно вплинути на роботу бізнес-процесів. Таким чином, на цьому етапі IDS були в основному засобом моніторингу та виявлення загроз але не блокували їх, а IPS – більш обережно застосовувалися через потенційні побічні ефекти.

Тому наступним етапом розвитку стало створення систем запобігання вторгненням (Intrusion Prevention Systems, IPS). На відміну від IDS, які лише фіксували підозрілу активність, IPS могли автоматично блокувати атаки, розривати з'єднання та змінювати правила фаєрвола.

У цей період IDS інтегруються з іншими засобами безпеки: міжмережевими екранами, антивірусними системами, SIEM-платформами (Security Information and Event Management), що дозволило створювати комплексні системи кіберзахисту.

Вже з 2005 IPS системи починають набирати популярність. Особливою популярністю користувалися гібридні системи, вони ефективно суміщали в собі IDS та IPS, а продуктивність таких систем становила до 5 Гбіт/с. Такі системи могли моніторити сегментовані мережі, DMZ, серверні ферми з веб-додатками і площу всередині периметра. Сучасні гібридні системи мають швидкість до 40 Гбіт/с.

5. 2010-ті. Використання машинного та глибокого навчання

В 2010-х роках з розвитком хмарних технологій і появою складних цілеспрямованих атак (APT) та zero-day уразливостей традиційні сигнатурні методи стали менш ефективними. У відповідь на це розпочалося активне впровадження:

– алгоритмів машинного навчання;
– поведінкової аналітики (UEBA);
– аналізу великих обсягів даних (Big Data);
– виявлення zero-day атак.

IDS почали застосовуватися у хмарних середовищах, віртуалізованих інфраструктурах та IoT-мережах.

Сучасні огляди показують, що алгоритми машинного навчання здатні підвищити точність виявлення й адаптивність систем до нових загроз, а також зменшити кількість хибних спрацювань при аналізі великого обсягу мережевого трафіку.

6. 2020-2025. Сучасні AI-платформи та адаптивні архітектури

У сучасних наукових працях описано кілька трендів розвитку IDS:

Оптимізація обробки правил у великих системах IDS – вивчається вплив алгоритмів оптимізації на продуктивність IDS, зокрема для Snort 3 [10].

Глибоке підсилене навчання для IoT-мереж, що дозволяє адаптувати захист у динамічних умовах IoT-середовищ [11].

Графові нейронні мережі та великі мовні моделі (LLM) для покращеної класифікації мережевих потоків та пояснюваності результатів виявлення [12].

Огляд сучасних ML-методів показує, що комбіновані підходи на основі глибокого навчання суттєво підвищують ефективність IDS шляхом виявлення складних аномалій [13].

Проєкти з оновленням правил та підтримкою адаптивних моделей демонструють ефективність поєднання класичних та AI-підходів [14].

Ці сучасні напрямки дозволяють створювати IDS, які не лише виявляють вторгнення в реальному часі, але й здатні адаптуватись до нових типів загроз.

Сучасні IDS еволюціонують у складні платформи:

– EDR (Endpoint Detection & Response);

– NDR (Network Detection & Response);

– XDR (Extended Detection & Response).

Вони використовують: штучний інтелект, автоматизоване реагування (SOAR), кореляцію подій з різних джерел.

1.2. Поняття, сутність та місце систем виявлення вторгнень у системі кібербезпеки

Сучасний розвиток інформаційних технологій супроводжується постійним зростанням кількості кіберзагроз, що створює необхідність упровадження ефективних механізмів захисту інформаційних систем. Одним із ключових інструментів забезпечення кібербезпеки є системи виявлення вторгнень (СВВ, англ. – Intrusion Detection Systems, IDS), які призначені для моніторингу мережевого трафіку, виявлення підозрілої активності та попередження несанкціонованих дій. Відповідно до рекомендацій National Institute of Standards and Technology (NIST), IDS – це програмний або апаратний засіб, що здійснює моніторинг подій у мережі або інформаційній системі та аналізує їх з метою виявлення ознак можливих інцидентів безпеки [15].

У документі NIST SP 800-94 зазначено, що системи IDS можуть функціонувати як окремі програмні модулі або як спеціалізовані апаратно-програмні комплекси, які аналізують мережевий трафік, журнали подій операційних систем, дії користувачів та інші джерела інформації. Такі системи виконують функцію додаткового рівня безпеки інформаційної інфраструктури.

Про будь-які вторгнення або порушення безпеки зазвичай повідомляється системному адміністратору або ж ці події централізовано збираються за допомогою системи управління інформацією та подіями безпеки SIEM (Security Information and Event Management), яка об’єднує дані з різних джерел – IDS/IPS, фаєрволів, серверів, мережевого обладнання, антивірусних рішень та інших компонентів інфраструктури – в єдину платформу для подальшого аналізу, щоб відрізнити шкідливу активність від хибних сигналів.

Основне завдання СВВ полягає у виявленні потенційно шкідливої активності, яка може загрожувати цілісності, доступності або конфіденційності інформаційних ресурсів. До таких загроз належать мережеві атаки на вразливі служби, спроби підвищення користувацьких привілеїв, несанкціонований доступ до критичних даних, а також дії шкідливого програмного забезпечення – вірусів, троянських програм і мережевих черв’яків.

На рис. 1.2 показано основний процес системи виявлення вторгнень, який здійснює моніторинг, аналіз, оповіщення та реагування на виявлений дефект. IDS створюються за допомогою програмного забезпечення, яке оцінює безпеку мережі за допомогою моніторингу мережевої діяльності. Програмне забезпечення дозволяє мережевому контролеру перевіряти мережу вразливостей, таким чином, захищаючи потенційні лазівки перш, ніж зловмисники скористаються ними.



Рисунок 1.2 – Основний процес системи виявлення вторгнень

Джерело: Розроблено автором на основі [15-17] за допомогою https://notebooklm.google.com

Отже, **IDS-система не відображає атаки, а лише виявляє їх і повідомляє адміністратора, допомагаючи знайти причину та усунути її** [16]. Інструменти IDS можуть використовуватися окремо або у складі міжмережевих екранів.

Крім функцій постійного моніторингу та аналізу того, що відбувається, IDS системи виконують такі функції:

– реєстрація інцидентів – збір та збереження інформації про виявлені події як локально, так і з передачею до централізованих систем збору журналів або SIEM-систем;

– оповіщення адміністраторів про інциденти інформаційної безпеки (далі – ІБ) за допомогою різних каналів сповіщення: електронної пошти, SNMP-trap, SMS або повідомлень у консолі керування;

– формування звітності – створення детальних або узагальнених звітів щодо окремих подій чи груп інцидентів для подальшого аналізу та прийняття управлінських рішень.

Таким чином, IDS виконують не лише функцію виявлення загроз, але й забезпечують комплексну підтримку процесу реагування на інциденти та аналізу безпеки інформаційної системи.

Технологія IPS в свою чергу у додачу до вище сказаного, здатна не тільки визначити загрозу і її джерело, а й здійснити їх блокування. Це говорить про розширений функціонал подібного рішення.

Вона здатна здійснювати наступні дії:

– обривати шкідливі сесії і запобігати доступу до найважливіших ресурсів;

– змінювати конфігурацію «підзахисної» середовища;

– проводити дії над інструментами атаки (наприклад, видаляти заражені файли) [17].

У комплексній системі захисту інформації IDS відіграє роль механізму контролю та аналітики. Вона доповнює фаєрволи, антивірусні засоби та інші інструменти безпеки, забезпечуючи виявлення атак, які можуть обходити традиційні механізми фільтрації. Таким чином, IDS є невід’ємним елементом багаторівневої моделі захисту інформації (defense in depth), підвищуючи загальний рівень кіберстійкості організації.

1.3. Класифікація систем виявлення вторгнень

Існує кілька способів класифікації СВВ в залежності від типу і розташування сенсорів, а також методів, використовуваних підсистемою аналізу для виявлення підозрілої активності. У багатьох простих СВВ всі компоненти реалізовані у вигляді одного модуля або пристрою.

Виявлення вторгнень у комп’ютерні мережі є критично важливим аспектом підтримки безпеки та цілісності цифрових систем. Існують кілька типів систем

виявлення вторгнень (IDS), які забезпечують виявлення аномальної чи шкідливої активності у комп'ютерних системах та мережах. Вони можуть бути поділені на дві основні категорії: мережеві системи виявлення вторгнень (Network-based IDS, NIDS), хост-системи виявлення вторгнень (Host-based IDS, HIDS) та для застосунків (AIDS – Application-based IDS) (рис. 1.3).



Рисунок 1.3 – Класифікація систем виявлення вторгнень

Джерело: розроблено автором на основі [18-22] за допомогою ChatGPT

Мережева система виявлення вторгнень (Network-based Intrusion Detection System, NIDS) призначена для моніторингу мережевого трафіку в реальному часі з метою виявлення підозрілих дій та атак. NIDS використовує комбінацію методів, описаних раніше: сигнатурний підхід, аномалійний аналіз, а також аналіз окремих пакетів даних, що передаються мережею.

Системи NIDS зазвичай розміщуються в мережі та працюють на різних мережевих рівнях:

– великі серверні NIDS можуть бути налаштовані для моніторингу всього трафіку магістральної мережі;

– менші системи налаштовуються для контролю трафіку, спрямованого на конкретний сервер, комутатор, шлюз або маршрутизатор;

– централізовані NIDS встановлюються на сервері для сканування системних файлів, виявлення несанкціонованої активності та підтримки цілісності даних.

Процес виявлення вторгнень зазвичай складається з двох різних етапів. На першому етапі модель навчається. На другому етапі побудована модель застосовується для аналізу поточного трафіку та виявлення будь-яких відхилень.

Завдяки такій архітектурі NIDS є ефективним інструментом для виявлення атак у реальному часі та додатковим рівнем захисту у комплексній системі безпеки інформації.

Виділяють такі види мережевих систем виявлення вторгнень (NIDS):

– Signature-Based NIDS – виявляють атаки шляхом порівняння мережевої активності з відомими сигнатурами.

– Anomaly-Based NIDS – визначають відхилення від нормальної поведінки мережі без використання наперед заданих сигнатур.

– Hybrid NIDS – поєднують сигнатурний і аномальний підходи для підвищення ефективності виявлення атак..

Хостова система виявлення вторгнень (HIDS, Host-based Intrusion Detection System) встановлюється на окремих хост-системах і здійснює моніторинг діяльності на рівні хоста. Основне призначення HIDS – захист індивідуальних комп’ютерних систем, а не всієї мережі, шляхом аналізу подій операційної системи та активності користувачів.

Основні завдання HIDS:

– виявлення несанкціонованих дій і атак на хості, включаючи спроби злому та зловмисні програми (віруси, трояни);

– контроль аномальної поведінки користувачів, що може вказувати на нові чи невідомі погрози;

– виявлення змін у файловій системі, реєстрі та інших критичних компонентах;

– фіксація подій, що можуть загрожувати безпеці та надійності системи.

HIDS аналізує активність на хості за допомогою:

– сигнатурного аналізу, використовуючи бази даних відомих загроз і патернів атак;

– аномалійного аналізу, що дозволяє виявляти нові або невідомі загрози.

– моніторингу доступу до файлів, системних журналів, мережевої активності та інших компонентів системи.

Коли HIDS виявляє підозрілу активність або порушення безпеки, вона може генерувати попереджувальні повідомлення або оповіщення для адміністратора системи. Прикладами HIDS є Snort (хоча зазвичай відомий як NIDS, може бути налаштований для роботи на хості), OSSEC (відкрита система для моніторингу та виявлення вторгнень на хості), Tripwire (система контролю цілісності файлів та виявлення змін) та інші програми, які призначені для виявлення вторгнень лише на рівні окремих хостів.

Хостові системи виявлення вторгнень (HIDS) можна класифікувати за принципом їх функціонування та об’єктом моніторингу. Виділяють такі основні типи HIDS:

− File Integrity Checkers – контролюють цілісність файлів, виявляючи несанкціоновані зміни у файловій системі.

Log-based HIDS – аналізують журнали подій та фіксують підозрілу активність (невдалі входи, запуск підозрілих програм тощо).

Behavior-based HIDS – відстежують поведінку процесів і додатків для виявлення аномалій.

Kernel-based HIDS – здійснюють моніторинг ядра операційної системи з метою виявлення критичних змін або атак.

До складу IDS також можуть входити:

− Аналізатори потоку даних (Flow-based IDS), які моніторять потоки даних у мережі та аналізують події на рівні потоків, що дозволяє виявляти аномалії у комунікації між вузлами.

− Інтегровані системи виявлення вторгнень (Integrated IDS), які об'єднують мережеві та хостові системи виявлення вторгнень для більш повного аналізу активності мережі. Застосування відповідної системи виявлення вторгнень

залежить від конкретних потреб та характеристик інфраструктури, яку необхідно захищати.

Комбіноване використання мережевих систем виявлення вторгнень (NIDS) та хост-систем виявлення вторгнень (HIDS) може забезпечити більш повний захист інфраструктури від внутрішніх та зовнішніх загроз. Це ставить нові задачі перед науковцями та практиками з кібербезпеки по удосконаленню існуючих систем виявлення вторгнень у комп'ютерні мережі та створення більш прогресивних [18].

Таким чином, HIDS є ключовим елементом захисту конкретних хостів і доповнює мережеві системи виявлення вторгнень (NIDS), забезпечуючи багаторівневу стратегію безпеки.

Схема мережі хостинг провайдера зображена на рис. 1.4.

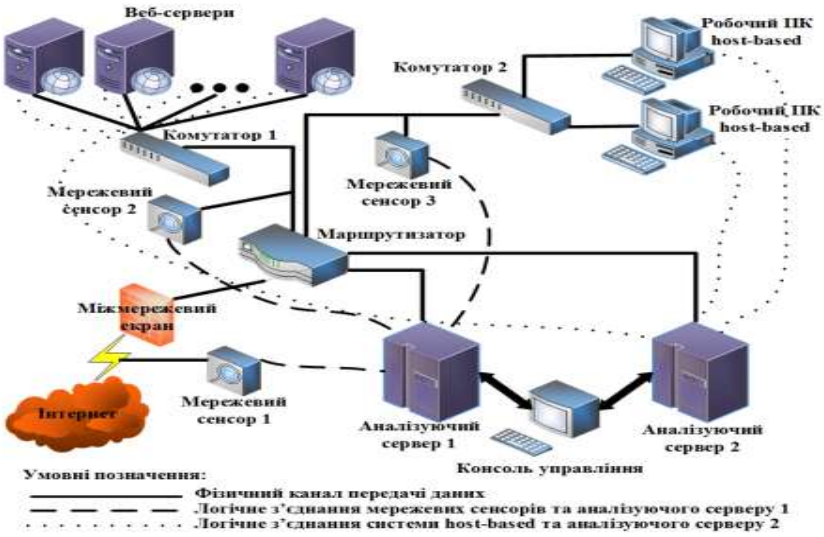


Рисунок 1.4 – Схема мережі хостинг провайдера [21]

AIDS (Application Intrusion Detection System) – система виявлення вторгнень на рівні застосунку, що аналізує його роботу та дії користувачів. Може використовувати сигнатурний, аномальний або гібридний підхід для виявлення атак (наприклад, SQL-ін’єкцій чи XSS).

Крім того, Системи виявлення вторгнень можна класифікувати за характером відповідної реакції, методами аналізу, рівнем виявленням атак.

1. За характером відповідної реакції системи можуть бути *пасивними* (реєструють події), *активними/превентивними* (IPS – запобігають загрозам

шляхом блокування або ізоляції трафіку) або *гібридними* (здійснюють виявлення та протистоять вторгненням в автоматичному режимі).

2. Основні методи, які використовуються в IDS [19]:

– сигнатурний аналіз – порівняння з базою відомих атак;

– аналіз аномалій – виявлення відхилень від «нормальної» поведінки;

– гібридні моделі – поєднання сигнатур і поведінкових патернів.

Ефективність виявлення загроз залежить від архітектурних особливостей мережі: наявності демілітаризованих зон (DMZ), сегментації мережі, побудови маршрутів та точок моніторингу трафіку. IDS/IPS мають бути правильно позиціоновані у мережі для того, щоб забезпечити повне охоплення трафіку та уникнути сліпих зон [20].

3. За рівнем виявленням атак IDS поділяються на:

–NIDS (Network Intrusion Detection System) – аналізує мережевий трафік і контролює кілька хостів одночасно. Забезпечує широке покриття та централізоване управління, але не аналізує зашифрований трафік і потребує додаткового налаштування мережевого обладнання.

– GrIDS (Graph-Based Intrusion Detection System) – удосконалена версія NIDS, що збирає дані з різних сегментів мережі та відображає їх у вигляді графа інформаційних потоків.

– OIDS (Operational Intrusion Detection System) – орієнтована на виявлення внутрішніх атак; порівнює поточні дії користувача з типовою поведінкою та фіксує відхилення.

– HIDS (Host-based Intrusion Detection System) – працює на рівні окремого хоста, аналізує журнали подій і системні процеси. Ефективна при зашифрованому трафіку, але має обмежене покриття та навантажує систему.

– ERIDS (External Routing Intrusion Detection System) – спеціалізована система для виявлення атак на маршрутизацію, зокрема змін у налаштуваннях маршрутизаторів [21, 22].

Обмеження традиційних IDS полягають у таких основних аспектах:

Традиційні системи виявлення вторгнень здебільшого не можуть ефективно аналізувати зашифрований трафік, що ускладнює виявлення атак у сучасних

мережах із широким використанням SSL/TLS. Сигнатурні IDS не здатні виявляти нові або модифіковані атаки без попередньо створених сигнатур, тому їх ефективність залежить від регулярного оновлення бази загроз.

Також характерною проблемою є велика кількість хибних спрацювань (false positives), що ускладнює роботу адміністраторів і може призводити до ігнорування реальних інцидентів. При аналізі значних обсягів трафіку IDS створюють додаткове навантаження на систему.

Крім того, традиційні IDS зазвичай лише фіксують та повідомляють про атаку, але не блокують її автоматично (на відміну від IPS), а їх правильне налаштування потребує значного часу та кваліфікації.

1.4. Архітектура та компоненти систем виявлення вторгнень

З кінця 1980-х років адміністратори корпоративних мереж стали включати СВВ до інструментів, що забезпечують безпеку мережі, і застосовували їх у роботі. Однак при функціонуванні були виявлені недоліки використання систем, такі як неможливість виявити атаки нульового дня, оскільки трафік порівнювався тільки зі списком відомих сигнатур, та використання великої кількості ресурсів для постійного сканування.

Вирішення проблеми виявлення нових атак прийшло з впровадженням нового методу – **виявлення аномалій** (ВА). Він був заснований на виявленні нетипових поведінок у мережі та забезпечував виявлення аномальних ситуацій [23].

Наприкінці 1990-х років Агентство передових оборонних дослідницьких проектів (англ. Defense Advanced Research Projects Agency, DARPA) ініціювало спробу систематизувати складові елементи систем виявлення вторгнень. Результатом стала модель Common Intrusion Detection Framework (CIDF) – загальна концепція побудови архітектури IDS.

Згідно з цією моделлю, типова архітектура СВВ включає такі блоки (рис. 1.5):

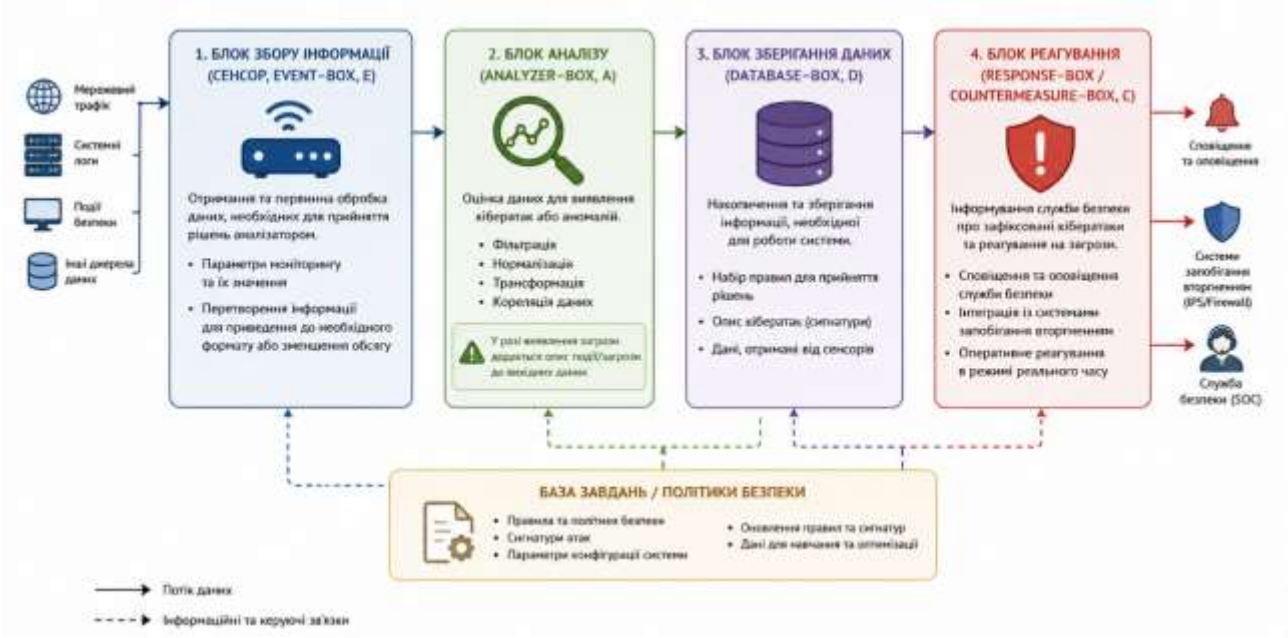


Рисунок 1.5 – Загальна схема роботи Системи виявлення вторгнень

Джерело: Розроблено автором на основі [16, 23-24] за допомогою https://notebooklm.google.com

Блок збору інформації (сенсор, Event–box, E) відповідає за отримання та первинну обробку даних, необхідних для прийняття рішень аналізатором. Отримані дані можуть містити параметри моніторингу, їх характеристики та значення. Сенсор також виконує перетворення інформації для приведення її до необхідного формату або зменшення обсягу переданої інформації.

Блок аналізу (Analyzer–box, A) оцінює отримані від сенсорів дані для виявлення можливих кібератак або аномалій. Під час аналізу система здійснює фільтрацію, нормалізацію, трансформацію та кореляцію даних. Якщо виявлено загрозу, система додає відповідний опис до вихідних даних. Аналізатор може мати багаторівневу архітектуру, що підвищує ефективність виявлення загроз.

Блок зберігання даних (Database–box, D) використовується для накопичення інформації, зокрема набору правил для прийняття рішень, опису кібератак та даних, отриманих від сенсорів. Інформація може зберігатися у вигляді текстових файлів, сигнатур, баз даних тощо.

Блок реагування (Response–box) (або **Countermeasure–box, C)** відповідає за інформування служби безпеки про зафіксовані кібератаки. У випадку

інтеграції з системами запобігання вторгнень цей блок забезпечує оперативне реагування на загрози в режимі реального часу.

Однією з найбільш критичних складових системи є підсистема аналізу, яка визначає наявність загроз на основі отриманих даних. Від її ефективності залежить рівень безпеки інформаційної інфраструктури. Оптимізація роботи цього блоку можлива завдяки використанню технологій штучного інтелекту для точнішого аналізу та оцінки загроз [24].

Завдяки такій модульній побудові СВВ забезпечують ефективне виявлення загроз у реальному часі та створюють основу для інтеграції з іншими елементами систем кібербезпеки.

Система запобігання вторгнень (англ. Intrusion Prevention System, IPS) – програмна або апаратна система мережевої та комп'ютерної безпеки, що виявляє вторгнення або порушення безпеки і автоматично захищає від них. IPS виконує зіставлення трафіку відомим патернам мережевих атак для виявлення: зміни тенденцій мережевого трафіку; спроб несанкціонованого доступу; спроб звернення до небезпечних ресурсів із мережі організації. IPS здатна не тільки виявляти ризики на різних рівнях, а й автоматично відповідати на них: блокувати небезпечний трафік; генерувати подію безпеки для адміністратора. Таким чином, IPS є інструментом активного захисту. Фактично IPS виступає другим рубежем захисту, що знаходиться за фаєрволом або входить до його складу [16].

Системи IPS можна розглядати як розширення Систем виявлення вторгнень (IDS), так як завдання відстеження атак залишається однаковою.

Тобто, Систему виявлення вторгнень (IDS) ще називають пасивною системою, при виявленні порушення безпеки, інформація про це порушення записується в log-додатку, а також сигнали небезпеки відправляються на консоль і / або адміністратору системи по певному каналу зв'язку.

В активній системі, також відомої як Система запобігання вторгнень (IPS), будуть виконані відповідні дії на порушення, спрямовані для його припинення, наприклад: відключення з'єднання, налаштування міжмережевого екрану для блокування трафіку від зловмисника, блокування IP адрес, блокування акаунтів користувачів, від яких надходить потенційно небезпечна активність, відновлення

log-файлів у випадку їх видалення, знищення процесів, запуск процесів, відключення систем, запис інформації про потенційну атаку і виконані дії для її припинення.

Як видно з цього списку, Система запобігання вторгнень (IPS), має широкий «арсенал» дій та гарантує певний рівень захисту. Проте вона є лише одним зі складових елементів захисту мережі, та має ряд дій які вона не може виконувати:

– запобігти копіюванню документів на зовнішні носії;

– змінювати права доступу користувачів;

– контролювати оновленням програмного забезпечення.

Однак, IDS та IPS відрізняються тим, що IPS повинна відстежувати активність в реальному часі і швидко реалізовувати дії щодо запобігання атак.

Основна відмінність між встановленням IDS та IPS полягає в їхній реакції на загрози: IDS (система виявлення вторгнень) тільки виявляє та сповіщає про підозрілу активність, а IPS (система запобігання вторгненням) виявляє і автоматично блокує шкідливий трафік, діючи як проактивний захисний бар'єр. Таким чином, IDS працює як сигналізація, тоді як IPS – як автоматичний бар'єр.

Крім відмінності у способі реагування на атакуючий або підозрілий трафік, IPS та IDS відрізняються способом встановлення в інфраструктурі мережі та по відношенню до мережевого трафіку. Якщо, як правило, IDS системи встановлюються «збоку» від мережевих потоків, обробляючи копію трафіку, що проходить через мережу, то IPS зазвичай встановлюються «в розрив» і стоять на проході трафіку через активне мережеве обладнання. На рис. 1.6 детально зображено відмінності у встановлені IPS та IDS систем [23].

У цьому випадку перевага IDS полягає у такому. При вичерпанні ресурсів, які є у засоби захисту для обробки трафіку, IDS не впливатиме на пропуск трафіку через мережу. IPS встановлений на проході оброблюваного трафіку, є вузьким місцем системи захисту. Як додатковий модуль у складі міжмережевого екрану, IPS дає додаткове навантаження на обладнання міжмережевого екрану і здебільшого є частиною міжмережевого екрану нового покоління (Next Generation Firewall, NGFW).

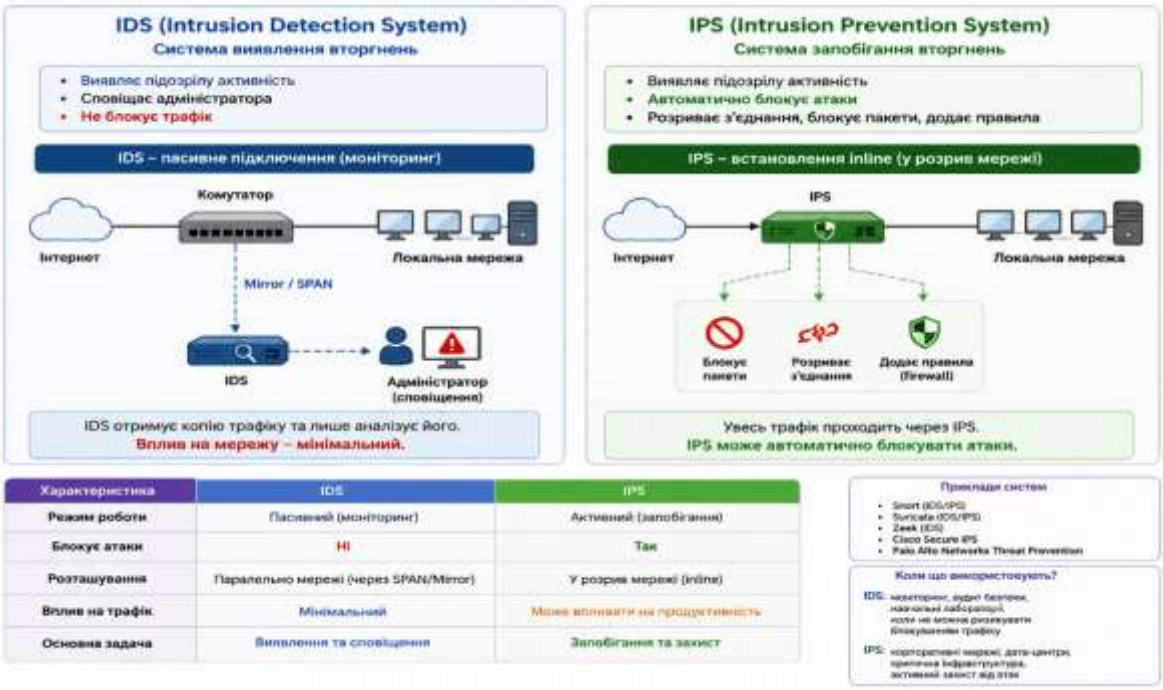


Рисунок 1.6 – Різниця між встановленням IDS та IPS систем

Джерело: розроблено автором на основі [16,18-24] за допомогою ChatGPT

В табл. 1.1 наведено основні переваги та недоліки систем IDS та IPS.

Таблиця 1.1 – Порівняльний аналіз систем IDS та IPS

Характеристика	**IDS (Система виявлення вторгнень)**	**IPS (Система запобігання вторгненням)**
Основна функція	Моніторинг та виявлення шкідливої активності	Виявлення, запобігання та блокування шкідливої активності
Реакція на загрозу	Генерує сповіщення, не втручаючись у трафік.	Автоматично зупиняє або видаляє шкідливі пакети, блокує IP-адресу зловмисника.
Тип дії	Реактивний (сповіщення).	Проактивний (запобігання).
Взаємодія з мережею	Не втручається в мережевий трафік.	Втручається в мережевий трафік, щоб заблокувати його.
Має можливість блокувати підозрілі запити	+	+
Може модифікувати фаєрвол	–	+
Відновлює систему після атаки	–	+
Порівняння	Працює як «сигналізація».	Працює як «автоматичний бар'єр».

Джерело: Розроблено автором на основі [16,18-24]

Як можна побачити, IPS має більший функціонал, та є не консультаційним додатком, а таким, який сам може модифікувати елементи мережі, як наприклад, відновлення після атак, модифікація файерволу, перевірка цілісності файлів, пошук вразливостей, у той час як IDS лише фіксують трафік, що проходить мережею та сповіщає адміністратора.

Висновки до першого розділу

1. Системи виявлення вторгнень пройшли тривалий етап розвитку – від базових засобів аналізу журналів подій до сучасних інтелектуальних платформ, що використовують технології штучного інтелекту. Їх удосконалення стало відповіддю на постійне зростання складності кіберзагроз і стрімкий розвиток інформаційних технологій. На сучасному етапі IDS відіграють важливу роль у забезпеченні кібербезпеки, оскільки дозволяють своєчасно виявляти атаки та підвищувати рівень захисту інформаційних ресурсів.

2. Системи виявлення вторгнень (IDS) і системи запобігання вторгненням (IPS) є невід'ємними компонентами сучасної кібербезпеки, що забезпечують захист інформаційних ресурсів від різноманітних кіберзагроз. IDS здійснюють моніторинг мережевого трафіку та системних подій для виявлення підозрілої активності, тоді як IPS не лише визначають загрози, а й автоматично протидіють їм у режимі реального часу. Таким чином, IDS орієнтовані переважно на контроль і сповіщення, а IPS – на активне реагування та блокування атак. Отже, їх спільне використання є важливою умовою забезпечення ефективного кіберзахисту в сучасному цифровому середовищі.

3. Системи виявлення вторгнень поділяються на кілька основних типів: мережеві (NIDS), хостові (HIDS) та системи захисту застосунків (AIDS). Кожен із цих видів виконує власні функції у сфері кібербезпеки: NIDS аналізують мережевий трафік, HIDS контролюють події на окремих пристроях, а AIDS забезпечують захист прикладного програмного забезпечення. Такий розподіл дозволяє ефективно виявляти різні види загроз і створювати багаторівневу систему захисту. Отже, комплексне застосування різних типів IDS сприяє підвищенню ефективності моніторингу, оперативності реагування на інциденти та загального рівня безпеки інформаційної інфраструктури.

4. Архітектура систем виявлення вторгнень базується на взаємодії ключових компонентів: сенсорів збору даних, модуля аналізу, бази даних і блоку реагування. Кожен із цих елементів виконує важливі функції, необхідні для ефективного виявлення та аналізу подій безпеки. Особливу роль відіграє підсистема аналізу, оскільки саме від її ефективності залежить точність виявлення загроз і швидкість реагування на них. Завдяки модульній структурі IDS можуть інтегруватися з іншими засобами кіберзахисту, зокрема IPS, міжмережевими екранами та системами управління безпекою. Поєднання IDS та IPS забезпечує комплексний підхід до моніторингу, виявлення та запобігання атакам, що значно підвищує рівень захисту інформаційної інфраструктури.

РОЗДІЛ 2. МОДЕЛЮВАННЯ АДАПТИВНОЇ IDS НА ОСНОВІ ГІБРИДНИХ МЕТОДІВ

2.1. Адаптивні системи виявлення вторгнень

Поняття адаптивності у сфері інформаційної безпеки пов’язується зі здатністю системи змінювати свої параметри та модель функціонування у відповідь на зміну середовища загроз. Основи адаптивного підходу до виявлення вторгнень були закладені у роботі Dorothy E. Denning An Intrusion-Detection Model (1987) [3, с. 222-232], де запропоновано механізм формування та оновлення профілю нормальної поведінки користувачів. Подальший розвиток ці ідеї отримали у працях Teresa F. Lunt [25, с. 22-46], яка розглядала автоматичне коригування профілів для підвищення точності виявлення атак.

У ширшому контексті адаптивність систем безпеки описується у книзі Security Engineering авторства Ross Anderson [26], де наголошується на необхідності динамічного реагування на еволюцію загроз. Теоретичні засади адаптивних систем базуються також на визначенні навчання як процесу покращення продуктивності на основі досвіду, запропонованому Tom M. Mitchell у праці Machine Learning [27].

Таким чином, у сучасному розумінні адаптивність IDS полягає у здатності системи самонавчатися, оновлювати моделі виявлення та підтримувати ефективність функціонування в умовах динамічного кіберсередовища.

Як зазначено у п.п. 1.3, у процесі функціонування системи виявлення вторгнень (IDS) здійснюється безперервний моніторинг і аналіз мережевих та системних даних з метою виявлення аномальних дій, підозрілих з’єднань і ознак кібератак. Залежно від архітектури, IDS можуть реалізовуватися як програмні агенти, апаратні сенсори або комплексні рішення і основними методами їх реалізації є сигнатурний (signature-based) та аномалійний (anomaly-based).

Системи виявлення вторгнень (IDS) залишаються предметом активних досліджень і вдосконалення протягом останніх десятиліть. Сучасні наукові роботи зосереджені на підвищенні точності класифікації атак, зменшенні кількості помилкових спрацювань (false positives) та пропущених атак (false negatives), а також на розробці рішень, здатних працювати в режимі реального часу та адаптуватися до нових загроз [28, 29, 30].

Особливу увагу приділено адаптивним методам виявлення атак, які здатні динамічно реагувати на зміни у характеристиках мережевого трафіку. Такі підходи спрямовані на подолання основного недоліку класичних методів – обмеженої здатності виявляти нові або модифіковані атаки, що не відповідають заздалегідь визначеним шаблонам.

Адаптивні системи виявлення вторгнень (Adaptive IDS) – це IDS, здатні самостійно підлаштовуватися під змінні умови роботи мережі або хосту, покращуючи точність виявлення атак. На відміну від традиційних систем, адаптивні IDS не лише сповіщають про аномалії, а й оновлюють свої моделі поведінки та сигнатури на основі аналізу попередніх подій.

Серед перспективних напрямів виділяється застосування методів машинного навчання та алгоритмів онлайн-навчання, які дозволяють IDS оновлювати свої моделі безпосередньо під час функціонування. Водночас більшість запропонованих рішень мають певні обмеження, зокрема ґрунтуються на припущенні про відносну статичність характеристик атак або навчальних даних, що не завжди відповідає реальній динаміці загроз у корпоративних мережах. Найбільш поширені адаптивні системи IDS та методи їх реалізації наведені в табл. 2.1.

Адаптивні системи виявлення вторгнень (IDS) можна класифікувати за рівнем реалізації механізмів адаптації до змін параметрів мережевого середовища та нових типів атак без повного ручного втручання адміністратора. Адаптивність досягається завдяки використанню алгоритмів машинного навчання, потокового навчання, ансамблевих методів та зворотного зв’язку. Такі підходи суттєво розширюють можливості класичних IDS у виявленні нових і змінених загроз [39].

Таблиця 2.1 – Адаптивні системи IDS та методи їх реалізації

Адаптивна система IDS	Методи реалізації адаптивності / Рівень адаптивності	Основні алгоритми	Характеристика адаптивності
ML-IDS з потоковим навчанням	Моделі онлайн-навчання (Online Learning) / Високий	SGD, Hoeffding Tree, Online NB	Використовує алгоритми онлайн-навчання для постійного оновлення моделей класифікації атак. Підлаштовується під зміни мережевого трафіку в реальному часі, швидко реагує на нові типи атак
Adaptive Random Forests, гібридні IDS	Розширені ансамблеві методи / Високий	ARF, Random Forest, Boosting, ADWIN	Поєднують декілька дерев рішень у ансамблі, який динамічно адаптує структуру при надходженні нових даних. Підвищують точність виявлення та зменшують false positives
Кластерні IDS, аномалійні системи	Інкрементальні методи кластеризації / Середній-високий	k-means, DBSCAN, Isolation Forest	Використовують інкрементальну кластеризацію для формування профілів нормальної поведінки мережі. Виявляють аномалії без попередньо відомих сигнатур, підлаштовуючись під поточний стан мережі.
NIDS/HIDS з ML, Behavior-based IDS	Аномалійні IDS з ML / Середній	SVM, ANN, CNN, LSTM	Поєднують методи машинного навчання та поведінковий аналіз. Виявляють відхилення у поведінці користувачів і процесів, дозволяють ідентифікувати нові атаки.
Snort з ML модулем, OSSEC розширений	Гібридні IDS з динамічним оновленням правил / Середній	Signature + Random Forest / SVM, Rule-based + ML	Гібридні системи, які поєднують сигнатурний та аномалійний підходи з адаптивним оновленням правил. Підвищують ефективність у виявленні нових і модифікованих атак.
HIDS (OSSEC, Tripwire)	Поведенкові IDS (Behavior-based IDS) / Низький	Hash-функції, rule-based	Фокусуються на захисті окремих хостів. Відстежують зміни файлової системи, реєстру та процесів, застосовуючи адаптивні профілі поведінки користувачів.
AdaptIDS, Adaptive Security Systems	Самоналаштовувальні IDS із зворотним зв’язком / Високий	Reinforcement Learning, Fuzzy Logic	Самоналаштовувальні IDS із зворотним зв’язком. Використовують адміністраторський або автоматичний фідбек для динамічної зміни порогів та моделей, зменшення false positives/negatives.

Джерело: побудовано автором на підставі [31-38]

За рівнем реалізації адаптивних механізмів адаптивні IDS можна розподілити на три групи:

1. Системи з низьким рівнем адаптивності. До них належать класичні HIDS, зокрема системи контролю цілісності файлів, такі як Tripwire та OSSEC у базовій конфігурації. Такі системи можуть використовувати статистичні пороги та контроль цілісності, але не здатні до самостійного оновлення моделей.

2. Системи із середнім рівнем адаптивності. До цієї категорії відносяться гібридні IDS, що поєднують сигнатурний та аномалійний підходи, а також NIDS/HIDS із методами машинного навчання. Ці системи реалізують часткову адаптацію шляхом періодичного оновлення правил або моделей на основі історичних даних. Наприклад, Snort у поєднанні з ML-модулем дозволяє частково оновлювати правила та підвищувати точність детекції.

3. Системи з високим рівнем адаптивності. Це ML-IDS з потоковим навчанням, Adaptive Random Forests та самоналаштовувальні системи типу AdaptIDS. Вони використовують алгоритми онлайн-навчання, ансамблеві методи та механізми зворотного зв'язку, що забезпечують автоматичне оновлення моделей у режимі реального часу та підтримку concept drift [40].

Отже, ключовими ознаками адаптивної IDS є:

– *динамічне оновлення моделей*. Система автоматично оновлює параметри або структуру моделі при надходженні нових даних (online / incremental learning);

– *реагування в режимі реального часу*. Обробка потокових даних без зупинки системи та без повного перенавчання;

– *виявлення нових (невідомих) атак*. Орієнтація не лише на сигнатури, а й на поведінкові або аномалійні ознаки;

– *самоналаштування параметрів*. Автоматичне коригування порогів спрацювання, ваг ознак, правил класифікації;\

– *зворотний зв'язок (feedback loop).* Використання підтверджень адміністратора або автоматичного аналізу для покращення точності;

– *зниження рівня хибних спрацювань*. Адаптація дозволяє зменшити кількість false positives та false negatives;

– *підтримка мінливості трафіку (concept drift handling).* Система враховує зміну статистичних характеристик мережевого середовища;

– *гібридність підходів*. Часто поєднує сигнатурний, аномалійний та ML-підходи.

У сучасних умовах розвитку кіберзагроз традиційні сигнатурні системи виявлення вторгнень дедалі частіше виявляються недостатньо ефективними для протидії новим та модифікованим атакам. Класичні IDS функціонують переважно на основі заздалегідь визначених правил і сигнатур, що забезпечує високу точність при виявленні відомих загроз, однак обмежує їх здатність реагувати на невідомі або змінені типи атак [34].

Натомість адаптивні IDS базуються на використанні методів машинного навчання, поведінкового аналізу та потокового навчання, що дозволяє їм автоматично оновлювати моделі детекції та враховувати зміни характеристик

мережевого трафіку (concept drift) [32]. Завдяки цьому вони здатні виявляти нові загрози без необхідності ручного додавання сигнатур, однак потребують більших обчислювальних ресурсів і складніших механізмів налаштування [39].

З метою систематизації відмінностей між традиційними та адаптивними підходами до виявлення вторгнень у табл. 2.2 наведено їх порівняльну характеристику за основними критеріями ефективності, адаптивності та експлуатаційних особливостей.

Таблиця 2.2 – Порівняння класичних і адаптивних IDS

Критерій	**Класичні IDS**	**Адаптивні IDS**
Підхід до виявлення	Сигнатурний / статичний	ML-орієнтований / адаптивний
Виявлення нових атак	Низька ефективність	Висока (zero-day)
Concept drift	Не підтримується	Підтримується
Хибні спрацювання	Часто висока кількість	Може зменшуватися з навчанням
Час реакції	Обмежений правилами	Швидкий при потоковому навчанні
Обчислювальні ресурси	Низькі	Високі
Автоматичне оновлення	Немає	Так
Інтерпретація результатів	Зрозуміла	Може бути складною

Джерело: побудовано автором на підставі [32, 34, 39]

Як видно з табл. 2.2, адаптивні IDS демонструють істотні переваги над класичними, зокрема здатність виявляти невідомі атаки та адаптуватися до змінних умов мережі, але потребують більшої обчислювальної потужності та мають складніші механізми інтерпретації результатів.

Сучасні адаптивні методи виявлення атак, попри численні переваги, мають суттєві обмеження, що впливають на їхню ефективність у реальних умовах.

По-перше, більшість алгоритмів онлайн-навчання або адаптивної кластеризації розробляються та тестуються для певного набору даних або конкретного типу атак. Через це вони демонструють високу точність лише в середовищі, для якого були оптимізовані. У разі швидкої зміни характеру загроз або мережевої інфраструктури моделі швидко втрачають актуальність. Особливо це проблематично у великих корпоративних чи державних мережах, де одночасно присутні різні типи атак, а умови середовища постійно змінюються.

По-друге, здатність адаптивних методів оновлювати параметри під час обробки нових даних може призвести до «забування» старих шаблонів або нормальної поведінки системи. Це явище, відоме як concept drift, знижує

здатність IDS розпізнавати добре відомі загрози, створюючи своєрідні «сліпі зони» у захисті. Таким чином, система стає надто гнучкою щодо нових загроз, але одночасно втрачає чутливість до відомих атак.

По-третє, сучасні адаптивні методи, особливо ансамблеві та інкрементальні алгоритми, мають високі обчислювальні потреби. Для обробки великого потоку мережевих подій у реальному часі потрібні потужні сервери або спеціалізоване обладнання, що обмежує застосування методів у малих організаціях або середовищах з обмеженими ресурсами. Затримки у обробці трафіку можуть знижувати оперативність реагування на загрози, що критично для запобігання серйозним інцидентам безпеки [41].

У підсумку, адаптивні методи IDS ефективні у певних сценаріях, але їхня універсальність, стабільність проти змін загроз і вимоги до ресурсів обмежують широке застосування. Баланс між гнучкістю, навчанням на нових даних та стійкістю проти відомих атак залишається ключовим викликом у їхній практичній реалізації.

2.2. Гібридні методи в задачах кібербезпеки

Сучасний цифровий світ динамічно розвивається завдяки впровадженню технологій хмарних обчислень, Інтернету речей (IoT) та великих даних, однак зростання цієї цифрової інфраструктури супроводжується дедалі складнішими кібератаками. Особливо вразливими виявляються розподілені інформаційні системи, які широко застосовують у сферах критичної інфраструктури (енергетика, транспорт, зв’язок), бізнесі та державному управлінні. У таких системах необхідно гарантувати високий рівень конфіденційності, цілісності й доступності даних та сервісів [42].

Одним із ефективних підходів у цьому напрямку є розробка гібридних методів виявлення. Під гібридними методами розуміють поєднання двох або більше підходів для виявлення або запобігання кібератакам, наприклад, сигнатурного та поведінкового аналізу, машинного навчання та експертних правил, IDS та IPS, статистики та AI.

Використання таких методів дозволяє підвищити ефективність детекції загроз та зменшити частоту хибних спрацювань [43, 44].

Таблиця 2.3 – Гібридні методи в кібербезпеці

№	Гібридний метод	Компоненти	Опис	Переваги	Застосування	Приклади алгоритмів / систем
1	Сигнатурний + поведінковий аналіз	Шаблони + аномалії	Поєднання детекції відомих атак через сигнатури та виявлення невідомих аномалій	Висока точність, здатність виявляти zero-day атаки	Антивірусні програми, IDS/IPS	Snort, Suricata, ClamAV, Bro/Zeek
2	Машинне навчання + експертні правила	ML + rule-based	Комбінація адаптивного навчання і правил, визначених експертами	Пояснюваність, гнучкість, адаптація до нових атак	Антифрод, SOC системи, аналіз мережевого трафіку	Random Forest, SVM, Decision Trees + правила експертів
3	IDS + IPS	Виявлення + блокування	Поєднання пасивного моніторингу та активного блокування загроз у реальному часі	Реакція в реальному часі, скорочення впливу атак	Корпоративні мережі, центри кібербезпеки	Snort + pfSense IPS, Suricata IDS/IPS, Cisco Firepower
4	Кластеризація + машинне навчання	Групування + ML	Виявлення прихованих аномалій і нових типів атак шляхом кластеризації даних та аналізу поведінки	Виявлення складних і невідомих атак, адаптивність	SOC, аналітика кібербезпеки, детекція аномалій	K-Means + Random Forest, DBSCAN + Neural Networks
5	Статистичні методи + AI	Статистика + нейромережі	Аналіз і прогнозування загроз на основі статистичних патернів та моделей AI	Прогнозування атак, виявлення аномалій	Аналіз мережевого трафіку, прогнозні системи кібербезпеки	ARIMA + LSTM, Bayesian Networks, Autoencoders
6	Deep Learning + Big Data	DL + Hadoop/Spark	Обробка великих обсягів даних для виявлення складних загроз	Високоточне виявлення атак, масштабованість	Threat detection, аналітика кібербезпеки	CNN/RNN/LSTM на Spark, TensorFlow, PyTorch, ELK + DL моделі

Джерело: [45-48]

Сигнатурний + поведінковий аналіз. Цей гібридний метод поєднує сигнатурну детекцію відомих атак (тобто порівняння активності зі заздалегідь визначеними шаблонами загроз) із поведінковим аналізом, що здатен виявляти невідомі чи аномальні дії. Такий підхід дає змогу значно розширити спектр виявлених атак – від традиційних вірусів і шкідливих пакетів до «zero-day» експлойтів, які ще не мають сигнатур [43].

Сигнатурно-поведінкові системи можуть, наприклад, моніторити мережевий трафік для відомих шаблонів і виявляти незвичні характеристики потоку, що можуть вказувати на нову загрозу. Hybrid IDS, які поєднують ці

підходи, показують кращу здатність розпізнавання атак без значного зростання хибних спрацювань [44].

Машинне навчання + експертні правила. Комбінація машинного навчання (ML) з експертними системами (rule-based) охоплює сильні сторони обох підходів: ML-алгоритми здатні автоматично виявляти складні шаблони й аномалії, а експертні правила забезпечують логіку та пояснюваність рішень.

У таких рішеннях модель навчання може перш за все обробляти велику кількість ознак поведінки мережевого трафіку чи системних подій, а правила експертів уточнювати класифікацію та ініціювати заходи реагування. Перевагою є зменшення частки хибних спрацювань і підвищення довіри до результатів — оскільки правила надають контекст-логіку, а ML забезпечує адаптивність [49].

IDS + IPS. Інтеграція систем виявлення вторгнень (IDS) з системами запобігання вторгнень (IPS) – це гібридний підхід, що поєднує виявлення аномалій із автоматичним блокуванням загроз у реальному часі. IDS відповідає за моніторинг і аналіз подій, а IPS – за миттєве реагування, наприклад, шляхом фільтрації трафіку чи блокування підозрілих IP-адрес.

Такі системи ефективні у корпоративних мережах, де швидке припинення атаки мінімізує потенційні збитки. Наприклад, сигнатурні та політичні підходи можуть комбінуватися в IDS/IPS для побудови гібридної логіки, що одночасно враховує правила безпеки й поточну поведінку трафіку [50].

Кластеризація + машинне навчання. Гібридний підхід, що поєднує кластеризацію даних (unsupervised learning) із супервізованим ML, покликаний виявляти приховані аномалії та нетипові шаблони, які не фігурують у відомих наборах сигнатур чи правилах [51].

Кластеризація групує схожі події або трафік за поведінковими патернами, після чого ML-алгоритми аналізують ці групи для визначення потенційно шкідливої активності. Такий підхід особливо корисний в складних мережах або IoT-середовищах, де традиційні методи можуть пропустити складні багатокомпонентні атаки.

Статистичні методи + штучний інтелект (AI). Статистичні методи аналізу використовуються для виявлення загальних патернів у даних, тоді як штучний

інтелект/нейронні мережі підтримують роботу із великими обсягами даних та складними взаємозв’язками. У поєднанні вони дозволяють не лише виявляти аномальні події, але й прогнозувати ризики, прогнозувати тенденції загроз і оптимізувати моделі виявлення. Такий гібридний підхід особливо ефективний у Threat Intelligence та аналізі масштабних наборів даних, де прості правила вже недостатні [52].

6. Deep Learning + Big Data. Поєднання глибокого навчання (Deep Learning) із технологіями обробки великих даних (Big Data) створює сучасні гібридні моделі, які можуть аналізувати масивні обсяги мережевого та системного трафіку в реальному часі для виявлення складних та нових загроз.

Deep Learning дозволяє моделювати складні нелінійні патерни поведінки, що значно підвищує точність виявлення розподілених, багатоетапних атак чи складних аномалій, які класичні ML-методи могли б пропустити [53].

Гібридні методи у кібербезпеці демонструють, що комбінація кількох підходів здатна значно підвищити ефективність захисту, зменшити частоту хибних спрацювань та розширити діапазон виявлених загроз. Поєднання сигнатурних, поведінкових, статистичних, ML/AI-методів – є сучасним трендом для побудови адаптивних та масштабованих систем захисту, здатних протистояти еволюціонуючим загрозам у складних IT-інфраструктурах.

2.3. Формалізація задачі виявлення вторгнень

Задача виявлення вторгнень (Intrusion Detection) є однією з ключових у сфері кібербезпеки та полягає у своєчасному виявленні несанкціонованої або шкідливої активності в інформаційних системах і мережах. Для побудови ефективних систем виявлення вторгнень необхідно формалізувати цю задачу з точки зору математичних моделей і алгоритмів обробки даних.

Нехай задано множину об’єктів спостереження:

$$X = \{x_1, x_2, \ldots, x_n\} \quad (2.1)$$

де x_i – це окремий запис (мережевий пакет, сесія, подія в системі), що описується вектором ознак:

$$x_i = (f_1, f_2, \ldots, f_m) \quad (2.2)$$

де f_j – значення j-ї ознаки (наприклад, IP-адреса, порт, протокол, обсяг трафіку, час сесії тощо).

Кожному об'єкту x_i відповідає клас:

$$y_i \in \{0,1\} \quad (2.3)$$

де:

- 0 – *нормальна поведінка (benign);*
- 1 – *вторгнення (malicious).*

Таким чином, задача виявлення вторгнень зводиться до побудови відображення:

$$F: X \to Y \quad (2.4)$$

яке дозволяє класифікувати нові об'єкти як нормальні або шкідливі [54].

Задача виявлення вторгнень може бути сформульована у вигляді кількох основних типів задач залежно від доступності даних, способу навчання та підходу до аналізу. Найбільш поширеними є задачі класифікації, виявлення аномалій та напівконтрольованого навчання. Формалізація залежить від підходу:

1. **Задача класифікації (Supervised Learning).** Формально навчальна вибірка задається як:

$$D = \{(x_i, y_i)\}_{i=1}^{n} \quad (2.5)$$

Мета полягає у побудові функції класифікації:

$$F(x): X \to Y \quad (2.6)$$

де $Y = \{0,1\}$ або множина типів атак.

Цей підхід широко використовується в системах, де доступні розмічені дані. До його переваг належать висока точність і можливість детального розпізнавання типів атак. Недоліком є залежність від якості та повноти навчальної вибірки.

2. Задача виявлення аномалій (Unsupervised Learning). Важливим підходом у задачі виявлення вторгнень є виявлення **аномалій**, яке базується на припущенні, що шкідлива активність суттєво відрізняється від нормальної поведінки системи. У цьому випадку будується модель нормального стану

$Normal$, а всі відхилення від нього розглядаються як потенційні атаки:

$$anomaly(x) = \begin{cases} 1, & x \notin Normal \\ 0, & x \in Normal \end{cases} \quad (2.7)$$

де $Normal$ – множина об'єктів, що відповідають нормальній поведінці системи.

Перевагою цього підходу є можливість виявлення **нових і невідомих атак (zero-day)**. Однак він часто супроводжується більшою кількістю хибних спрацювань.

3. Напівконтрольоване навчання (Semi-supervised Learning). Цей підхід є компромісом між попередніми двома і передбачає використання невеликої кількості розмічених даних разом із великою кількістю нерозмічених.

Формально:

$$D = D_l \cup D_u \quad (2.8)$$

де:

- D_l *– розмічені дані,*
- D_u *– нерозмічені дані.*

Модель використовує D_l для початкового навчання та уточнює свої параметри на основі структури D_u. Такий підхід дозволяє зменшити витрати на розмітку даних і підвищити ефективність у реальних умовах [55].

4. Гібридні задачі виявлення вторгнень. У сучасних системах кібербезпеки часто використовується **гібридна постановка задачі**, яка поєднує кілька підходів одночасно, тобто використовується комбінація декількох функцій:

$$F(x) = \alpha F_{sig}(x) + \beta F_{anom}(x) + \gamma F_{ml}(x) \quad (2.9)$$

де:

- F_{sig} *– сигнатурна модель,*
- F_{anom} *– модель аномалій,*
- F_{ml} *– модель машинного навчання,*
- α, β, γ *– вагові коефіцієнти.*

Рішення про наявність вторгнення приймається на основі порогової функції:

$$F(x) > T \Rightarrow \text{вторгнення} \quad (2.10)$$

Такий підхід забезпечує більш високу ефективність виявлення загроз і є основою сучасних IDS/IPS систем.

Формалізація задачі виявлення вторгнень має такі особливості: незбалансованість даних (кількість нормальних подій значно перевищує атаки), динамічність середовища (постійна поява нових типів атак), великий обсяг даних (Big Data), необхідність роботи в реальному часі.

Таким чином, задача виявлення вторгнень може бути сформульована як задача класифікації, виявлення аномалій або їх комбінації. Вибір конкретного підходу залежить від доступності даних, вимог до точності та умов застосування. Найбільш ефективними є гібридні підходи, які поєднують кілька типів задач і дозволяють одночасно виявляти як відомі, так і нові кіберзагрози [56].

Для оцінювання ефективності систем виявлення вторгнень використовуються спеціальні **метрики**, які дозволяють кількісно визначити якість роботи моделі. Оскільки задача виявлення вторгнень є задачею класифікації, оцінювання базується на матриці помилок (*confusion matrix*).

Матриця помилок включає такі компоненти:

– TP (True Positive) – правильно виявлені атаки;
– TN (True Negative) – правильно визначена нормальна активність;
– FP (False Positive) – нормальна активність, помилково визначена як атака;
– FN (False Negative) – атака, яку система не змогла виявити.

Розглянемо основні метрики.

1. **Точність (Accuracy).** Показує загальну частку правильних рішень:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \tag{2.11}$$

Однак у задачах кібербезпеки ця метрика може бути неінформативною через незбалансованість даних.

2. Точність позитивних спрацювань (Precision) визначає, яка частка виявлених атак є дійсно атаками:

$$Precision = \frac{TP}{TP+FP} \tag{2.12}$$

Високе значення Precision означає низьку кількість хибних спрацювань.

3. Повнота (Recall, Detection Rate) показує, яку частку атак система змогла виявити:

$$Recall = \frac{TP}{TP+FN} \quad (2.13)$$

Це одна з найважливіших метрик у кібербезпеці, оскільки пропущені атаки (FN) є критично небезпечними.

4. F1-score є гармонійним середнім між Precision та Recall:

$$F1 = 2 \cdot \frac{Precision \cdot Recall}{Precision+Recall} \quad (2.14)$$

Дозволяє збалансовано оцінити модель при нерівномірному розподілі класів [57].

Окрім базових метрик метрик (Accuracy, Precision, Recall, F1-score), доцільно використовувати **додаткові показники**, які враховують специфіку задачі виявлення вторгнень, зокрема незбалансованість даних та вимоги до швидкості реагування. До основних додаткових метрик належать Specificity, False Alarm Rate, Matthews Correlation Coefficient, ROC-AUC та Time to Detect. Використання цих метрик дозволяє більш повно оцінити ефективність системи в умовах реальної експлуатації.

1. Specificity (True Negative Rate, TNR)

Показує здатність системи правильно визначати нормальну активність і дуже актуально для SOC (щоб не «завалити» аналітиків алертами):

$$TNR = \frac{TN}{TN+FP} \quad (2.15)$$

Високе значення означає низьку кількість хибних тривог.

2. False Alarm Rate (FAR) – у кібербезпеці це одна з ключових метрик, є прямою протилежністю до Specificity – показує рівень «шуму» системи:

$$FAR = \frac{FP}{FP+TN} \quad (2.16)$$

3. Matthews Correlation Coefficient (MCC) – комплексна метрика дає об'єктивну оцінку всієї моделі, добре працює при незбалансованих даних [58]:

$$MCC = \frac{TP \cdot TN - FP \cdot FN}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}} \quad (2.17)$$

Значення:

– + 1– ідеальна класифікація;
– 0 – випадкова;
– 1 – повністю неправильна.

4. ROC-AUC (або PR-AUC) – оцінює модель **на різних порогах;** PR-AUC особливо важлива при **рідкісних атаках** [59].

5. Time to Detect (TTD) – особливо важлива для систем реального часу, показує середній час виявлення атаки:

$$TTD = t_{detect} - t_{attack} \quad (2.18)$$

Метрики оцінювання є ключовим інструментом аналізу ефективності систем виявлення вторгнень. Вибір метрик залежить від конкретних вимог системи, однак у кібербезпеці особливу увагу приділяють мінімізації пропущених атак і контролю рівня хибних спрацювань.

Висновки до другого розділу

1. Адаптивні системи виявлення вторгнень є важливим етапом розвитку сучасних засобів кібербезпеки, оскільки здатні змінювати принципи своєї роботи залежно від нових загроз і особливостей функціонування інформаційних систем. На відміну від традиційних IDS, вони застосовують методи машинного навчання, поведінкового аналізу та штучного інтелекту для виявлення аномалій і невідомих атак у режимі реального часу. Головними перевагами таких систем є здатність до самонавчання, підвищення точності аналізу та зменшення кількості хибних спрацювань. Отже, використання адаптивних IDS сприяє підвищенню ефективності кіберзахисту, швидкості реагування на інциденти та стійкості інформаційних систем до сучасних кіберзагроз.

2. Гібридні методи належать до найбільш перспективних напрямів розвитку систем кібербезпеки, оскільки дозволяють об’єднати переваги різних підходів до виявлення та протидії атакам. Поєднання сигнатурного аналізу, поведінкових методів, машинного навчання, кластеризації, статистичних моделей та адаптивних алгоритмів забезпечує підвищення точності функціонування систем виявлення вторгнень і зниження кількості помилкових спрацювань. Завдяки цьому гібридні підходи забезпечують більш надійний і комплексний захист інформаційних ресурсів в умовах постійного розвитку кіберзагроз.

3. Важливу роль у створенні адаптивних систем відіграють методи машинного навчання та кластерного аналізу, які дозволяють виявляти приховані закономірності у мережевому трафіку та визначати нові типи атак без використання заздалегідь створених сигнатур. Сучасні гібридні підходи, зокрема поєднання сигнатурного та поведінкового аналізу, машинного навчання й експертних правил, IDS та IPS, кластеризації та штучного інтелекту, забезпечують високий рівень захисту інформаційних систем і здатність адаптуватися до змін у кіберпросторі. Таким чином, застосування гібридних методів дозволяє створювати інтелектуальні системи виявлення вторгнень, які ефективно працюють у реальному часі та забезпечують надійний кіберзахист сучасних мереж і інформаційних ресурсів.

4. У процесі формалізації задачі виявлення вторгнень були визначені основні компоненти системи: множина подій, набір ознак, механізми класифікації та критерії прийняття рішень. Задача виявлення вторгнень розглядається як задача бінарної класифікації мережевого трафіку на нормальний та аномальний.

Запропоновані математичні моделі дозволяють описати процес аналізу мережевих подій і створюють основу для використання сучасних методів машинного навчання та інтелектуального аналізу даних. Формалізований підхід забезпечує підвищення точності виявлення атак, зменшення кількості хибних спрацювань і підвищення рівня захисту інформаційних систем.

Значну увагу приділено гібридним системам виявлення вторгнень, які поєднують сигнатурні методи, аналіз аномалій та алгоритми машинного навчання. Використання такого підходу дозволяє ефективніше виявляти як відомі, так і нові типи атак, а також підвищує адаптивність системи до змін мережевого середовища. Крім того, важливим елементом оцінювання ефективності IDS є використання спеціальних метрик, які дають змогу комплексно аналізувати якість роботи моделей, контролювати рівень хибних спрацювань та мінімізувати кількість пропущених атак.

РОЗДІЛ 3. РОЗРОБКА ТА РЕАЛІЗАЦІЯ АДАПТИВНОЇ ГІБРИДНОЇ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ

3.1. Розробка гібридної моделі адаптивної IDS

Розробка гібридної адаптивної IDS (Intrusion Detection System) – це сучасний підхід до виявлення кіберзагроз. Суть гібридної системи виявлення вторгнень (IDS) полягає в поєднанні методів виявлення на основі сигнатур та на основі аномалій, що дозволяє використовувати переваги обох підходів. Виявлення на основі сигнатур забезпечує швидшу обробку та нижчий рівень помилкових спрацьовувань, тоді як виявлення на основі аномалій підвищує точність завдяки виявленню нових або раніше невідомих атак. Щоб використати переваги обох методів, гібридні парадигми виявлення інтегрують дві групи алгоритмів у взаємодоповнювальну систему дотримуючись принципів, продемонстрованих у гібридних інтелектуальних архітектурах для складних і динамічних середовищ [60].

Архітектура гібридної моделі IDS складається з послідовності етапів обробки мережевого трафіку (рис. 3.1):

– виокремлення ознак (Feature Extraction);
– первинне виявлення аномалій (кластеризація – Anomaly Detection);
– ідентифікація атак (класифікація – Attack Identification);
– адаптивне оновлення моделі (адаптивне навчання – Model Update).

Feature Extraction (виокремлення ознак) – це один із ключових етапів у побудові IDS, де «сирий» мережевий трафік перетворюється у числові характеристики (features), які модель може аналізувати. На початковому етапі здійснюється отримання мережевих даних із джерел (мережеві інтерфейси, журнали подій або файли формату PCAP).

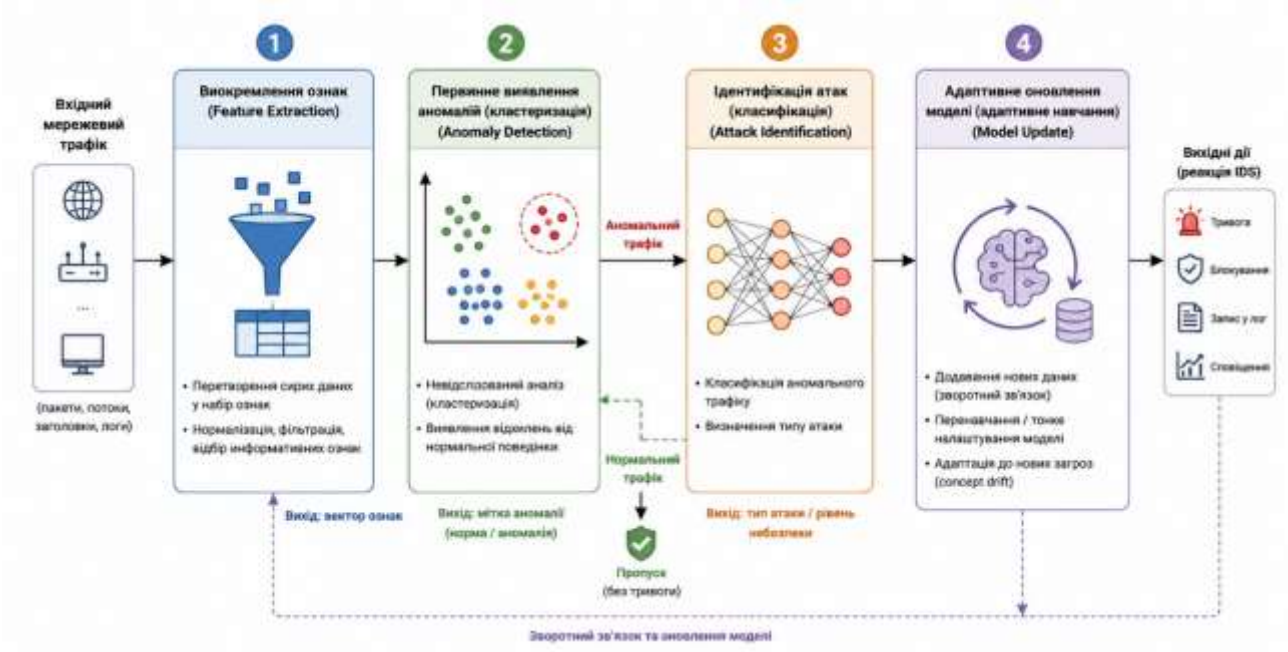


Рисунок 3.1 – Архітектура гібридної адаптивної IDS

Джерело: Розроблено автором на основі [61-67] за допомогою https://notebooklm.google.com

У мережі дані виглядають як: пакети (packets), потоки (flows), сесії (sessions). Але алгоритми ML не працюють із «сирими пакетами», тому їх необхідно перетворити у **вектор ознак**:

$$X = (x_1, x_2, x_3, \ldots, x_n) \tag{3.1}$$

На першому етапі сирі мережеві дані перетворюються у структурований набір ознак. Для кожного мережевого потоку формується вектор характеристик, таких як: тривалість з'єднання, кількість пакетів, кількість байтів (вхід/вихід), протокол передачі (TCP, UDP, ICMP), статистичні параметри трафіку.

Ознаки можуть бути **статистичними** (середній розмір пакета, швидкість передачі (bytes/sec), кількість запитів за секунду; **поведінковими** (кількість підключень до одного IP, кількість невдалих логінів, частота SYN-запитів); **ознаки рівня TCP/IP** (TCP flags (SYN, ACK, FIN), стан з'єднання).

Feature Extraction робить дані зрозумілими для ML, зменшує шум, підвищує точність, впливає на якість виявлення атак. Feature Extraction – це процес перетворення мережевого трафіку у числовий опис поведінки системи, без нього IDS або не працює, або дає дуже слабкі результати.

Далі відбувається попередня обробка даних, виконується підготовка даних до аналізу, а саме: нормалізація або стандартизація ознак, усунення пропущених значень, кодування категоріальних змінних.

На **другому етапі** до підготовлених даних застосовується алгоритм кластеризації. **Кластеризація** для виявлення кібератак – метод пошуку закономірностей в нерозмічених даних. Протягом останнього десятиліття до систем виявлення вторгнень (IDS) застосовувались різні технології машинного навчання та інтелектуального аналізу даних, які відігравали важливу роль у захисті критичних комп'ютерних систем та мереж від кібератак.

Основною перевагою алгоритму кластеризації є здатність виявляти вторгнення без явних описів вторгнень, які зазвичай надаються експертами по кібербезпеці. Використання даних про шкідливі програми в методі кластеризації є підходящим, так як характеристики шкідливих даних майже аналогічні нормальним даним, однак вони не можуть приховати свою поведінку, яка відрізняється від нормальних даних. Таким чином, відмінності в поведінці можуть бути виявлені даним методом кластеризації.

Цей метод заключається в визначенні характеризуючого вектора кожного кластера для виявлення відхилення від середньостатистичного значення і на підставі відстані середньостатистичної характеристики певний пакет відноситься до того чи іншого кластеру.

Стандартний процес кластеризації можна поділити на кілька основних етапів: [61]:

– виділення та вибір найбільш репрезентативних характеристик з вихідного набору даних;

– вибір алгоритму кластеризації та метрик відповідно до суті проблеми;

– оцінка результату кластеризації з метою визначення валідності алгоритму;

– пояснення практичного результату кластеризації.

Алгоритм кластеризації можна представити у вигляді наступної схеми, представленої на рис. 3.2.

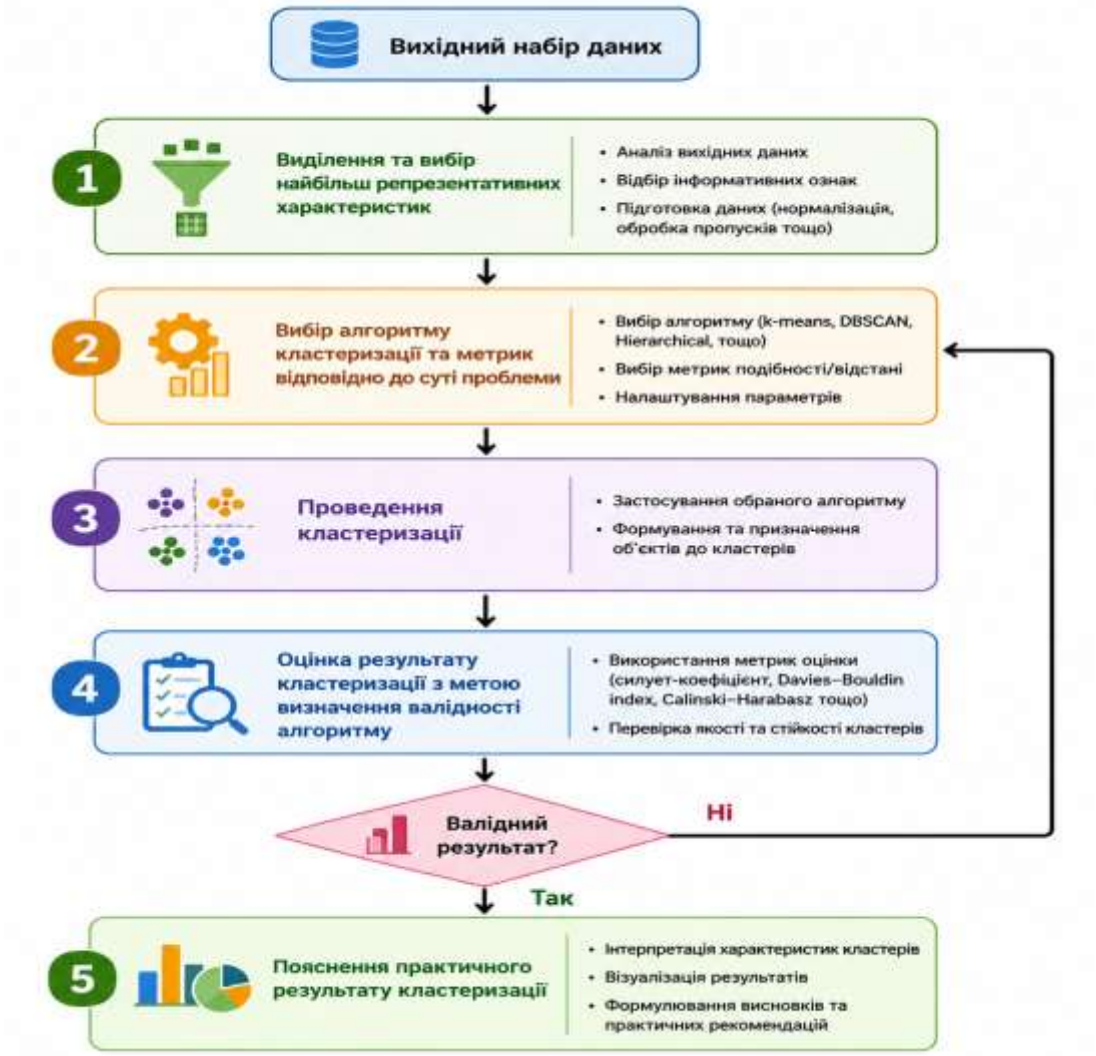


Рисунок 3.2 – Стандартний процес кластеризації

Джерело: розроблено автором на основі [61-67] за допомогою ChatGPT

Кластерний аналіз є потужним інструментом для дослідження багатовимірних даних, який дозволяє виявити внутрішні закономірності без попередніх припущень про структуру вибірки. Правильний вибір метрики подібності, кількості кластерів та алгоритму визначає ефективність і точність результатів кластеризації.

У процесі кластеризації даних важливим є вибір правильного методу, який буде найбільш ефективним для конкретної задачі. Існує багато алгоритмів кластеризації, кожен з яких має свої особливості та підходить для різних типів даних і завдань. Серед типів виділяють ієрархічні та неієрархічні, чіткі та нечіткі, алгоритми теорії графів та алгоритми, пов’язані з векторними моделями (рис. 3.3).

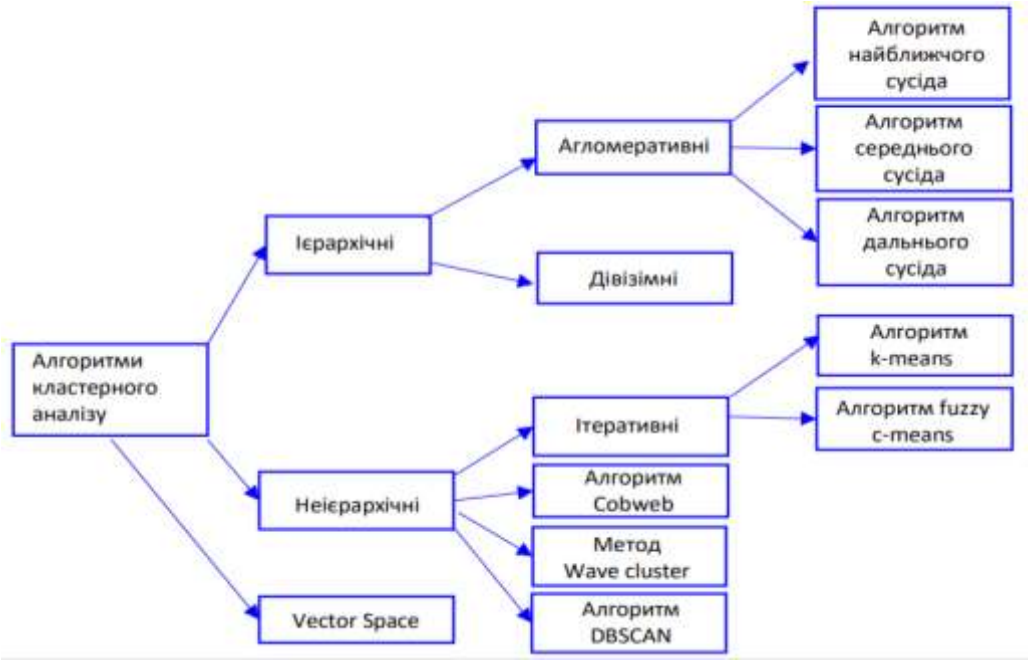


Рисунок 3.3 – Найбільш популярні алгоритми кластерного аналізу [62]

Розглянемо деякі з основних алгоритмів та їх характеристики.

Кластеризація методом k-середніх (K-means) є одним із найпростіших і популярних алгоритмів машинного навчання без нагляду. Як правило, неконтрольовані алгоритми роблять висновки з наборів даних, використовуючи лише вхідні вектори, не посилаючись на відомі або позначені результати.

Алгоритм роботи:

- Вибрати кількість кластерів k.
- Ініціалізувати k початкових центроїдів випадковим чином.
- Для кожної точки визначити найближчий центроїд (за обраною метрикою відстані, зазвичай – евклідовою).
- Перерахувати положення центроїдів як середнє всіх точок, що належать до відповідного кластера.
- Повторювати кроки 3–4 доки центроїди не стабілізуються (зміни незначні або відсутні).

Мета K-means проста: групувати схожі точки даних разом і виявляти основні закономірності. Для досягнення цієї мети K-means шукає фіксовану кількість (k) кластерів у наборі даних. Кластер відноситься до набора точок даних, агрегованих разом через певну схожість. Необхідно визначити цільове число k, яке відноситься до кількості центроїдів, які вам потрібні в наборі даних. **Центроїд** – це уявне або реальне розташування, що представляє центр

скупчення. Кожна точка даних розподіляється для кожного з кластерів шляхом зменшення внутрішньокластерної суми квадратів. Іншими словами, алгоритм K-середніх визначає k кількість центроїдів, а потім розподіляє кожну точку даних найближчому кластеру, залишаючи центроїди якомога меншими. «Середнє» в K-середніх відноситься до усереднення даних; тобто знайти центроїд. Мета методу – розділити n спостережень на k кластерів, так щоб кожне спостереження належало до кластера з найближчим до нього середнім значенням. Метод базується на мінімізації суми квадратів відстаней між кожним спостереженням та центром його кластера.

Принцип алгоритму полягає в пошуку таких центрів кластерів та наборів елементів кожного кластера при наявності деякої функції f (*), що виражає якість поточного розбиття множини на k кластерів, коли сумарне квадратичне відхилення елементів кластерів від центрів цих кластерів буде найменшим.

$$V = \sum_{i=1}^{k} \sum_{x \in S} (x_j - \mu_i)^2 \quad (3.2)$$

де k – число кластерів, S – отримані кластери, I = 1,2,3….k, μ – центроїд , xj – точки кластера.

Для більше детального розуміння алгоритм варто зобразити графічно (рис. 3.4). Для прикладу, необхідно взяти кількість k кластерів рівну 2, тобто K=2, щоб ідентифікувати набір даних і помістити їх у різні кластери. Потрібно вибрати кілька випадкових k точок або центроїд, щоб сформувати кластер. Ці точки можуть бути як точками з набору даних, так і будь-якою іншою точкою. У даному випадку, центроїди будуть обрані довільно (рис. 3.5)

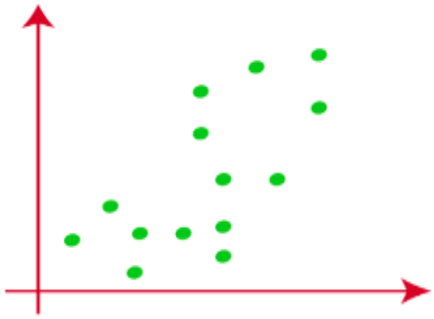


Рисунок 3.4 – Початкова модель дослідження [63]

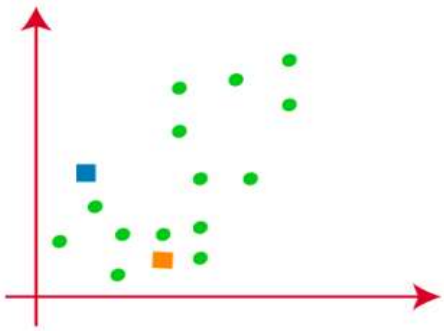


Рисунок 3.5 – Модель дослідження із довільними центроїдами [63]

Отже, наступним кроком необхідно зробити так, щоб кожен з n елементів на графіку був у складі певного кластеру, так щоб кожен елемент належав до кластера з найближчим до нього середнім значенням. Метод базується на мінімізації суми квадратів відстаней між кожним елементом та центром його кластера, тобто центроїдом. Далі, будуть застосовані обчислення, які вираховуватимуть суми відстаней між елементами та центроїдами (рис. 3.6).

Наступним кроком, необхідно обрати інший центроїд, таким же випадковим способом (рис. 3.7).

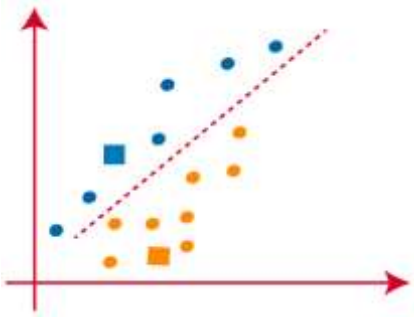


Рисунок 3.6 – Модель дослідження після виконаних операцій обчислення [63]

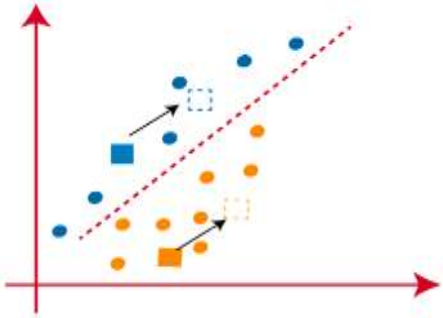


Рисунок 3.7 – Модель дослідження після вибору іншого центроїда [63]

Необхідно продовжувати зміщувати центроїди та проводити розрахунки до тих пір, поки не буде середнє квадратичне відхилення елементів найменшим (рис. 3.8).

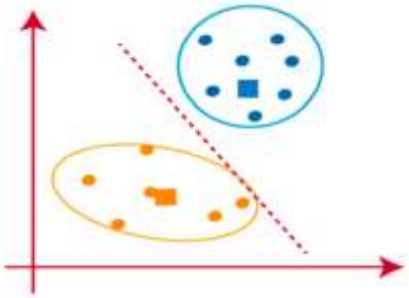


Рисунок 3.8 – Фінальний результат кластеризації [63]

Отже одразу після виконання певної кількості обчислень, отримаємо два кластери.

Переваги методу k-середніх (K-means): простота реалізації, висока швидкість обробки, підходить для великих наборів даних.

Недоліки методу k-середніх (K-means): необхідно задавати кількість кластерів k, чутливість до вибору k та початкових центрів; погано працює з кластерами довільної форми.

Алгоритм DBSCAN (Density-Based Spatial Clustering of Applications with Noise) – це алгоритм кластеризації даних, який ґрунтується на щільності даних. Основна ідея алгоритму DBSCAN полягає у виявленні щільних областей (кластерів) всередині даних та ідентифікації викидів (шуму, аномалій) на основі розподілу точок у просторі.

У 2014 році алгоритм DBSCAN отримав премію «перевірено часом» (премія дається алгоритмам, які отримали значну увагу в теорії і практиці) на провідній конференції з інтелектуального аналізу даних [64].

DBSCAN (Density-based spatial clustering of applications with noise) запропонували М. Естер, Г. Кригель, Y.Сандер і С. Су в 1996 році. Алгоритм слід використовувати для пошуку асоціацій і структур в даних, які важко знайти вручну, але які можуть бути актуальними і корисними для пошуку закономірностей і прогнозування тенденцій.

Основні параметри DBSCAN:

– ε – радіус околу точки;

– MinPts – мінімальна кількість сусідів у межах ε, щоб точка вважалась «основною».

Класифікація точок:

– **Core point (основна точка)** – має не менше ніж MinPts сусідів у радіусі ε;

– **Border point (гранична точка)** – має менше сусідів, але належить до околу основної точки;

– **Noise point (шумова точка)** – не належить до жодного кластера.

Основні концепції та ідеї алгоритму DBSCAN:

– DBSCAN починає з вибору випадкової точки даних і визначає, чи є ця точка «ядром» (core point) щільного кластера. Точка вважається ядром, якщо в заданому радіусі (epsilon, ε) від неї міститься не менше певної кількості точок (MinPts).

– Якщо точка є ядром, а всі точки в її радіусі також є ядрами (або досяжними з інших ядер), ці точки утворюють одну щільну область (кластер).

– Точки, що знаходяться всередині радіусу (ε) від ядра, але самі не є ядрами, вважаються граничними точками. Вони можуть бути частиною кластера, якщо пов'язані з ядром, але не можуть утворити окремі кластери.

– Точки, які не є ядрами і не знаходяться всередині радіусу (ε) від жодного ядра, вважаються викидами або шумом і не включаються до кластерів.

Алгоритм DBSCAN розглядає кластери як області високої щільності, розділені областями низької щільності. Завдяки цьому досить загальному погляду, кластери, знайдені DBSCAN, можуть мати будь-яку форму, на відміну від k-середніх, які припускають, що кластери мають опуклу форму.

Центральним компонентом DBSCAN є концепція кернових проб, тобто проб, що знаходяться в зонах високої щільності. Таким чином, кластер – це набір основних зразків, кожен з яких знаходиться близько один до одного (вимірюється деякою мірою відстані), і набір неосновних зразків, які близькі до основного зразка (але самі по собі не є основними зразками). Існує два параметри алгоритму, **min_samples і eps**, які формально визначають, що мається на увазі, коли говоримо про щільність. Вищі min_samples або менші eps вказують на вищу щільність, необхідну для формування кластера.

Більш формально, визначається базова вибірка як вибірка в наборі даних, що існує min_samples інших зразків на відстані eps, які визначаються як сусіди основної вибірки. Це говорить нам про те, що зразок ядра знаходиться в щільній області векторного простору. Кластер – це набір основних зразків, які можна побудувати шляхом рекурсивного взяття основного зразка, пошуку всіх його сусідів, які є основними зразками, пошуку всіх їхніх сусідів, які є основними зразками, і так далі. Кластер також має набір неосновних зразків, які є зразками, які є сусідами основного зразка в кластері, але самі не є основними зразками. Інтуїтивно зрозуміло, що ці зразки знаходяться на периферії кластера.

Будь-який базовий зразок за визначенням є частиною кластера. Алгоритм вважає будь-який зразок, який не є основним зразком і знаходиться на відстані принаймні eps від будь-якого основного зразка.

У той час як параметр min_samples головним чином контролює, наскільки алгоритм толерантний до шуму (на галасливих і великих наборах даних може

бути бажаним збільшити цей параметр), параметр eps має вирішальне значення для правильного вибору для набору даних і функції відстані, і зазвичай його не можна залишати. за значенням за замовчуванням. Він контролює локальне оточення точок. Якщо вибрати занадто малий розмір, більшість даних взагалі не буде кластеризовано (і позначено як -1 для «шуму»). Якщо вибрано надто великий, це призводить до об'єднання близьких кластерів в один кластер і, зрештою, весь набір даних повертається як один кластер. Деякі евристики для вибору цього параметра обговорювалися в літературі, наприклад, на основі коліна на графіку відстаней найближчого [65].

На зображенні (рис. 3.9) кольором позначено належність об'єктів до певного кластера: великі кола відповідають основним зразкам, визначеним алгоритмом, а менші – позначають неосновні зразки, які також належать до кластерів. Крім того, викиди представлені чорними точками в нижній частині рисунка.

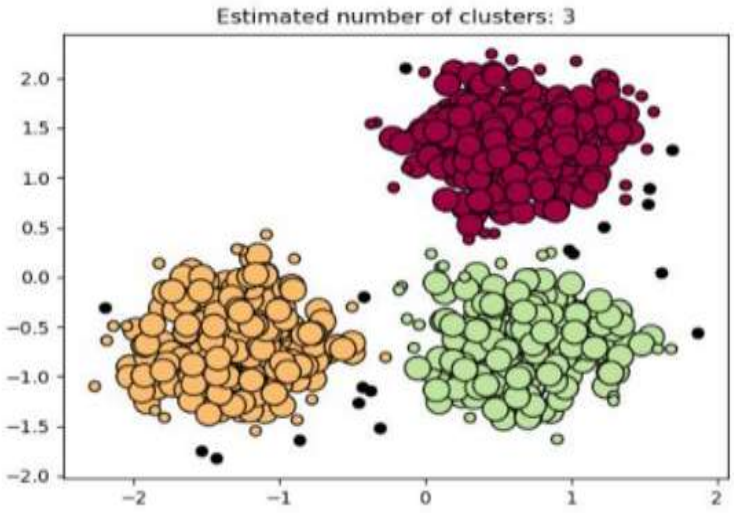


Рисунок 3.9 – Розподіл кластерів [65]

Переваги методу DBSCAN:

– не потребує вказувати кількість кластерів;

– добре працює для кластерів довільної форми;

– автоматично видаляє викиди або шумові (аномальні) точки та ігнорує їх при формуванні кластерів.

– його ефективність дозволяє працювати з більшими обсягами даних.

Недоліки методу DBSCAN полягають у складності підібрати оптимальні параметри ε (радіус сусідства) та MinPts (мінімальна кількість точок у кластері).

Ієрархічна кластеризація. Методи кластерного аналізу можуть бути ієрархічними і неієрархічними. Ієрархічна кластеризація (Hierarchical clustering) починається з трактування кожного спостереження як окремого кластеру. Потім він неодноразово виконує наступні два кроки:

- 1 – ідентифікує два кластери, які є найближчими один до одного;
- 2 – об'єднає два найбільш схожі кластери. Це триває поки всі кластери не об'єднаються.

Етапи проведення кластерного аналізу:

– Підготовка даних до кластеризації. Виділення даних для аналізу:

```
data_for_clust=data.drop(data.columns[0], axis=1).values
data_for_clust[0].
```

– Виконуємо препроцесинг за допомогою бібліотеки sklearn:

```
from sklearn import preprocessing
dataNorm = preprocessing.scale(data_for_clust).
```

– Вираховуємо відстань між кожним набором даних, вираховуємо евклідову відстань (за замовчуванням):

```
data_dist = pdist(dataNorm, 'euclidean').
```

– Головна функція ієрархічної кластеризації проводить об’єднання елементів в кластери і збереження в спеціальній змінній (використовується далі для візуалізації і виділення кількості кластерів):

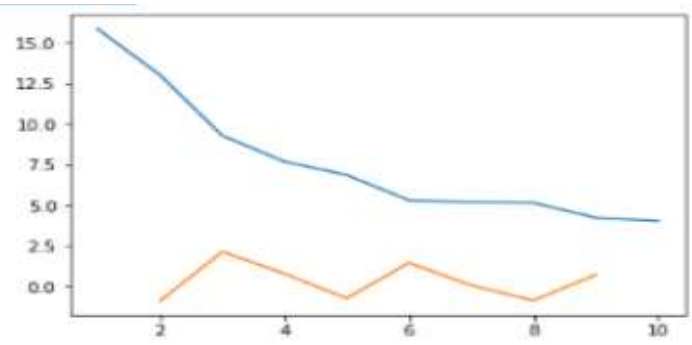
```
data_linkage = linkage(data_dist, method='average').
```

– Використаємо метод Ліктя, він дозволяє оцінити оптимальну кількість сегментів. Метод Ліктя – це графічне відображення, рекомендація по кількості кластерів. Коли верхні і нижні лінії сходяться максимально один до одного – саме таку кількість кластерів і рекомендується розглядати. Як можна побачити за результатами виконання дій – система рекомендує 3 кластери (рис. 3.10).

– Виконуємо побудову дендрограми для наочності результатів кластеризації:

```
nCluster=6
fancy_dendrogram(data_linkage,truncate_mode='lastp',
        p=nCluster,leaf_rotation=90.,leaf_font_size=12.,
show_contracted=True, annotate_above=10, )
```

```
plt.show()
```




```
clusters: 3
```

Рисунок 3.10 – Рекомендована кількість кластерів для розгляду [66]

Основним результатом ієрархічної кластеризації є дендрограма (рис.3.10), яка показує ієрархічну залежність між кластерами. Виконавши побудову можна зробити висновок про відстань між кластерами, чим вище стовпець тим більше відстань між кластерами, кластеризація виконана у вигляді вкладених груп. В результаті кластеризації в кожний кластер визначена певна група даних, наприклад група з 699 клієнтів, яка є не вкладеною і відрізняється від інших (рис. 3.11).

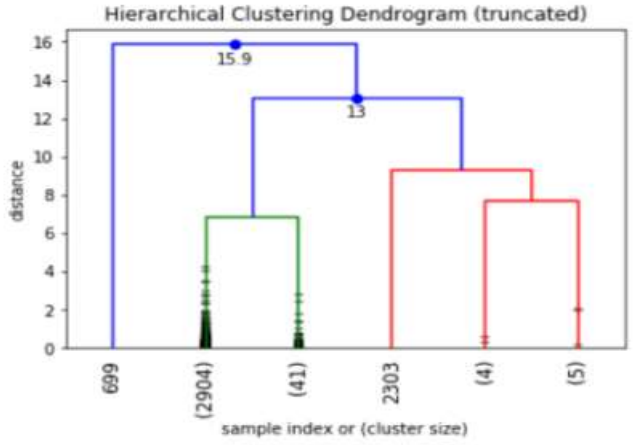


Рисунок 3.11 – Ієрархічна кластеризація [66]

Ієрархічна кластеризація зазвичай працює шляхом послідовного об'єднання подібних кластерів, як показано вище. Це відоме як агломераційна ієрархічна кластеризація. Теоретично це також можна зробити, спочатку групуючи всі спостереження в один кластер, а потім послідовно розбиваючи ці кластери. Це відоме як розділення ієрархічної кластеризації. Особливість ієрархічної кластеризації, що всі кластери вкладені, тобто слідують один за одним.

На основі результатів кластеризації здійснюється **фільтрація трафіку**. Нормальні дані не підлягають подальшому аналізу, тоді як аномальні передаються до класифікаційного модуля.

Кластерний аналіз зазвичай поєднують з іншими підходами:

– кластеризація + машинне навчання (ML);

– кластеризація + статистичні методи;

– кластеризація + сигнатурний аналіз.

На **третьому етапі** відбувається ідентифікація (класифікація) атак, тобто аномальні дані подаються до класифікатора (наприклад, Random Forest), який визначає тип атаки, зокрема: DoS / DDoS, Probe, R2L, U2R.

Функція класифікації має вигляд:

$$f: X \to Y, \tag{3.3}$$

де Y – множина класів атак.

Результатом роботи класифікатора є визначення типу атаки або підтвердження відсутності загрози.

Четвертий етап – адаптивне оновлення моделі (адаптивне навчання). Адаптивність є однією з ключових характеристик сучасних систем виявлення вторгнень, оскільки кіберзагрози постійно еволюціонують, змінюючи свої ознаки та механізми реалізації. Традиційні підходи, що базуються лише на фіксованих правилах або сигнатурах, не здатні ефективно протидіяти новим і невідомим атакам, що обумовлює необхідність впровадження адаптивних механізмів. Система:

– виконує адаптацію на основі нових даних шляхом оновлення параметрів моделі, що дозволяє підвищити точність виявлення кіберзагроз та враховувати зміни в поведінці мережевого трафіку. Це досягається завдяки використанню методів машинного навчання, які здатні автоматично аналізувати нові зразки даних і коригувати внутрішні моделі без необхідності повного перепроєктування системи;

– передбачає динамічне коригування параметрів системи виявлення вторгнень на основі нових вхідних даних, що дозволяє системі навчатися в процесі експлуатації та ефективно реагувати на появу нових типів кіберзагроз.

Адаптивне оновлення моделі реалізується через механізми онлайн-навчання (online learning), інкрементального навчання (incremental learning) та періодичного перенавчання (retraining). Онлайн-навчання дозволяє системі обробляти дані в реальному часі, одразу враховуючи нову інформацію, тоді як інкрементальне навчання забезпечує поступове накопичення знань без втрати раніше отриманого досвіду. Крім того, адаптивні системи часто використовують гібридні підходи, зокрема поєднання кластерного аналізу та методів класифікації. Кластеризація дозволяє виявляти нові шаблони поведінки без попередньої розмітки даних, а класифікаційні алгоритми уточнюють результати, відносячи події до конкретних типів атак [67].

Застосування адаптивних механізмів дозволяє значно зменшити кількість хибних спрацювань (false positives), підвищити швидкість реагування на інциденти та забезпечити ефективне виявлення як відомих, так і нових кіберзагроз. Таким чином, адаптивність є необхідною умовою побудови сучасних інтелектуальних систем кіберзахисту.

3.2. Алгоритм функціонування розробленої адаптивної гібридної системи виявлення вторгнень

Розроблена адаптивна гібридна система виявлення вторгнень (IDS) призначена для аналізу мережевого трафіку в реальному часі та виявлення як відомих, так і нових (невідомих) типів атак. Основною особливістю системи є поєднання методів кластеризації та машинного навчання з механізмом адаптивного оновлення моделі, що дозволяє враховувати зміни у поведінці мережевого середовища.

Алгоритм функціонування розробленої адаптивної гібридної системи виявлення вторгнень полягає у постійному аналізі мережевого трафіку з використанням комбінації кластеризації та класифікації з подальшим автоматичним оновленням моделі при зміні характеристик даних.

Функціонування розробленої адаптивної гібридної системи виявлення вторгнень базується на послідовності взаємопов’язаних етапів обробки даних, що забезпечують як виявлення відомих атак, так і ідентифікацію нових загроз (рис. 3.12).



Рисунок 3.12 – Модель адаптивної гібридної системи IDS: поєднання сигнатурного та аномального підходів

Джерело: Розроблено автором на основі [68-69] за допомогою https://notebooklm.google.com

1. Збір даних (Data Acquisition). На першому етапі здійснюється безперервний моніторинг мережевого середовища, системних журналів (logs) та системних викликів. Система здійснює захоплення мережевих пакетів у режимі реального часу, формуючи потік даних для подальшого аналізу.

2. Попередня обробка та виділення ознак (Preprocessing & Feature Extraction). Отримані дані проходять етап попередньої обробки, який включає:

– очищення від шумів і некоректних записів;

– нормалізацію числових значень;

– трансформацію неструктурованих даних у формалізований вигляд;

– виділення інформативних ознак, що характеризують поведінку користувачів та мережевих процесів.

Метою цього етапу є формування якісного простору ознак для подальшого машинного аналізу.

3. Гібридний механізм виявлення (Hybrid Detection Mechanism). На цьому етапі застосовується комбінований підхід, який включає два взаємодоповнюючі методи:

3.1. Сигнатурний аналіз (Signature-based detection) [68].

Здійснюється порівняння вхідних даних із базою відомих сигнатур атак.

Даний підхід забезпечує високу швидкість і точність виявлення вже відомих загроз.

3.2. Аномальний аналіз (Anomaly-based detection) [69].

Використовуються методи машинного навчання (наприклад, нейронні мережі або інші моделі), які формують модель «нормальної» поведінки системи.

Відхилення від цієї моделі розглядаються як потенційні аномалії, що дозволяє виявляти раніше невідомі (zero-day) атаки.

4. Прийняття рішень та кореляція подій (Decision Making & Correlation). Результати сигнатурного та аномального аналізу інтегруються для підвищення точності прийняття рішень. На цьому етапі здійснюється:

– зменшення кількості хибнопозитивних спрацьовувань (false positives);

– класифікація подій;

– визначення рівня загрози.

У результаті система формує остаточне рішення щодо наявності або відсутності атаки.

5. Реагування (Alerting & Response) [68]. Залежно від політики безпеки система може працювати у двох режимах:

– активний режим (IPS) – автоматичне блокування підозрілого трафіку, розрив з’єднань, оновлення правил міжмережевого екрану.

– пасивний режим (IDS) – фіксація інциденту та надсилання повідомлень адміністратору безпеки.

6. Адаптація та навчання (Adaptation&Learning). Ключовою особливістю системи є механізм адаптивного навчання. У разі виявлення змін у характері вхідних даних (concept drift) система здійснює автоматичне оновлення:

– перенавчання або донавчання моделі;

– корекцію кластерів;

– оновлення параметрів класифікатора.

Це забезпечує здатність системи адаптуватися до нових типів атак і змін у мережевому середовищі без повного переналаштування.

Таким чином, гібридний підхід забезпечує поєднання двох ключових переваг: високої швидкості виявлення відомих атак за рахунок сигнатурного аналізу та високої гнучкості і здатності виявляти нові загрози завдяки методам аномального аналізу та машинного навчання.

3.3. Реалізація та налаштування гібридної моделі IDS

Реалізація та налаштування гібридної моделі IDS включає побудову архітектури системи, вибір алгоритмічних компонентів, формування математичної моделі, параметризацію моделей та організацію процедури навчання. Математична модель IDS описує процес перетворення вхідного набору мережевих характеристик у результат класифікації, що визначає належність мережевого трафіку до нормального або аномального класу. У межах гібридного підходу модель може включати функції кластеризації для виділення аномальних груп даних та класифікаційні функції для прийняття остаточного рішення щодо типу активності.

На рис. 3.13 представлено архітектуру гібридної системи виявлення вторгнень (IDS), яка поєднує сигнатурний та аномальний підходи до аналізу мережевого трафіку. Робота системи починається зі збору даних із різних джерел, зокрема мережевого трафіку, системних журналів, NetFlow/sFlow та даних хостів. Отримані дані передаються до модуля попередньої обробки, де виконується очищення, нормалізація, кодування категоріальних ознак та формування набору характеристик для подальшого аналізу.

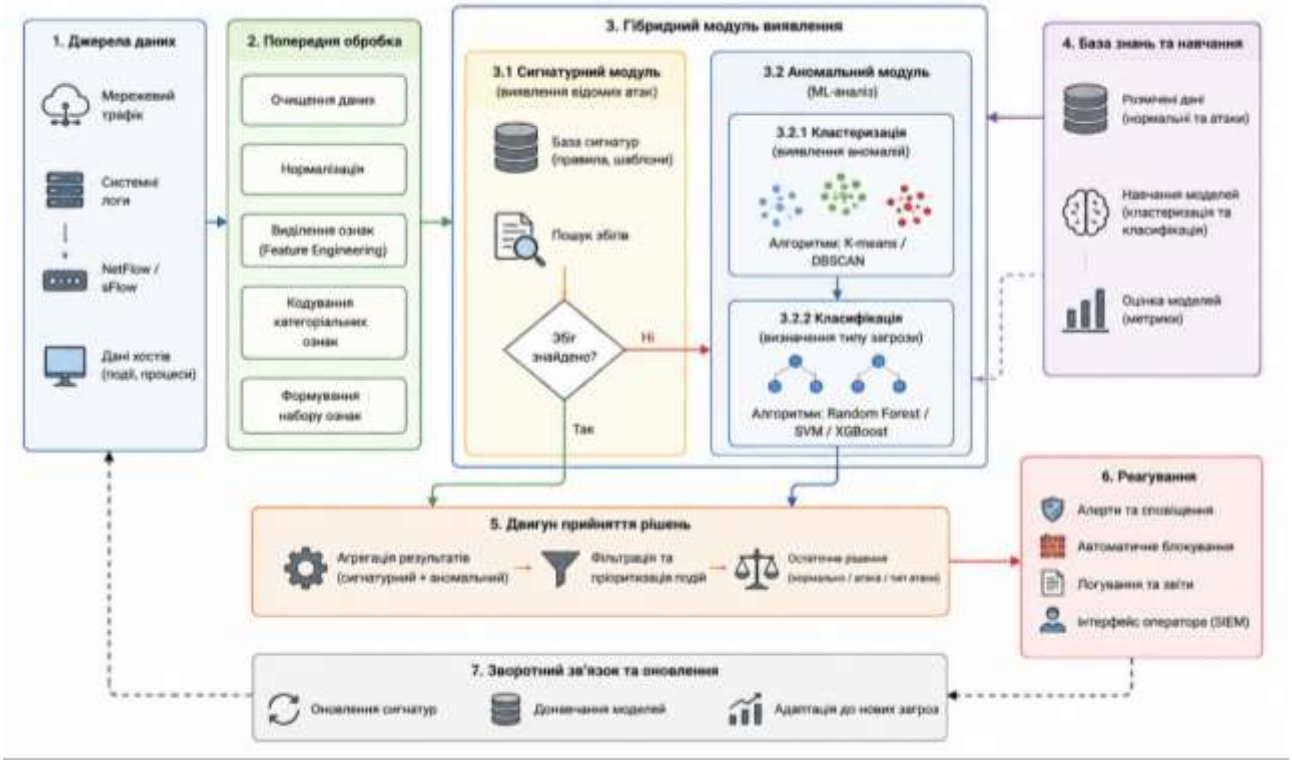


Рисунок 3.13 – Архітектура гібридної IDS

Джерело: Розроблено автором на основі [32, 71-72] за допомогою https://notebooklm.google.com

Архітектура гібридної системи виявлення вторгнень (IDS) складається з декількох взаємопов'язаних модулів, кожен з яких виконує окрему функцію в процесі моніторингу, аналізу та виявлення кіберзагроз. Для реалізації кожного етапу гібридної IDS використовуються різні програмні інструменти, платформи та бібліотеки.

На етапі збору мережевого трафіку та системних подій використовуються інструменти:

– Wireshark аналіз мережевих пакетів;
– Tcpdump – захоплення мережевого трафіку;
– Zeek – моніторинг мережевої активності;
– Snort – сигнатурна IDS;
– Suricata – IDS/IPS для аналізу трафіку;
– NetFlow/sFlow collectors – збір статистики мережевого трафіку.

Дані можуть надходити у вигляді мережевих пакетів, NetFlow/sFlow статистики, системних журналів або подій хостів.

Після збору інформації виконується попередня обробка даних. На цьому етапі проводиться очищення даних, нормалізація, кодування категоріальних

ознак та формування набору характеристик (feature engineering). Для реалізації preprocessing та аналізу даних використовуються інструменти Python, Pandas, NumPy та Scikit-learn. У випадку роботи з великими обсягами даних може застосовуватися платформа Apache Spark.

Ключовим елементом архітектури є гібридний модуль виявлення, який поєднує сигнатурний та аномальний аналіз. Сигнатурний модуль використовує базу правил і шаблонів атак для пошуку збігів із відомими загрозами. Реалізація цього підходу зазвичай базується на системах Snort, Suricata або YARA. Перевагою сигнатурного підходу є висока точність при виявленні відомих атак та низький рівень хибних спрацювань.

Якщо сигнатурний модуль не знаходить відповідності, дані передаються до аномального модуля, який використовує алгоритми машинного навчання. На першому етапі виконується кластеризація мережевого трафіку за допомогою алгоритмів K-means або DBSCAN, що дозволяє виявляти аномальні групи даних. Для реалізації кластеризації та класифікації використовуються бібліотеки Scikit-learn, TensorFlow та PyTorch. Після кластеризації результати передаються до класифікаційного модуля, де застосовуються алгоритми Random Forest, SVM або XGBoost для визначення типу загрози та прийняття остаточного рішення щодо належності трафіку до нормального або шкідливого класу.

Результати роботи сигнатурного та аномального модулів об’єднуються у двигуні прийняття рішень. На цьому етапі здійснюється агрегація подій, фільтрація помилкових спрацювань та визначення пріоритетності загроз. Для централізованого аналізу та кореляції подій використовуються SIEM-платформи, зокрема Elastic Stack (ELK), Wazuh, Splunk та Graylog.

У разі виявлення атаки система реагування виконує автоматичне блокування підозрілої активності, генерацію сповіщень, логування подій та передачу інформації оператору або SIEM-системі. Для цього можуть використовуватися рішення IBM QRadar, Microsoft Sentinel або Splunk Enterprise Security.

Важливою складовою гібридної IDS є механізм зворотного зв’язку та оновлення моделей. Він забезпечує адаптацію системи до нових типів атак шляхом оновлення сигнатур та повторного навчання моделей машинного

навчання. Для автоматизації цього процесу можуть застосовуватися MLOps-платформи MLflow [70] та Kubeflow [71].

Застосування математичних методів та алгоритмів машинного навчання дозволяє підвищити точність виявлення вторгнень, зменшити кількість помилкових спрацювань і забезпечити ефективне функціонування IDS в умовах постійного зростання кількості та складності кіберзагроз. Математична модель адаптивної гібридної системи виявлення вторгнень описує процес аналізу мережевих подій як поєднання сигнатурного та аномального підходів із подальшим адаптивним оновленням параметрів моделі у динамічному середовищі. Розглянемо її більш детальніше.

1. Модель вхідних даних. Потік мережевих подій (з'єднань) представимо у вигляді множини:

$$X = \{x_1, x_2, \dots, x_t, \dots, x_n\}, \tag{3.4}$$

де $x_t \in \mathbb{R}^d$ *– вектор ознак мережевої події у момент часу* t*,* d *– кількість ознак.*

Формула описує вхідні дані системи як часову послідовність об'єктів (мережевих подій), що надходять у режимі реального часу.

Кожна подія представлена у вигляді вектора ознак, що характеризують її поведінкові або мережеві параметри:

$$x_t = (x_{t,1}, x_{t,2}, \dots, x_{t,d}). \tag{3.5}$$

2. Попередня обробка даних. Для усунення впливу масштабів ознак використовується нормалізація, яка забезпечує приведення всіх ознак до однакового масштабу, що підвищує ефективність алгоритмів машинного навчання:

$$\tilde{x}_{t,j} = \frac{x_{t,j} - \mu_j}{\sigma_j}, j = 1, \dots, d, \tag{3.6}$$

де μ_j *– середнє значення,* σ_j *– стандартне відхилення ознаки* j*.*

3. Сигнатурний аналіз. Нехай задано множину сигнатур відомих атак:

$$S = \{s_1, s_2, \dots, s_m\}. \tag{3.7}$$

Множина S містить еталонні шаблони (сигнатури) відомих атак, з якими порівнюються нові дані.

Відстань між вектором події та сигнатурою визначається як:

$$d_s(x_t, s_i) = \sqrt{\sum_{j=1}^{d} (x_{t,j} - s_{i,j})^2}. \quad (3.8)$$

Використовується евклідова відстань для оцінки схожості між поточною подією та сигнатурою.

Результат сигнатурного аналізу:

$$R_s(t) = \begin{cases} 1, & \min_i d_s(x_t, s_i) \le \tau_s, \\ 0, & \text{інакше}, \end{cases} \quad (3.9)$$

де τ_s – поріг спрацювання сигнатурного детектора.

Якщо хоча б одна сигнатура достатньо близька до події (менше порогу), вона вважається атакою.

4. Аномальний аналіз. Нехай модель машинного навчання задається функцією:

$$f_\theta(x_t) = a_t, a_t \in [0,1], \quad (3.10)$$

де a_t – оцінка аномальності.

Модель оцінює ступінь аномальності події, де значення ближче до 1 означає більшу ймовірність атаки.

Рішення аномального детектора:

$$R_a(t) = \begin{cases} 1, & a_t \ge \tau_a, \\ 0, & \text{інакше.} \end{cases} \quad (3.11)$$

Якщо рівень аномальності перевищує заданий поріг, подія вважається підозрілою.

5. Гібридне прийняття рішення. Комбінований показник визначається як:

$$S_t = w_s R_s(t) + w_a a_t, \quad (3.12)$$

де w_s, w_a – вагові коефіцієнти, $w_s + w_a = 1$.

Результати сигнатурного та аномального аналізу об'єднуються з урахуванням вагових коефіцієнтів.

Остаточне рішення системи:

$$D_t = \begin{cases} 1, & S_t \ge \tau_d, \\ 0, & \text{інакше}, \end{cases} \quad (3.13)$$

де $D_t = 1$ відповідає наявності атаки.

Якщо комбінований показник перевищує поріг, система фіксує атаку.

6. Виявлення зміни розподілу даних. Для виявлення змін у потоці даних використовується критерій:

$$D(P_t(X), P_{t-1}(X)) > \delta, \tag{3.14}$$

де $D(\cdot)$ – міра відстані між розподілами, δ – поріг чутливості.

Перевіряється, чи змінився статистичний розподіл даних; у разі перевищення порогу запускається адаптація [72].

7. Адаптивне оновлення моделі. Оновлення параметрів моделі виконується за правилом:

$$\theta_{t+1} = \theta_t - \eta \nabla L(\theta_t, B_t), \tag{3.15}$$

де: L – функція втрат, B_t – нові дані (батч), η – швидкість навчання.

Параметри моделі коригуються методом градієнтного спуску на основі нових даних, що забезпечує адаптацію до змін у середовищі [32].

Запропонована математична модель дозволяє формалізувати процес функціонування адаптивної гібридної системи виявлення вторгнень, поєднуючи сигнатурний та аномальний підходи з механізмом адаптації до змін у мережевому середовищі. Програмний код адаптивної гібридної IDS та блок-схема алгоритму наведено у вигляді послідовності кроків, що відповідають математичній моделі (3.4–3.15) (рис. 3.14, 3.15).

```
Algorithm AdaptiveHybridIDS

Input: потік даних X = (x₁, x₂, ..., xₜ)  // (3.4)
Output: рішення D_t ∈ {0,1}                // (3.13)

1: // ІНІЦІАЛІЗАЦІЯ
2: Завантажити множину сигнатур S          // (3.7)
3: Ініціалізувати модель f_θ               // (3.10)
4: Обчислити μ_j, σ_j для нормалізації     // (3.6)
5: Встановити пороги τ_s, τ_a, τ_d         // (3.9), (3.11), (3.13)
6: Встановити ваги w_s, w_a (w_s + w_a = 1) // (3.12)
7: Встановити швидкість навчання η         // (3.15)

8: // ОСНОВНИЙ ЦИКЛ
9: для кожного x_t ∈ X виконувати

10:    // 1. НОРМАЛІЗАЦІЯ (3.6)
11:    для j = 1 до d:
12:        x̃_t,j ← (x_t,j − μ_j) / σ_j
13:    кінець для

14:    // 2. СИГНАТУРНИЙ АНАЛІЗ (3.8-3.9)
15:    d_min ← +∞
16:    для кожної сигнатури s_i ∈ S:
17:        d ← sqrt(Σ_{j=1}^{d} (x̃_t,j − s_i,j)²)
18:        якщо d < d_min:
19:            d_min ← d
20:    кінець для

21:    якщо d_min ≤ τ_s:
22:        R_s(t) ← 1
23:    інакше:
24:        R_s(t) ← 0

25:    // 3. АНОМАЛЬНИЙ АНАЛІЗ (3.10-3.11)
26:    a_t ← f_θ(x̃_t)
27:    якщо a_t ≥ τ_a:
28:        R_a(t) ← 1
29:    інакше:
30:        R_a(t) ← 0

31:    // 4. ГІБРИДНЕ РІШЕННЯ (3.12-3.13)
32:    S_t ← w_s * R_s(t) + w_a * a_t
33:    якщо S_t ≥ τ_d:
34:        D_t ← 1
35:    інакше:
36:        D_t ← 0

37:    // 5. РЕАГУВАННЯ
38:    якщо D_t = 1:
39:        виконати блокування / alert
40:    інакше:
41:        зберегти як нормальну подію

42:    // 6. ВИЯВЛЕННЯ DRIFT (3.14)
43:    якщо D(P_t(X), P_{t-1}(X)) > δ:

44:        // 7. АДАПТАЦІЯ (3.15)
45:        сформувати батч B_t
46:        θ ← θ − η * ∇L(θ, B_t)
47:        оновити модель f_θ

48: кінець для

49: Кінець алгоритму
```

Рисунок 3.14 – Програмний код адаптивної гібридної IDS

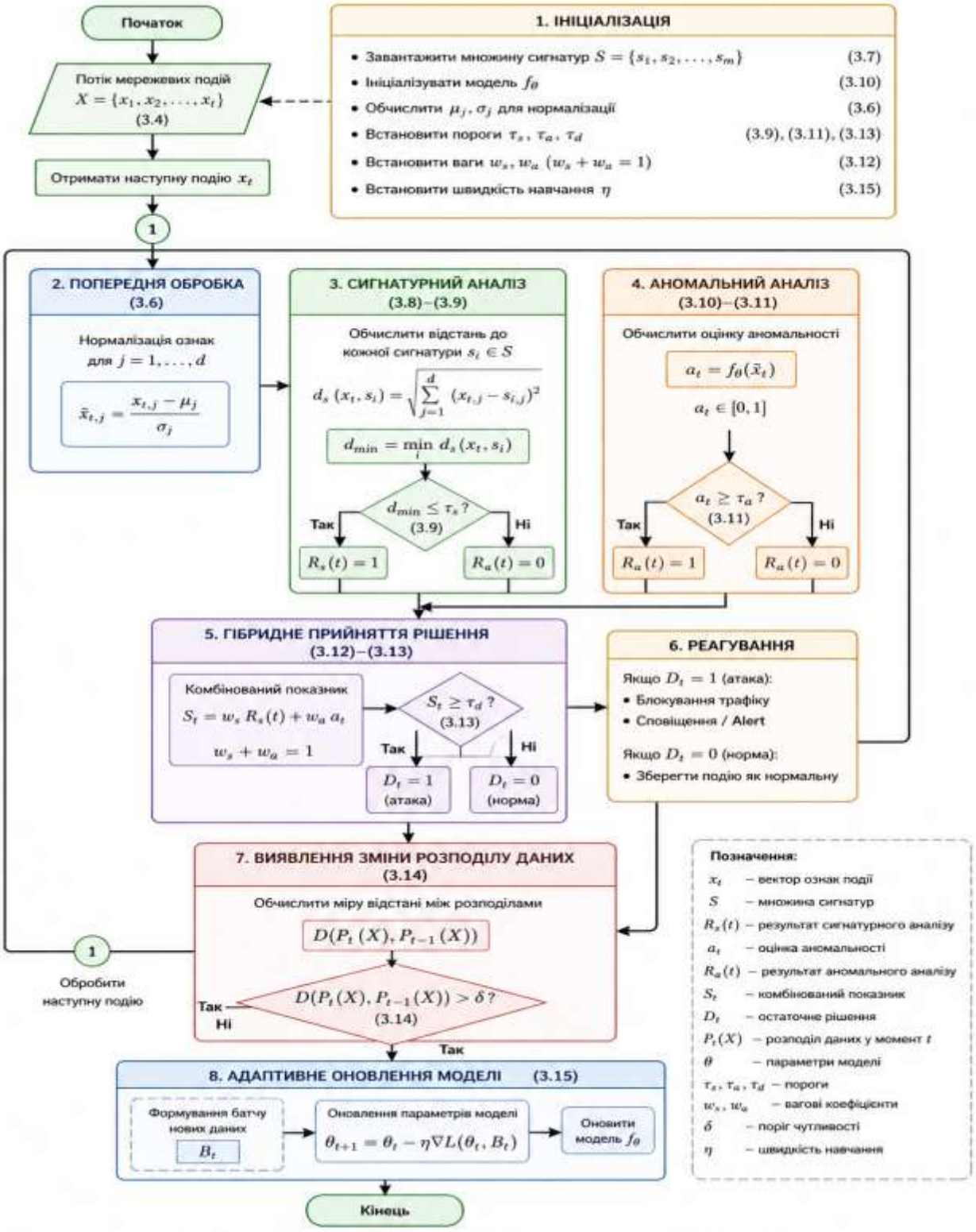


Рисунок 3.15 – Блок-схема алгоритму функціонування адаптивної гібридної системи виявлення вторгнень (IDS)

Джерело: Розроблено автором за допомогою https://notebooklm.google.com

Запропонований алгоритм забезпечує:

- виявлення як відомих, так і нових атак
- зменшення кількості хибних спрацьовувань
- адаптацію до змін у мережевому середовищі

Далі розглянемо гібридну IDS, що базується на **комбінації кластерного методу k-means та сигнатурного аналізу** [73] (рис. 3.16).

Запропонована система дозволяє одночасно:

– виявляти відомі атаки (сигнатурний підхід);

– ідентифікувати нові, раніше невідомі аномалії (поведінковий підхід k-means).

Архітектура системи включає такі основні модулі: 1) Модуль збору та попередньої обробки даних; 2) Модуль кластеризації (k-means); 3) Сигнатурний модуль; 4) Модуль прийняття рішень; 5) Модуль адаптації (реакції).

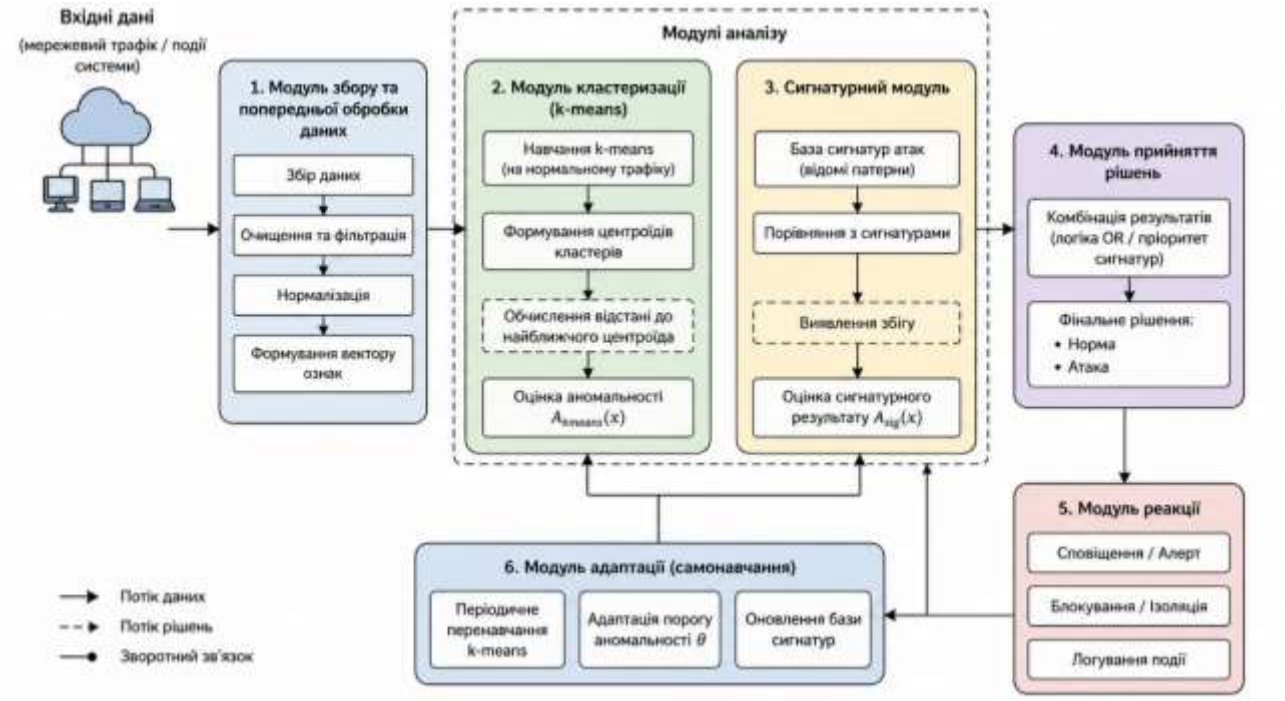


Рисунок 3.16 – Структурна схема гібридної IDS: комбінація кластерного методу k-means та сигнатурного аналізу

Джерело: Розроблено автором на основі [73] за допомогою https://notebooklm.google.com

Спочатку розглянемо **математичну модель кластеризаційної частини**.

Нехай множина вхідних даних має вигляд:

$$X = \{x_1, x_2, \ldots, x_n\}, x_i \in \mathbb{R}^m$$

де x_i – вектор ознак мережевого трафіку або системної події.

Метод k-means розбиває дані на k-кластерів, мінімізуючи функцію внутрішньокластерної дисперсії:

$$J = \sum_{j=1}^{k} \sum_{x_i \in C_j} \| x_i - \mu_j \|^2 \qquad (3.16)$$

де:

C_j – множина об'єктів j-го кластера,

μ_j – центроїд кластера,

$\|\cdot\|$ – евклідова норма.

Центроїд обчислюється як:

$$\mu_j = \frac{1}{|C_j|}\sum_{x_i \in C_j} x_i \tag{3.17}$$

Оцінюємо аномальності. Для кожного нового спостереження xвизначається його відхилення від нормальної поведінки:

$$A_{kmeans}(x) = \min_j \| x - \mu_j \| \tag{3.18}$$

Якщо виконується умова:

$$A_{kmeans}(x) > \theta$$

де θ – порогове значення, то об'єкт вважається аномальним.

Наступний крок – математична модель сигнатурного аналізу

Нехай задано множину сигнатур відомих атак:

$$S = \{s_1, s_2, \ldots, s_p\}$$

Тоді функція сигнатурного виявлення визначається як:

$$A_{sig}(x) = \begin{cases} 1, & x \in S \\ 0, & x \notin S \end{cases} \tag{3.19}$$

Гібридна модель прийняття рішень.

У системі використовується комбіноване правило прийняття рішення. Найпростішим варіантом є логіка **OR**, яка визначає подію як атаку, якщо хоча б один модуль спрацював:

$$A(x) = A_{sig}(x) \vee (A_{kmeans}(x) > \theta) \tag{3.20}$$

Альтернативно може застосовуватись пріоритет сигнатурного аналізу, коли перевірка k-means виконується лише у разі відсутності збігу із сигнатурою.

Алгоритм роботи вищезазначеної гібридної IDS складається з двох основних фаз: навчання та детекції.

Фаза 1. Навчання

– збір нормального трафіку;

– формування ознак;

– виконання кластеризації k-means;

– обчислення центроїдів μ_j.

Фаза 2. Детекція

– отримання нового вхідного об’єктах;

– перевірка сигнатурного модуля;

– обчислення відстані до центроїдів;

– прийняття рішення про тип події;

– реакція системи (блокування / сповіщення / логування).

Програмний код гібридної IDS, що базується на комбінації кластерного методу k-means та сигнатурного аналізу, наведено на рис. 3.17.

```
Вхід: X – потік даних, k – кількість кластерів, θ – поріг, S – сигнатури

// НАВЧАННЯ
1. Ініціалізувати μ1...μk
2. Повторювати до збіжності:
      для кожного x ∈ X:
            призначити x до найближчого кластера
      оновити μj як середнє значення кластера

// ДЕТЕКЦІЯ
3. Для кожного нового x:

      // сигнатурна перевірка
      якщо x ∈ S:
            позначити як ATTACK
      інакше:
            A = min ||x - μj||
            якщо A > θ:
                  позначити як ATTACK
            інакше:
                  позначити як NORMAL

// АДАПТАЦІЯ
4. Періодично:
      оновити μj
      оновити θ
      оновити сигнатурну базу
```

Рисунок 3.17 – Програмний код гібридної IDS: комбінація кластерного методу k-means та сигнатурного аналізу

Важливою особливістю запропонованої IDS є її здатність до адаптації. Вона реалізується за рахунок:

– періодичного перенавчання моделі k-means;

– корекції порогового значення θ;

– оновлення сигнатурної бази на основі нових загроз.

Це дозволяє системі зберігати актуальність у змінному мережевому середовищі та зменшувати кількість хибних спрацювань. Отже, запропонована система є ефективним рішенням для побудови сучасних IDS з підвищеним рівнем виявлення загроз та стійкістю до змін характеру атак.

3.4. Формування експериментального середовища та підготовка даних мережевого трафіку для задачі виявлення вторгнень

Формування експериментального середовища є одним із ключових етапів розробки та оцінювання систем виявлення вторгнень (Intrusion Detection Systems, IDS). Якість побудованого середовища безпосередньо впливає на достовірність результатів дослідження, точність моделей машинного навчання та можливість відтворення експериментів. Для задач аналізу мережевого трафіку особливого значення набуває процес підготовки даних, який включає збір, очищення, нормалізацію, а також формування ознак для подальшого навчання моделей. Складові формування експериментального середовища та підготовка даних мережевого трафіку для задачі виявлення вторгнень представлено на рис. 3.18.

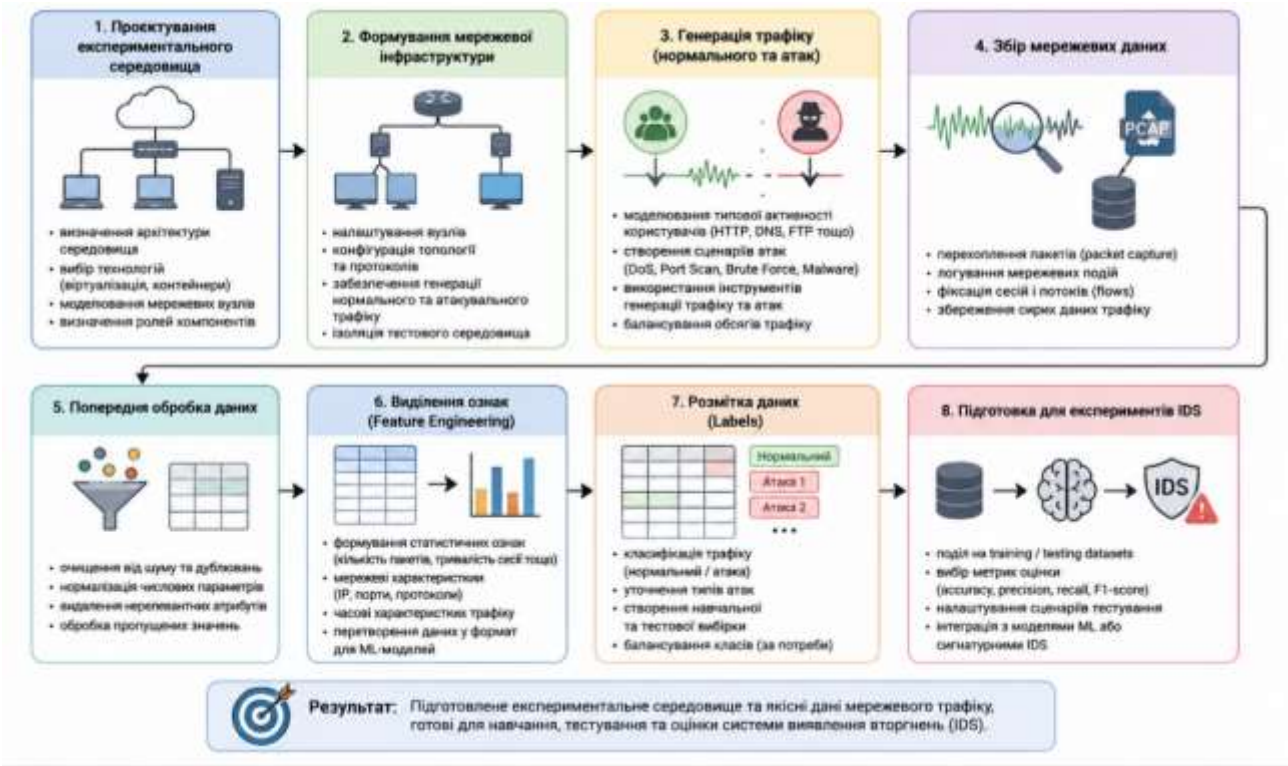


Рисунок 3.18 – Складові формування експериментального середовища та підготовка даних мережевого трафіку для задачі виявлення вторгнень

Джерело: розроблено автором за допомогою ChatGPT

У сучасних умовах зростання кількості кіберзагроз та ускладнення мережевих атак виникає необхідність використання автоматизованих підходів до виявлення аномалій і вторгнень. Одним із найбільш ефективних підходів є застосування методів машинного навчання та глибокого навчання, що потребує

наявності якісного набору даних і контрольованого експериментального середовища.

Метою формування експериментального середовища та підготовки даних мережевого трафіку для задачі виявлення вторгнень є створення умов для моделювання реальних або наближених до реальних мережевих атак і нормальної активності, щоб можна було ефективно розробляти, навчати та оцінювати системи виявлення вторгнень (IDS).

1. Проєктування експериментального середовища є одним із ключових етапів дослідження систем виявлення вторгнень (IDS), оскільки саме від правильності побудови інфраструктури залежить достовірність отриманих результатів [74]. Вибір архітектури визначається метою експерименту, вимогами до масштабованості та доступними обчислювальними ресурсами. Основною метою даного етапу є створення контрольованого середовища, у якому можливо моделювати реальні мережеві процеси та генерувати різні типи трафіку і починається він з вибору його архітектури, яка визначає спосіб організації обчислювальних ресурсів та мережевих взаємодій (рис. 3.19).

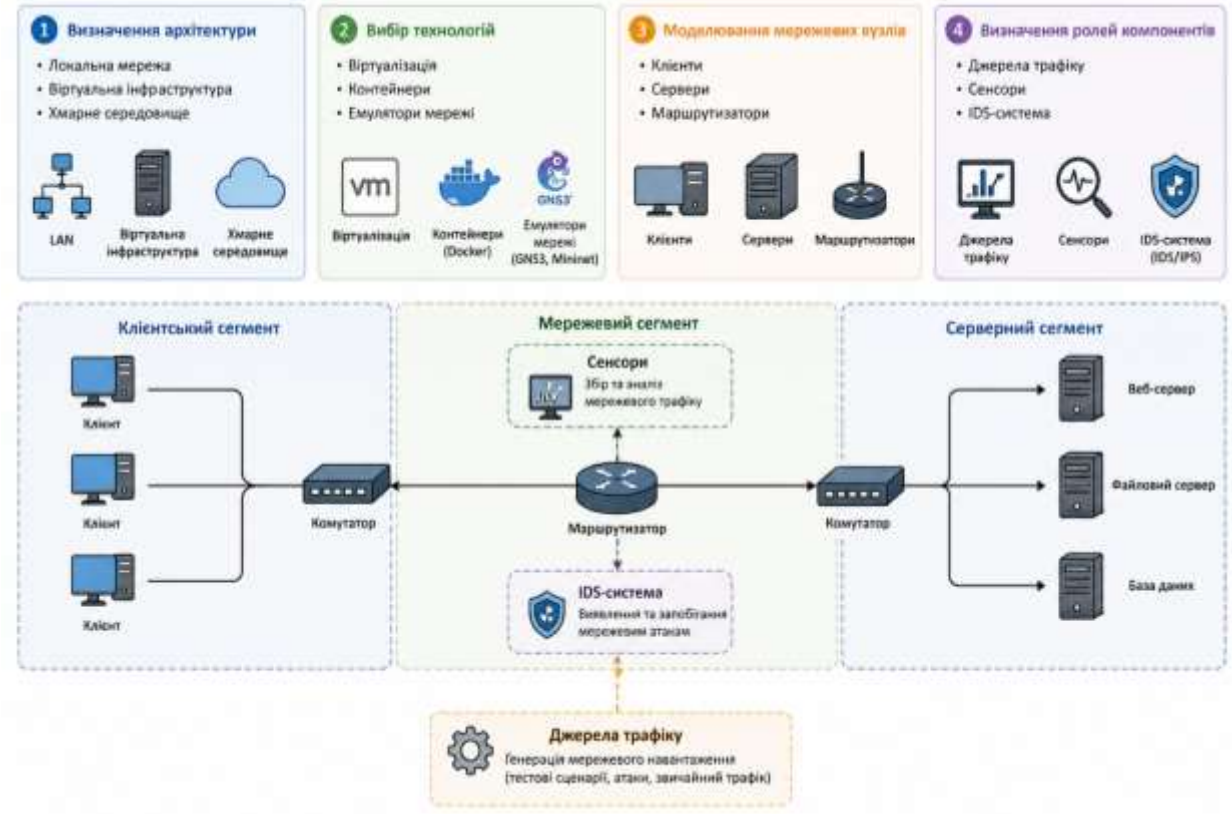


Рисунок 3.19 – Проєктування експериментального середовища

Джерело: розроблено автором на основі [74-76] за допомогою ChatGPT

У сучасних дослідженнях застосовуються три основні підходи:

Локальна мережа (LAN) – передбачає використання фізично розташованих вузлів у межах однієї лабораторії. Перевагами є висока керованість і точність вимірювань, однак масштабування такої архітектури є обмеженим.

Віртуальна інфраструктура – базується на використанні гіпервізорів (VMware, VirtualBox, KVM), що дозволяє створювати ізольовані віртуальні середовища з гнучким налаштуванням параметрів мережі.

Хмарне середовище – використовує сервіси провайдерів (AWS, Microsoft Azure, Google Cloud) для створення масштабованих і розподілених експериментальних платформ.

На першому етапі визначається архітектура експериментального середовища. Найчастіше використовуються віртуальні мережі або гібридні інфраструктури, оскільки вони забезпечують гнучкість та ізоляцію [75]. У роботі доцільно застосовувати віртуалізацію або контейнеризацію, а також мережеві емулятори:

– віртуалізація забезпечує можливість запуску кількох операційних систем на одному фізичному сервері, що дозволяє ефективно використовувати ресурси. Найчастіше застосовуються: VirtualBox (https://www.virtualbox.org/) та VMware Workstation (https://www.vmware.com/products/desktop-hypervisor/workstation-and-fusion) – цей підхід використовує віртуальні машини, де кожна віртуальна машина має власну гостьову операційну систему, що працює поверх гіпервізора;

– **контейнери (Docker, Podman, Kubernetes)** застосовуються для швидкого розгортання ізольованих сервісів та забезпечення масштабованості експериментів;

- Docker (https://www.docker.com/) – стандарт індустрії (станом на 2026 рік використовується ~87% компаній). Найкращий вибір для локальної розробки та швидкого створення ізольованих середовищ;
- Podman (https://podman.io/) – бездемонна (daemonless) альтернатива Docker, яка набуває популярності завдяки вищій безпеці (rootless) та сумісності;

- Kubernetes (https://kubernetes.io/) – де-факто стандарт для керування контейнерами в продуктивному середовищі та складних експериментах (використовують >80% організацій). Ідеальна для експериментів з високонавантаженими або розподіленими системами.

Вибір між віртуалізацією та контейнеризацією для експериментального середовища залежить від конкретних завдань, вимог до ізоляції та доступних ресурсів.

– емулятори мережі (GNS3, Mininet, Cisco Packet Tracer) дозволяють моделювати складні топології та мережеві протоколи без використання фізичного обладнання.

Застосування цих технологій забезпечує гнучкість, відтворюваність та масштабованість експериментів.

В експериментальному середовищі мережеві вузли використовуються для моделювання, тестування та аналізу роботи комп'ютерних мереж без ризику для реальної інфраструктури. Вузол – це будь-який пристрій або програмний елемент у мережі: комп'ютер, сервер, маршрутизатор, сенсор, віртуальна машина тощо. У межах експериментального середовища формуються такі **основні типи мережевих вузлів:**

- **клієнтські вузли** – генерують трафік та імітують поведінку кінцевих користувачів;
- **серверні вузли** – надають мережеві сервіси (веб-сервери, бази даних, файлові сервіси);
- **маршрутизатори та комутатори** – забезпечують передачу та маршрутизацію даних між сегментами мережі;
- **IDS-система та вузли генерації трафіку** – є ключовими компонентами експериментального середовища, оскільки саме вони забезпечують виявлення атак та формування набору даних для подальшого аналізу.

Розподіл ролей дозволяє створити реалістичну модель мережі, де IDS виконує моніторинг і аналіз трафіку. При моделюванні враховуються параметри продуктивності, затримки передачі даних та можливі відмови компонентів.

Взаємодія клієнтів, серверів та маршрутизаторів реалізується відповідно до архітектури комп'ютерних мереж [76].

Кожен компонент експериментального середовища виконує певну функціональну роль:

- **джерела трафіку** – створюють навантаження для аналізу продуктивності мережі;
- **сенсори** – здійснюють збір даних про мережеву активність, включаючи аналіз пакетів і виявлення аномалій;
- **IDS/IPS системи –** відповідають за виявлення та запобігання мережевим атакам.

Такий розподіл дозволяє створювати реалістичні сценарії кіберзагроз і оцінювати ефективність механізмів захисту інформації.

2. Формування мережевої інфраструктури є одним із ключових етапів створення тестового середовища для дослідження кіберзагроз, моделювання атак та аналізу мережевого трафіку. На цьому етапі здійснюється побудова структури мережі, налаштування її компонентів та забезпечення умов для безпечного проведення експериментів (рис. 3.20).

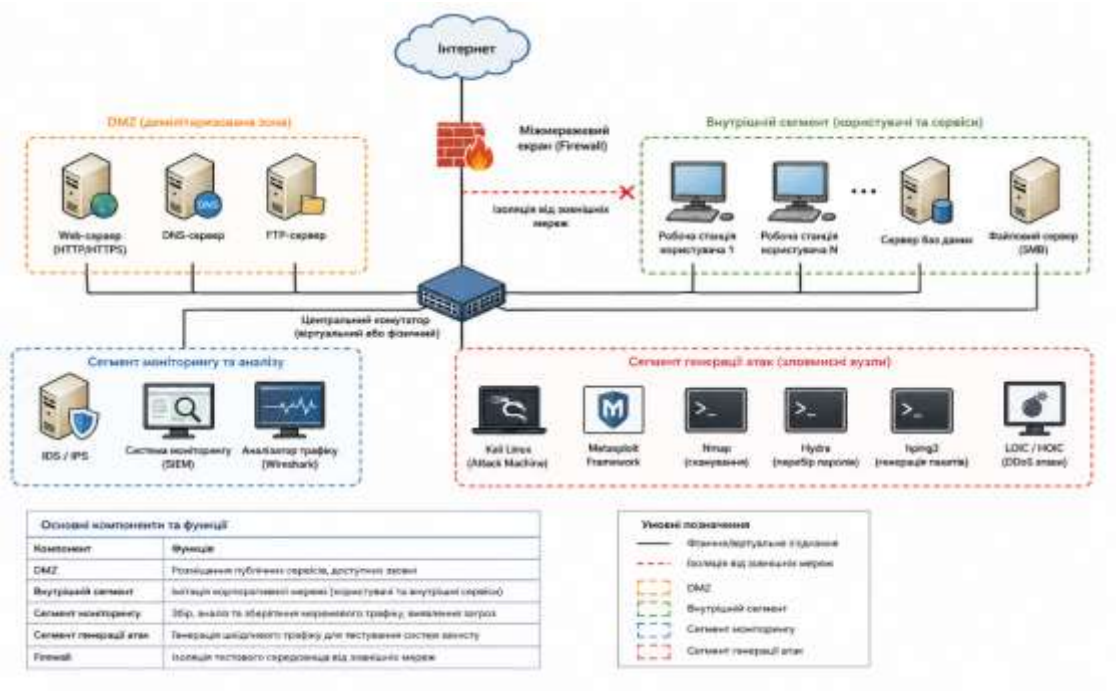


Рисунок 3.20 – Схема мережевої інфраструктури ізольованого середовища для моделювання кіберзагроз та аналізу мережевого трафіку

Джерело: розроблено автором на основі [74, 76, 77, 79] за допомогою ChatGPT

Першим кроком є **створення мережевих вузлів**, які будуть використовуватись у тестовому середовищі. Вузлами можуть бути сервери, робочі станції, маршрутизатори, комутатори або спеціалізовані системи моніторингу. Залежно від цілей дослідження використовуються фізичні або віртуальні машини (найчастіше для побудови лабораторних середовищ застосовуються засоби віртуалізації, такі як VirtualBox, VMware Workstation, оскільки вони дозволяють швидко створювати, змінювати та відновлювати конфігурацію мережі без потреби у великій кількості фізичного обладнання.

Під час налаштування вузлів визначаються: IP-адресація, параметри DNS, ролі вузлів у мережі, права доступу користувачів, служби та сервіси, що будуть функціонувати у мережі [76].

Наступним етапом є **налаштування мережевої топології та протоколів передачі даних**. Топологія визначає структуру взаємодії між вузлами мережі та може бути реалізована у вигляді: зірки, шини, кільця, деревоподібної або гібридної структури. У більшості сучасних тестових середовищ використовується топологія типу «зірка», де всі вузли підключаються через центральний комутатор або віртуальний мережевий міст [76].

Особлива увага приділяється налаштуванню мережевих протоколів. Основою функціонування мережі є стек TCP/IP, який забезпечує маршрутизацію пакетів, встановлення з’єднань та передачу даних між вузлами. Також можуть налаштовуватись: DHCP для автоматичної видачі IP-адрес, DNS для перетворення доменних імен, HTTP/HTTPS для вебтрафіку, SSH для віддаленого адміністрування, FTP або SMB для передачі файлів.

У деяких випадках додатково реалізується VLAN-сегментація для поділу мережі на ізольовані логічні сегменти та моделювання корпоративної інфраструктури [74].

Для ефективного аналізу систем виявлення вторгнень необхідно **забезпечити генерацію нормального та шкідливого трафіку** [77]. Нормальний трафік імітує типову роботу користувачів у мережі: вебперегляд, передачу файлів, використання електронної пошти та роботу з мережевими сервісами [78]. Для генерації звичайного трафіку можуть використовуватись: веббраузери,

скрипти автоматизації; утиліти iperf, curl, wget; емулятори користувацької активності.

Шкідливий трафік (аномальний, мережевий трафік атак) створюється для перевірки ефективності засобів моніторингу та виявлення загроз; це проактивний метод у кібербезпеці, відомий як симуляція атак (Breach and Attack Simulation – BAS) або тестування на проникнення (Penetration Testing) [79]. Для цього застосовуються спеціалізовані інструменти:

– Nmap Official Documentation – для сканування мережі;

– Metasploit Framework Documentation – для моделювання експлуатації вразливостей;

– Hydra – для атак перебором паролів;

– hping3 – для генерації спеціалізованих пакетів;

– LOIC або аналоги – для імітації DDoS-навантаження.

Мережа може включати внутрішній сегмент, DMZ та сегмент зловмисних вузлів. Це дозволяє відтворювати реальні сценарії кіберзагроз.

Генерація шкідливого трафіку дозволяє отримати реалістичні набори даних для подальшого аналізу та навчання систем виявлення вторгнень.

Однією з найважливіших вимог під час створення тестового середовища є його **повна ізоляція від зовнішніх та корпоративних мереж**. Це необхідно для запобігання випадковому поширенню шкідливого трафіку, витоку даних або несанкціонованому доступу до реальної інфраструктури [79].

Використання ізольованого середовища, сучасних засобів генерації трафіку, інструментів аналізу пакетів та методів попередньої обробки даних дозволяє створити надійну основу для дослідження та впровадження інтелектуальних систем кібербезпеки. Подальший розвиток даного напряму пов’язаний із застосуванням глибокого навчання, потокової обробки трафіку та адаптивних моделей виявлення аномалій у реальному часі.

3. Генерація трафіку (нормального та атак) є важливим етапом дослідження та тестування систем виявлення вторгнень (IDS/IPS), міжмережевих екранів і засобів кіберзахисту. Вона дозволяє створити контрольоване

середовище, у якому моделюється як нормальна поведінка користувачів, так і шкідлива активність для аналізу ефективності засобів захисту [80] (рис. 3.21).

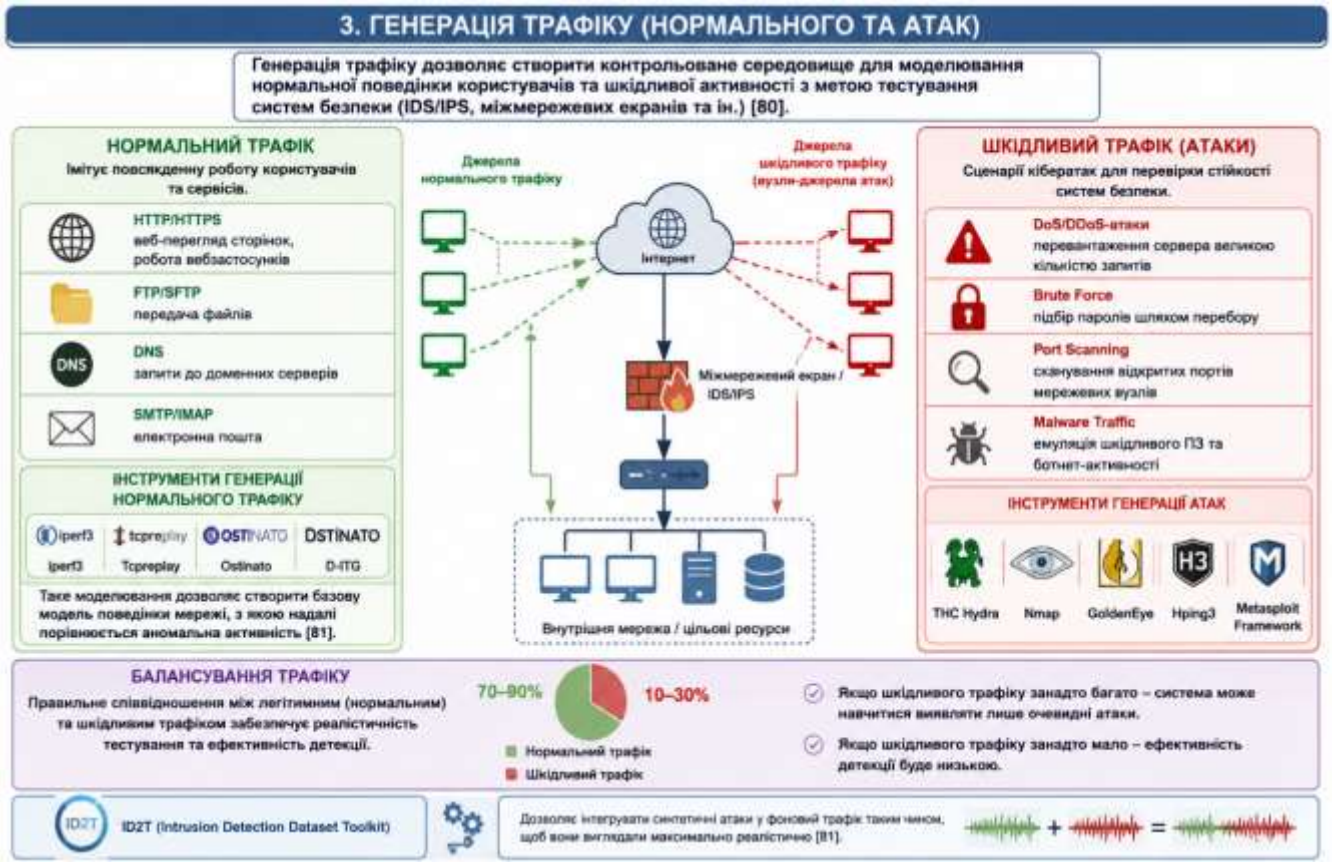


Рисунок 3.21 – Генерація нормального та шкідливого мережевого трафіку для тестування систем кібербезпеки

Джерело: розроблено автором на основі [80-81] за допомогою ChatGPT

Нормальний мережевий трафік імітує повсякденну роботу користувачів та сервісів. Найчастіше генеруються такі типи протоколів:

– HTTP/HTTPS – веб-перегляд сторінок, робота вебзастосунків;

– FTP/SFTP – передача файлів;

– DNS – запити до доменних серверів;

– SMTP/IMAP – електронна пошта.

Для генерації нормального трафіку застосовують інструменти **Iperf3**, **Tcpreplay**, **Ostinato** та **D-ITG**. Таке моделювання дозволяє створити базову модель поведінки мережі, з якою надалі порівнюється аномальна активність [81].

Для перевірки стійкості систем безпеки створюються сценарії кібератак. Найпоширенішими є:

– DoS/DDoS-атаки – перевантаження сервера великою кількістю запитів;

– Brute Force – підбір паролів шляхом автоматизованого перебору;

– Port Scanning – сканування відкритих портів мережевих вузлів;

– Malware Traffic – емуляція шкідливого програмного забезпечення та ботнет-активності.

Для моделювання шкідливого трафіку використовуються спеціалізовані засоби:

– THC Hydra – brute force атаки;

– Nmap – сканування портів і сервісів;

– GoldenEye – HTTP DoS-атаки;

– Hping3 – генерація TCP/UDP/ICMP пакетів;

– Metasploit Framework – створення складних сценаріїв експлуатації вразливостей.

Важливим аспектом є правильне співвідношення між легітимним (нормальним) та шкідливим трафіком. Якщо шкідливого трафіку занадто багато, система може навчитися виявляти лише очевидні атаки; якщо занадто мало — ефективність детекції буде низькою. Для реалістичного тестування поєднують нормальний і шкідливий трафік. Зазвичай нормальний трафік становить 70-90%, а атакувальний – 10-30%.

Сучасні інструменти, такі як ID2T (Intrusion Detection Dataset Toolkit), дозволяють інтегрувати синтетичні атаки у фоновий трафік таким чином, щоб вони виглядали максимально реалістично [81].

4. Збір мережевих даних є важливою складовою функціонування систем моніторингу мережі та забезпечення інформаційної безпеки. Отримані дані використовуються для виявлення атак, аналізу поведінки користувачів, дослідження мережевих інцидентів та забезпечення безперервного контролю за станом мережевої інфраструктури. Основними методами збору мережевої інформації є перехоплення пакетів, логування мережевих подій, фіксація потоків даних та збереження сирого мережевого трафіку (рис. 3.22).

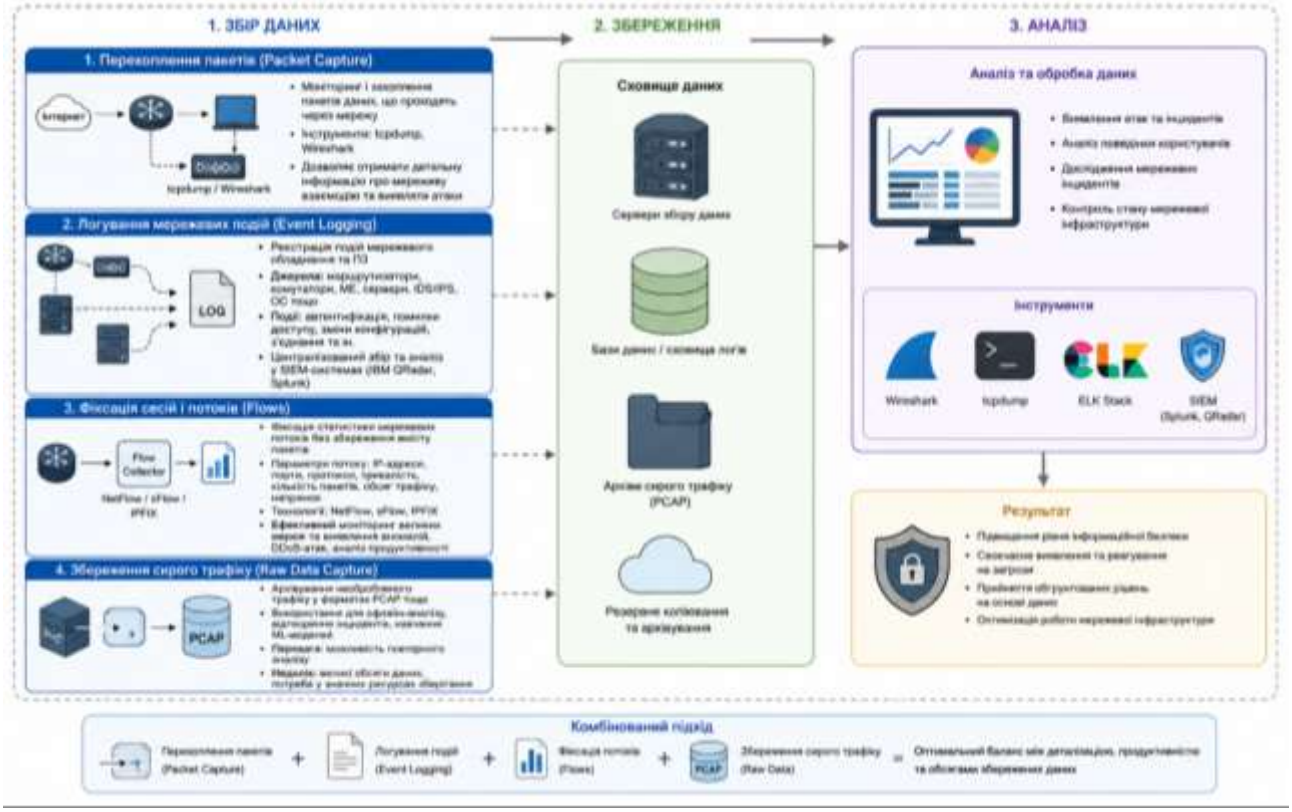


Рисунок 3.22 – Основні методи збору мережевих даних

Джерело: розроблено автором на основі [75, 77, 82, 83] за допомогою ChatGPT

Перехоплення пакетів (Packet Capture) полягає у моніторингу та захопленні пакетів даних, що проходять через задану мережу. Те, що робить **перехоплення пакетів відмінним від аналізу пакетів**, в основному полягає у їхній меті: перше «перехоплює» дані інших користувачів і, отже, є несанкціонованим втручанням, тоді як аналіз пакетів є легітимним аналізом потоку даних. Зазвичай на основі таких інструментів, як **tcpdump** та **Wireshark**, аналіз та перехоплення пакетів широко використовуються для моніторингу стану конкретної системи [82]. При комплексному підході до аналізу мережевого трафіку доцільно виділити три основні етапи: перехоплення трафіку, його збереження та подальший аналіз отриманих даних. Такий поділ дозволяє ефективніше організувати процес обробки мережевої інформації та підвищити якість виявлення мережевих інцидентів і загроз інформаційній безпеці (рис. 3.23).

Перехоплення мережевого трафіку здійснюється за допомогою спеціалізованих засобів – сніфферів. Сніффер (від англ. sniffer – «аналізатор» або

«перехоплювач») являє собою програмний чи програмно-апаратний засіб, призначений для захоплення та аналізу мережевого трафіку.

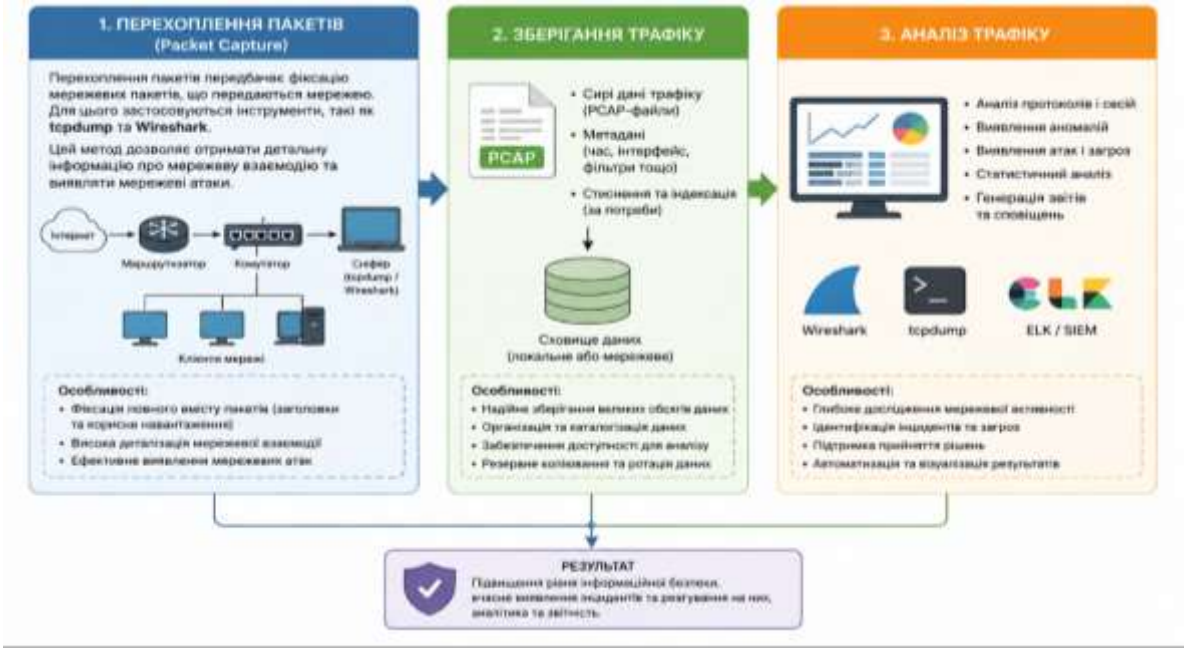


Рисунок 3.23 – Комплексний підхід до аналізу мережевого трафіку

Джерело: розроблено автором на основі [83, 84] за допомогою ChatGPT

Перехоплення трафіку може виконуватися кількома способами: шляхом прослуховування мережевого інтерфейсу, підключенням пристрою у розрив каналу зв’язку, дзеркалюванням (mirroring) трафіку на окремий інтерфейс, аналізом побічних електромагнітних випромінювань або через атаки на канальному чи мережевому рівнях, які забезпечують перенаправлення потоку даних через сніффер [83].

Залежно від місця розташування розрізняють сніффери, встановлені на маршрутизаторах або шлюзах мережі, а також сніффери, що функціонують на кінцевих вузлах мережі. У першому випадку перехоплюється весь мережевий трафік, що проходить через інтерфейси пристрою. У другому випадку можливе захоплення лише трафіку конкретного вузла мережі, якщо мережева карта функціонує у стандартному режимі, або трафіку всіх пристроїв певного сегмента мережі при роботі мережевого адаптера у режимі прослуховування (promiscuous mode) [84].

Цей метод є особливо важливим під час проведення цифрової криміналістики та аналізу мережевих атак, оскільки забезпечує максимально детальну інформацію про взаємодію вузлів мережі. Разом із тим, перехоплення

пакетів потребує значних обсягів пам’яті та ресурсів обробки, особливо у високошвидкісних мережах.

Логування мережевих подій передбачає реєстрацію подій, що виникають у процесі функціонування мережевого обладнання та програмного забезпечення. Джерелами логів можуть бути маршрутизатори, комутатори, міжмережеві екрани, сервери, системи виявлення вторгнень та операційні системи. У логах фіксуються спроби автентифікації, помилки доступу, зміни конфігурацій, мережеві з’єднання та інші події безпеки. Для централізованого збору та аналізу журналів часто застосовуються SIEM-системи, зокрема IBM QRadar або Splunk.

Перевагою логування є відносно невеликий обсяг даних у порівнянні з повним перехопленням трафіку, однак цей підхід не завжди дозволяє отримати повну картину мережевої взаємодії [75].

Фіксація сесій і потоків (Flows). Технологія flow-моніторингу базується на фіксації статистичної інформації про мережеві потоки без збереження повного вмісту пакетів. Потік визначається як сукупність пакетів, що мають однакові параметри: IP-адреси джерела та призначення, порти, тип протоколу тощо.

Найбільш поширеними технологіями є NetFlow, sFlow та IPFIX. Flow-записи містять інформацію про тривалість з’єднання, кількість переданих пакетів, обсяг трафіку та напрям передачі даних. Такий підхід дозволяє ефективно здійснювати моніторинг великих мереж із мінімальним навантаженням на систему зберігання даних.

Фіксація потоків широко застосовується для виявлення аномальної мережевої активності, DDoS-атак та аналізу продуктивності мережі.

Збереження сирих даних трафіку передбачає архівування необробленого трафіку у форматах PCAP або аналогічних структурах. Такі дані можуть використовуватись для подальшого офлайн-аналізу, повторного відтворення мережевих інцидентів та навчання систем машинного навчання. Основною перевагою збереження сирого трафіку є можливість повторного аналізу даних із використанням нових методів або інструментів. Водночас цей підхід характеризується високими вимогами до обсягів дискового простору та засобів резервного копіювання.

У сучасних системах кібербезпеки часто застосовується комбінований підхід, коли одночасно використовуються packet capture, flow-моніторинг та фіксація подій. Це дозволяє досягти оптимального балансу між деталізацією інформації, продуктивністю системи та обсягами збережених даних [77].

5. Попередня обробка даних є важливим етапом підготовки інформації до аналізу та машинного навчання. Її основна мета полягає у підвищенні якості даних, зменшенні впливу шуму та забезпеченні коректної роботи алгоритмів аналізу (рис. 3.24).

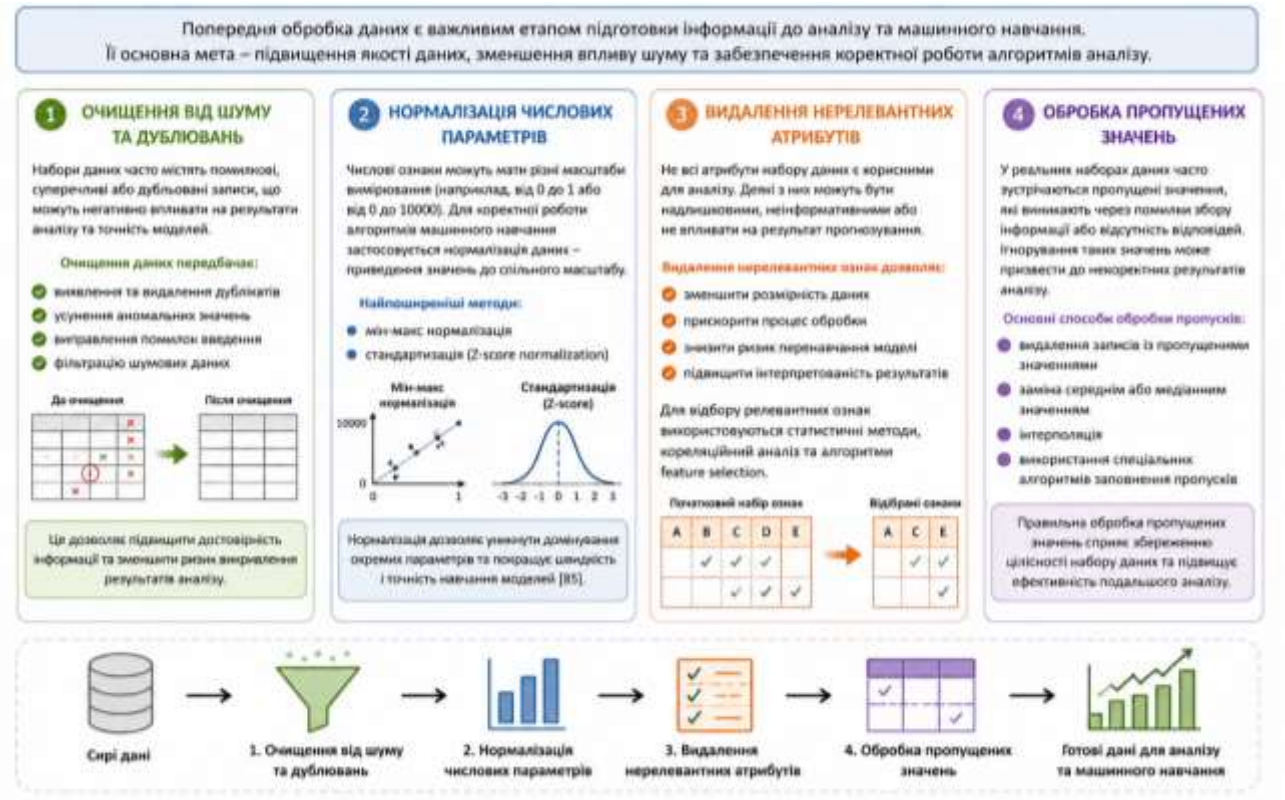


Рисунок 3.24 – Основні процеси попередньої обробки даних

Джерело: розроблено автором на основі [85, 86] за допомогою ChatGPT

Очищення від шуму та дублювань. На практиці набори даних часто містять помилкові, суперечливі або дубльовані записи. Такі дані можуть негативно впливати на результати аналізу та точність моделей. Очищення даних передбачає: виявлення та видалення дублікатів, усунення аномальних значень, виправлення помилок введення, фільтрацію шумових даних. Цей етап дозволяє підвищити достовірність інформації та зменшити ризик викривлення результатів аналізу.

Нормалізація числових параметрів. Числові ознаки у наборах даних можуть мати різні масштаби вимірювання. Наприклад, один параметр може змінюватися в межах від 0 до 1, а інший – від 0 до 10000. Для забезпечення коректної роботи алгоритмів машинного навчання застосовується нормалізація даних – приведення значень до спільного масштабу.

Найпоширенішими методами є:

- мін-макс нормалізація;
- стандартизація (Z-score normalization).

Нормалізація дозволяє уникнути домінування окремих параметрів та покращує швидкість і точність навчання моделей [85].

Видалення нерелевантних атрибутів. Не всі атрибути набору даних є корисними для аналізу. Деякі з них можуть бути надлишковими, неінформативними або не впливати на результат прогнозування. Видалення нерелевантних ознак дозволяє: зменшити розмірність даних, прискорити процес обробки, знизити ризик перенавчання моделі, підвищити інтерпретованість результатів.

Для відбору релевантних ознак використовуються статистичні методи, кореляційний аналіз та алгоритми feature selection.

Обробка пропущених значень. У реальних наборах даних часто зустрічаються пропущені значення, які виникають через помилки збору інформації або відсутність відповідей. Ігнорування таких значень може призвести до некоректних результатів аналізу. Основними способами обробки пропусків є: видалення записів із пропущеними значеннями, заміна середнім або медіанним значенням, інтерполяція, використання спеціальних алгоритмів заповнення пропусків. Правильна обробка пропущених значень сприяє збереженню цілісності набору даних та підвищує ефективність подальшого аналізу [86].

6. Виділення ознак (Feature Engineering) є одним із ключових складників побудови систем аналізу мережевого трафіку на основі машинного навчання. На цьому етапі сирі мережеві дані перетворюються у набір інформативних характеристик, придатних для подальшого навчання моделей класифікації або

виявлення аномалій. До основних типів ознак належать статистичні характеристики трафіку. Вони описують поведінку мережевих потоків і включають тривалість сесії, кількість пакетів у потоці, середній розмір пакета, швидкість передачі даних, кількість байтів, співвідношення вхідного та вихідного трафіку тощо. Такі параметри дозволяють моделі виявляти закономірності між нормальним і шкідливим трафіком [87]. Схема процесу виділення ознак для аналізу мережевого трафіку наведена на рис. 3.25.

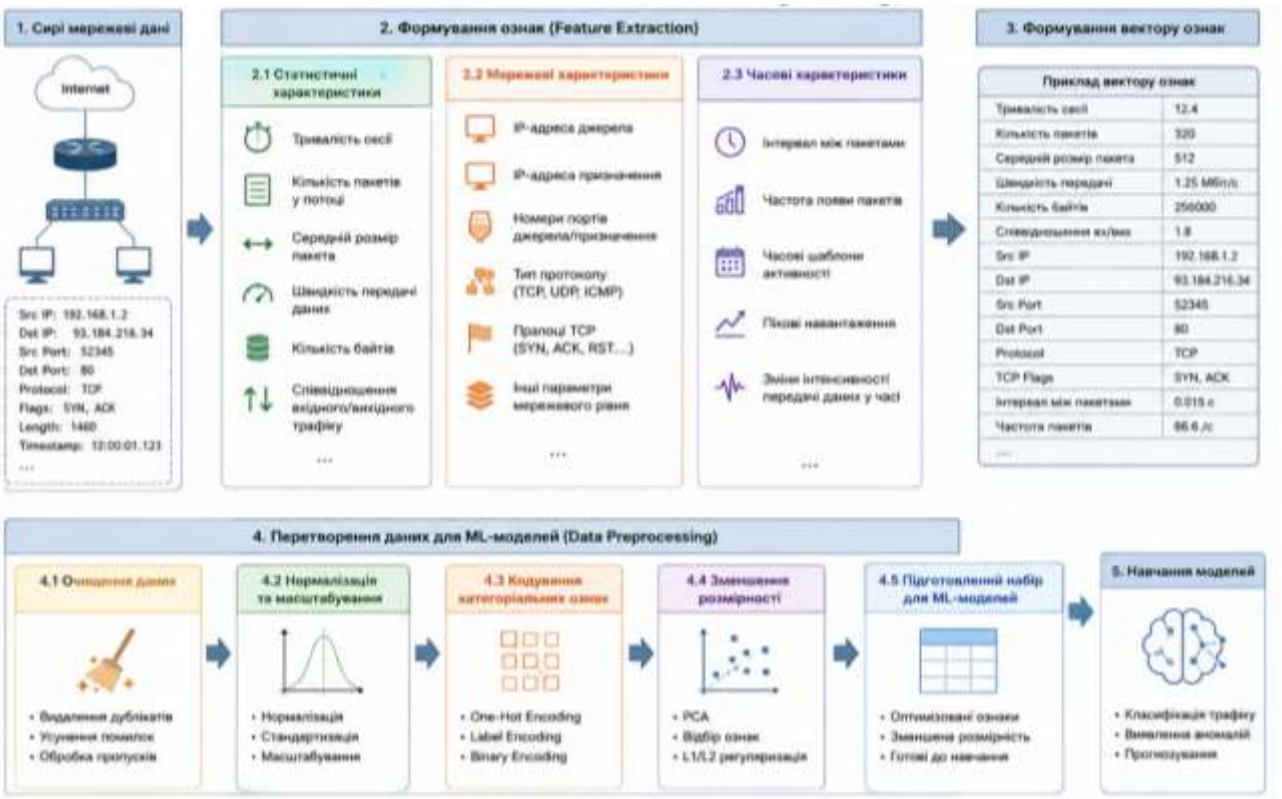


Рисунок 3.25 – Схема процесу виділення ознак для аналізу мережевого трафіку

Джерело: розроблено автором на основі [87, 88] за допомогою ChatGPT

Важливу роль відіграють також мережеві характеристики, серед яких IP-адреси джерела та призначення, номери портів, типи транспортних протоколів (TCP, UDP, ICMP), прапорці TCP-з’єднань та інші параметри мережевого рівня. Аналіз цих ознак дозволяє ідентифікувати типи сервісів, напрямки передачі даних та потенційно небезпечні з’єднання.

Для задач аналізу трафіку велике значення мають часові характеристики. До них належать інтервали між пакетами, частота появи пакетів, часові шаблони активності, пікові навантаження та зміни інтенсивності передачі даних у часі.

Саме часові залежності особливо ефективно аналізуються моделями глибокого навчання, зокрема LSTM-мережами, які здатні враховувати послідовність подій у мережевому потоці [88].

Після формування ознак виконується перетворення даних у формат, придатний для ML-моделей. Цей процес включає очищення даних, нормалізацію та масштабування числових параметрів, усунення пропущених значень, кодування категоріальних ознак, а також зменшення розмірності за допомогою методів PCA або відбору найбільш інформативних характеристик. Такі процедури дозволяють підвищити точність класифікації та зменшити обчислювальні витрати.

7. Розмітка даних. Після етапу попередньої обробки даних виконується розмітка мережевого трафіку, яка є необхідною для подальшого навчання моделей машинного навчання та систем виявлення вторгнень. На цьому етапі кожен запис у наборі даних отримує відповідну мітку класу, що дозволяє алгоритму відрізняти нормальну мережеву активність від шкідливих дій. Процес розмітки даних мережевого трафіку наведено на рис. 3.26.

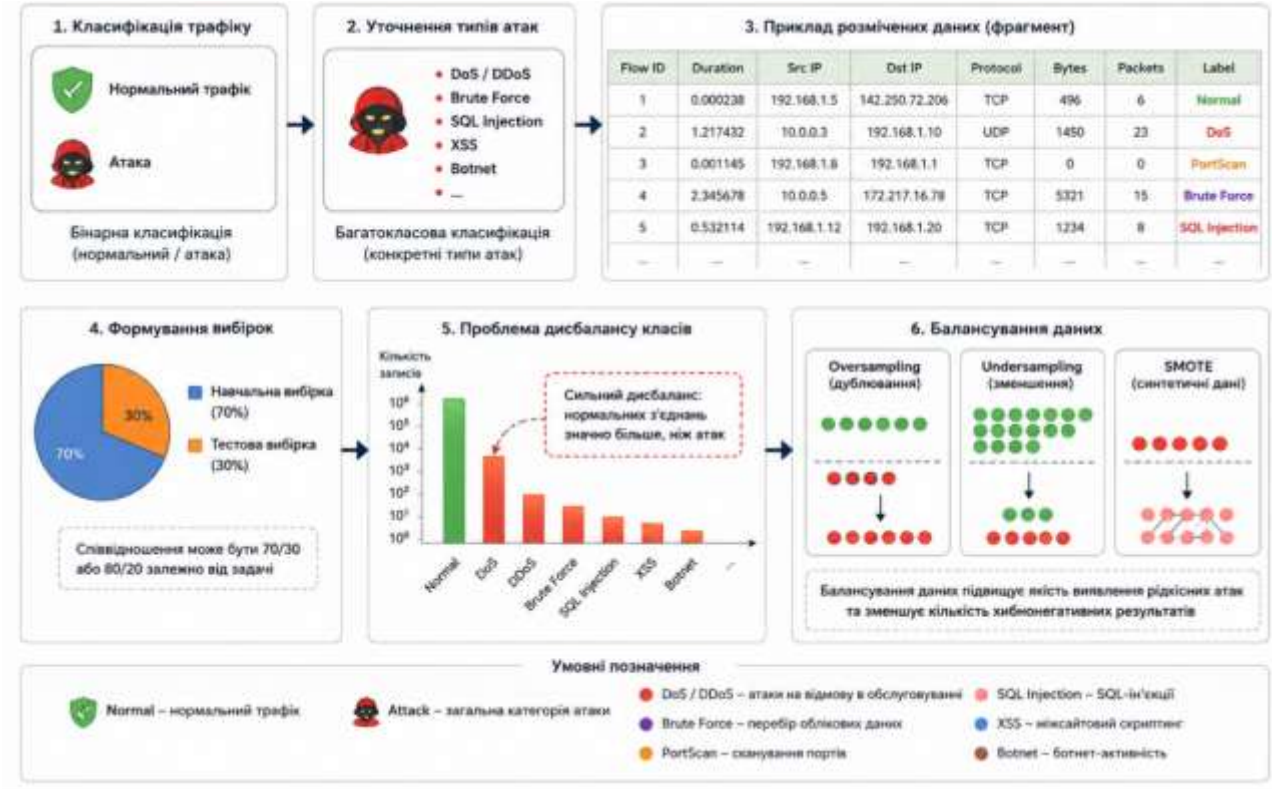


Рисунок 3.26 – Процес розмітки даних мережевого трафіку

Джерело: розроблено автором на основі [89, 90] за допомогою ChatGPT

Першочергово здійснюється класифікація трафіку на два основні класи: **«нормальний»** та **«атака»**. Такий підхід використовується у бінарній класифікації IDS-систем і дозволяє навчити модель виявляти аномалії у мережевих потоках. У сучасних дослідженнях також застосовується багатокласова класифікація, де окремо виділяються конкретні типи атак, зокрема DoS, DDoS, Brute Force, SQL Injection, XSS, Botnet та інші [89].

Для підвищення точності моделі проводиться уточнення типів атак відповідно до структури обраного датасету. Наприклад, у наборах CIC-IDS2017 або UNSW-NB15 кожен запис містить окрему категорію загрози, що дає змогу навчати систему не лише визначати факт атаки, а й класифікувати її тип. Це особливо важливо для сучасних систем кібербезпеки, оскільки різні атаки потребують різних механізмів реагування.

Після завершення розмітки формується навчальна та тестова вибірки. Найчастіше дані поділяються у співвідношенні 70/30 або 80/20, де більша частина використовується для навчання моделі, а менша – для перевірки її ефективності. Такий підхід дозволяє оцінити здатність алгоритму узагальнювати знання та виявляти нові загрози на невідомих даних.

Однією з основних проблем під час розмітки є дисбаланс класів, оскільки у реальному мережевому трафіку нормальних з’єднань значно більше, ніж атак. Для вирішення цієї проблеми застосовуються методи балансування даних: oversampling, undersampling або алгоритм SMOTE, який синтетично генерує нові приклади для міноритарних класів. Використання балансування дозволяє підвищити якість виявлення рідкісних атак та зменшити кількість хибнонегативних результатів [90].

8. Підготовка експериментального середовища для систем виявлення вторгнень (Intrusion Detection Systems, IDS) є важливим етапом дослідження, оскільки від правильного налаштування наборів даних, вибору метрик та сценаріїв тестування залежить достовірність отриманих результатів (рис. 3.27). У сучасних дослідженнях IDS широко використовуються як сигнатурні підходи, так і моделі машинного навчання та глибокого навчання.

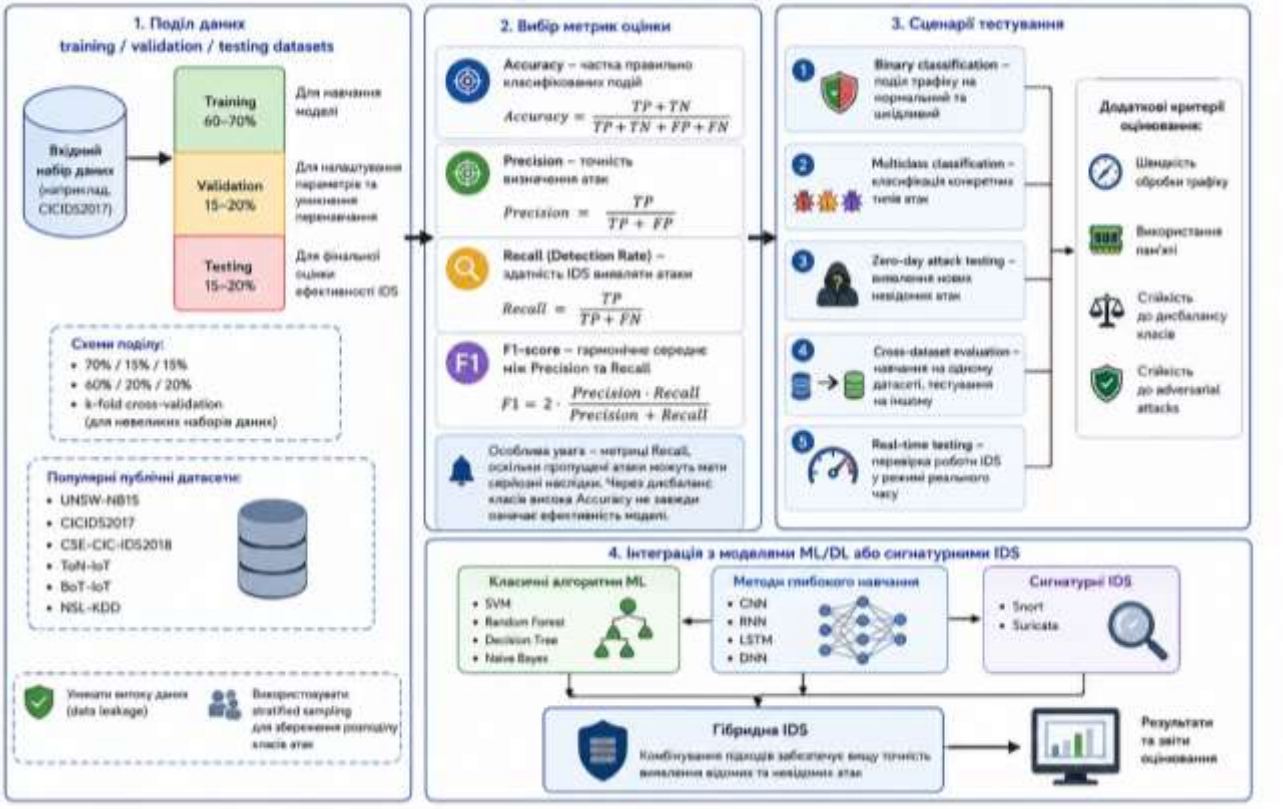


Рисунок 3.27 – Підготовка експериментального середовища для систем виявлення вторгнень (IDS)

Джерело: розроблено автором за допомогою ChatGPT

Поділ на training / validation / testing datasets. Для забезпечення коректного оцінювання моделей IDS набір даних поділяють на декілька частин:

- **Training dataset** – використовується для навчання моделі;
- **Validation dataset** – застосовується для налаштування параметрів та уникнення перенавчання;
- **Testing dataset** – використовується для фінальної оцінки ефективності IDS.

Найпоширенішими схемами є [91, 92]:

- 70% / 15% / 15%;
- 60% / 20% / 20%;
- k-fold cross-validation для невеликих наборів даних.

У дослідженнях IDS важливо забезпечити відсутність витоку даних (data leakage), коли однакові або дуже схожі записи потрапляють одночасно до training та testing datasets. Також рекомендується використовувати **stratified sampling**, що дозволяє зберігати однаковий розподіл класів атак у всіх вибірках.

Для експериментів часто застосовують такі публічні датасети: UNSW-NB15, CICIDS2017, CSE-CIC-IDS2018, ToN-IoT, BoT-IoT, NSL-KDD.

Вибір метрик оцінки. Для оцінювання IDS використовують декілька основних метрик, які більш детально описані в п.п 2.3 даної кваліфікаційної роботи:

- **Accuracy** – частка правильно класифікованих подій;
- **Precision** – точність визначення атак;
- **Recall (Detection Rate)** – здатність IDS виявляти атаки;
- **F1-score** – гармонічне середнє між Precision та Recall.

Формули цих метрик наведено в п.п. 2.3 (формули 2.11– 2.14).

У сучасних IDS особлива увага приділяється метриці **Recall**, оскільки пропущені атаки можуть призвести до серйозних наслідків для інформаційної безпеки. Через дисбаланс класів висока Accuracy не завжди означає ефективність моделі.

Для комплексного оцінювання IDS необхідно **налаштувати різні сценарії тестування**:

1. **Binary classification** – поділ трафіку на нормальний та шкідливий.
2. **Multiclass classification** – класифікація конкретних типів атак.
3. **Zero-day attack testing** – тестування здатності IDS виявляти нові невідомі атаки.
4. **Cross-dataset evaluation** навчання на одному датасеті та тестування на іншому.
5. **Real-time testing** – перевірка роботи IDS у режимі реального часу.

Додатково можуть оцінюватися: швидкість обробки трафіку, використання пам’яті, стійкість до дисбалансу класів, стійкість до adversarial attacks.

Інтеграція з моделями машинного навчання або сигнатурними IDS. Сучасні IDS можуть інтегруватися з:

- класичними алгоритмами машинного навчання (SVM, Random Forest, Decision Tree, Naive Bayes);
- методами глибокого навчання (CNN, RNN, LSTM, DNN);
- сигнатурними IDS (наприклад, Snort або Suricata).

Моделі ML/DL дозволяють виявляти невідомі атаки та аномалії, тоді як сигнатурні IDS ефективно працюють із відомими шаблонами атак. Комбінування цих підходів формує гібридні IDS, які забезпечують вищу точність виявлення вторгнень.

На рис. 3.28 представлено архітектуру експериментального середовища для виявлення мережевих вторгнень та аналізу мережевого трафіку.

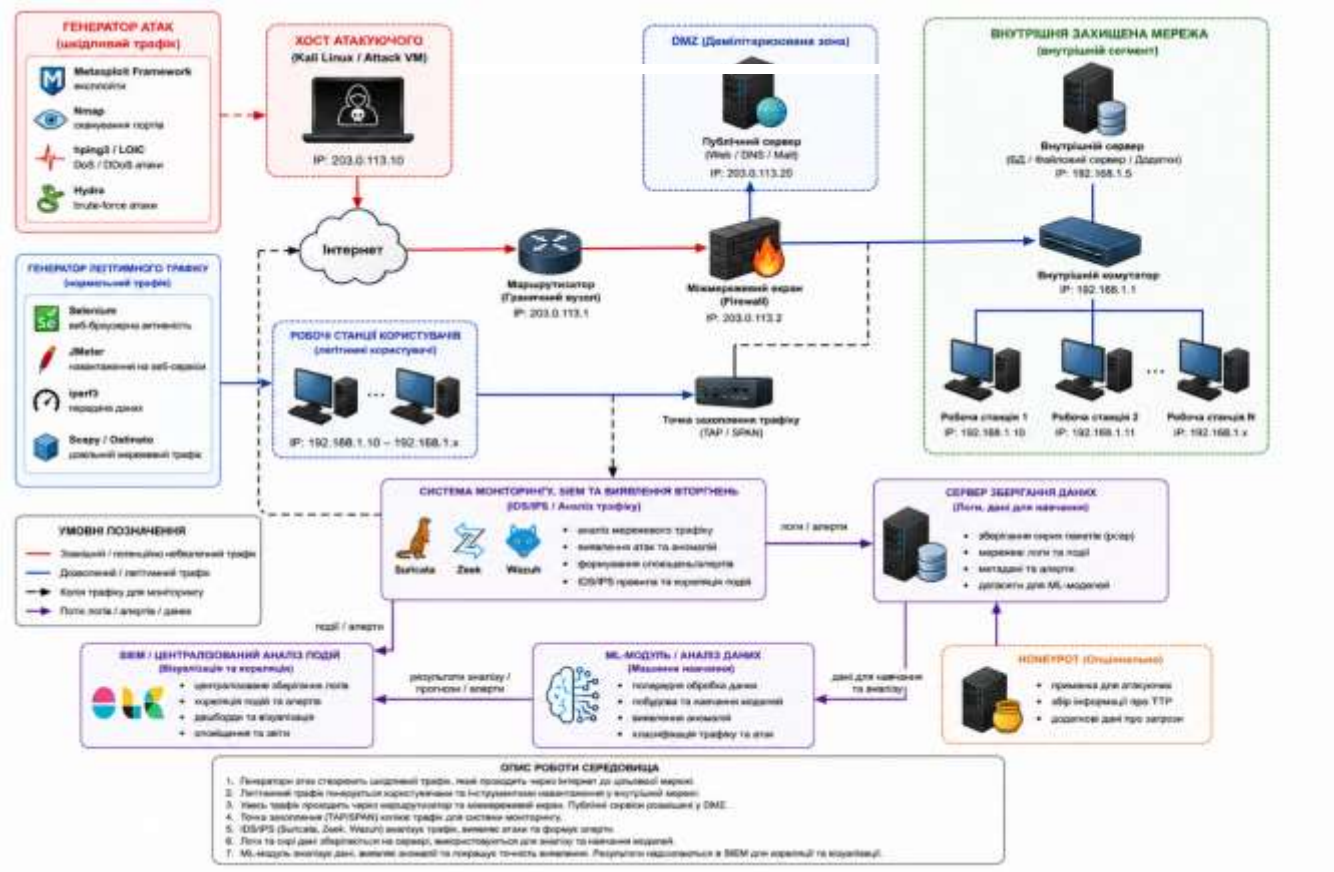


Рисунок 3.28 – Архітектура експериментального середовища для виявлення мережевих вторгнень

Джерело: розроблено автором за допомогою ChatGPT

Середовище включає генератори шкідливого та легітимного трафіку, зовнішню мережу Інтернет, демілітаризовану зону (Demilitarized Zone – DMZ), внутрішню захищену мережу, а також систему моніторингу та аналізу подій безпеки. Генератор атак імітує різні типи кіберзагроз, зокрема сканування портів, DoS/DDoS-атаки, brute-force атаки та SQL-ін’єкції, тоді як генератор легітимного трафіку створює нормальну мережеву активність користувачів. Увесь мережевий трафік проходить через маршрутизатор і міжмережевий екран, що забезпечує фільтрацію та сегментацію мережі між DMZ і внутрішнім сегментом. Для моніторингу та аналізу мережевої активності у середовищі використовується система IDS/IPS та SIEM, яка здійснює захоплення, обробку й кореляцію подій безпеки. Зібрані журнали, мережеві пакети та

метадані передаються на сервер зберігання даних, де формуються набори даних для подальшого аналізу. Додатково у структурі середовища передбачено ML-модуль, який реалізує методи машинного навчання для виявлення аномалій, класифікації мережевого трафіку та прогнозування атак. Запропонована архітектура дозволяє моделювати реальні сценарії кіберзагроз, здійснювати дослідження ефективності систем виявлення вторгнень та формувати якісні набори даних для навчання інтелектуальних систем кібербезпеки.

Формування експериментального середовища та підготовка даних мережевого трафіку є критично важливими етапами створення систем виявлення вторгнень. Якість зібраних та оброблених даних безпосередньо впливає на точність моделей машинного навчання та ефективність виявлення кіберзагроз.

Висновки до третього розділу

1. У ході виконання роботи було створено гібридну модель адаптивної системи виявлення вторгнень (IDS), яка поєднує сигнатурний і поведінковий підходи до аналізу мережевого трафіку. Розроблена модель забезпечує підвищення точності виявлення атак завдяки використанню методів машинного навчання, адаптивного аналізу аномалій та механізмів динамічного оновлення правил безпеки. Це дозволяє ефективніше реагувати на сучасні кіберзагрози та підвищувати рівень захисту інформаційних систем.

2. У процесі дослідження були проаналізовані сучасні підходи до побудови систем виявлення вторгнень, визначені їх сильні та слабкі сторони, а також обґрунтована необхідність використання адаптивної гібридної архітектури. Запропонована модель здатна ефективно виявляти як відомі, так і нові типи кібератак, що є особливо актуальним в умовах постійного розвитку загроз інформаційній безпеці. Отримані результати підтвердили, що застосування гібридного підходу дозволяє зменшити кількість хибнопозитивних спрацювань і підвищити швидкість реагування системи на підозрілу активність. Крім того, механізми адаптивного навчання забезпечують автоматичне пристосування IDS до змін мережевого середовища та поведінки користувачів.

Практичне значення розробленої моделі полягає у можливості її інтеграції в корпоративні мережі для підвищення ефективності захисту від кіберзагроз. Подальші дослідження доцільно спрямувати на вдосконалення продуктивності моделі, розширення набору алгоритмів машинного навчання та використання технологій штучного інтелекту для прогнозування складних багатовекторних атак.

3. Запропонована архітектура гібридної IDS реалізує комплексний підхід до аналізу мережевого трафіку шляхом поєднання методів виокремлення ознак, кластеризації, класифікації та адаптивного навчання. Така структура забезпечує ефективне виявлення аномалій, ідентифікацію типів атак та адаптацію системи до нових кіберзагроз. Використання гібридного підходу сприяє підвищенню точності виявлення вторгнень, зменшенню кількості хибних спрацювань і забезпечує більш гнучке функціонування IDS у динамічному мережевому середовищі.

4. Алгоритм функціонування розробленої адаптивної гібридної системи виявлення вторгнень забезпечує комплексний аналіз мережевого трафіку завдяки поєднанню методів кластеризації, класифікації та адаптивного оновлення моделі. Використання гібридної архітектури дозволяє виявляти як відомі атаки, так і нові аномальні загрози, які відсутні у навчальній вибірці. Завдяки механізму автоматичного оновлення система здатна адаптуватися до змін у мережевому середовищі та підтримувати високий рівень точності виявлення атак у режимі реального часу. Це підвищує ефективність кіберзахисту та забезпечує оперативне реагування на потенційні загрози інформаційній безпеці.

5. Реалізація та налаштування гібридної моделі IDS базується на поєднанні сигнатурного аналізу з поведінковим методом виявлення аномалій на основі алгоритму k-means. Такий підхід дозволяє здійснювати комплексний аналіз мережевого трафіку, виявляючи як відомі атаки за наявними сигнатурами, так і нові загрози шляхом аналізу відхилень у поведінці мережевих потоків. Запропонована архітектура охоплює всі основні етапи функціонування IDS: збір

даних, попередню обробку, кластеризацію, сигнатурну перевірку, прийняття рішень і формування реакції системи.

Використання алгоритму k-means підвищує здатність IDS виявляти невідомі або модифіковані атаки, тоді як сигнатурний модуль забезпечує високу швидкість і точність розпізнавання вже відомих загроз. Поєднання цих компонентів дозволяє зменшити кількість пропущених атак та підвищити загальну ефективність системи. Таким чином, розроблена гібридна модель IDS є ефективним рішенням для захисту сучасних комп'ютерних мереж і поєднує переваги традиційних методів із можливістю адаптації до нових кіберзагроз.

6. У результаті роботи було створено експериментальне середовище для дослідження та тестування системи виявлення вторгнень на основі аналізу мережевого трафіку. Розроблена архітектура включає зовнішню мережу, демілітаризовану зону (DMZ), внутрішній захищений сегмент, генератори легітимного та шкідливого трафіку, IDS/IPS-систему, SIEM-компоненти, сервер зберігання даних і модуль машинного навчання. Така структура дозволяє моделювати реальні сценарії мережевої взаємодії та кіберзагроз у контрольованих умовах. У процесі підготовки мережевого трафіку були розглянуті основні етапи попередньої обробки даних, зокрема очищення, формування ознак, нормалізація, кодування категоріальних параметрів і балансування класів. Використання як легітимного, так і шкідливого трафіку забезпечує створення репрезентативного набору даних для навчання та тестування моделей виявлення вторгнень. Отже, реалізоване експериментальне середовище формує надійну основу для подальших досліджень методів машинного навчання та оцінювання ефективності сучасних систем кібербезпеки в умовах реальних мережевих загроз.

ВИСНОВКИ

На основі проведеного дослідження щодо теми кваліфікаційної бакалаврської роботи «Розробка адаптивних систем виявлення вторгнень гібридними методами», можемо зробити наступні висновки.

1. Системи виявлення вторгнень пройшли значний шлях розвитку – від простих засобів аналізу журналів подій до сучасних інтелектуальних платформ на основі штучного інтелекту. Їх еволюція була зумовлена постійним ускладненням кіберзагроз та розвитком інформаційних технологій. Сьогодні IDS є важливою складовою систем кібербезпеки, забезпечуючи своєчасне виявлення атак і підвищення рівня захисту інформаційних ресурсів.

2. Системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS) є важливими складовими сучасної системи кібербезпеки, які забезпечують комплексний захист інформаційних ресурсів від кіберзагроз. Їх головне призначення полягає у виявленні, аналізі та протидії несанкціонованим діям у мережі або інформаційній системі. Сутність IDS полягає у постійному моніторингу мережевого трафіку та системних подій з метою виявлення ознак атак, підозрілої активності чи порушень політики безпеки. На відміну від IDS, системи IPS не лише виявляють загрози, а й автоматично блокують або обмежують шкідливу активність у режимі реального часу. Таким чином, IDS виконує переважно функцію контролю та сповіщення, тоді як IPS забезпечує активний захист і реагування на інциденти. Отже, впровадження та ефективне використання IDS і IPS є необхідною умовою забезпечення належного рівня кіберзахисту в сучасному цифровому середовищі.

3. Існують різні типи систем виявлення вторгнень (IDS), серед яких основними є мережеві системи виявлення вторгнень (NIDS), хост-системи (HIDS) та системи для застосунків (AIDS). Кожен із цих типів виконує окремі функції у процесі забезпечення кібербезпеки: NIDS контролюють мережевий трафік, HIDS аналізують події на окремому пристрої, а AIDS забезпечують захист прикладного програмного забезпечення. Така класифікація дозволяє ефективно виявляти різні види кіберзагроз та забезпечувати багаторівневий

захист інформаційних систем. Отже, комплексне використання різних типів IDS підвищує ефективність моніторингу, своєчасність реагування на інциденти та загальний рівень безпеки інформаційної інфраструктури.

4. Архітектура систем виявлення вторгнень ґрунтується на взаємодії основних компонентів: сенсорів збору інформації, блоку аналізу, бази даних та блоку реагування. Кожен із цих елементів виконує окремі функції, що забезпечують ефективне виявлення, обробку та аналіз подій безпеки. Особливе значення має підсистема аналізу, від ефективності якої залежить точність виявлення кіберзагроз та швидкість реагування на них.

Модульна побудова IDS дозволяє інтегрувати їх із іншими засобами кіберзахисту, зокрема IPS, міжмережевими екранами та системами управління безпекою. На відміну від IDS, системи IPS не лише виявляють загрози, а й автоматично блокують шкідливу активність у режимі реального часу, забезпечуючи активний захист мережі. Таким чином, поєднання IDS та IPS створює комплексний механізм моніторингу, виявлення та запобігання атакам, що підвищує рівень захищеності інформаційної інфраструктури.

5. Адаптивні системи виявлення вторгнень є сучасним напрямом розвитку засобів кібербезпеки, оскільки здатні змінювати алгоритми роботи відповідно до нових загроз та особливостей функціонування інформаційної системи. На відміну від традиційних IDS, адаптивні системи використовують методи машинного навчання, аналізу поведінки та штучного інтелекту для виявлення невідомих атак і аномалій у режимі реального часу.

Основною перевагою адаптивних IDS є здатність до самонавчання, підвищення точності аналізу та зменшення кількості хибних спрацювань. Це дозволяє забезпечити більш ефективний захист інформаційної інфраструктури в умовах постійного розвитку кіберзагроз. Таким чином, впровадження адаптивних систем виявлення вторгнень сприяє підвищенню рівня кібербезпеки, оперативності реагування на інциденти та стійкості інформаційних систем до сучасних атак.

6. Гібридні методи є одним із найбільш перспективних напрямів розвитку сучасних систем кібербезпеки, оскільки дозволяють поєднати переваги різних

підходів до виявлення та протидії кіберзагрозам. Використання комбінації сигнатурного аналізу, поведінкових методів, машинного навчання, кластеризації, статистичного аналізу та адаптивних алгоритмів забезпечує підвищення точності роботи систем виявлення вторгнень і зменшення кількості хибних спрацювань.

7. Особливу роль у побудові адаптивних систем відіграють методи машинного навчання та кластерного аналізу, які дозволяють виявляти приховані закономірності в мережевому трафіку та знаходити нові типи атак без попередньо визначених сигнатур. Крім того, сучасні гібридні підходи, зокрема Сигнатурний + поведінковий аналіз, Машинне навчання + експертні правила, IDS + IPS, Кластеризація + машинне навчання, Статистичні методи + штучний інтелект (AI), Deep Learning + Big Data тощо забезпечують високий рівень захисту інформаційних ресурсів і підтримують можливість роботи в умовах постійної зміни кіберзагроз.

Таким чином, застосування гібридних методів дозволяє створювати інтелектуальні адаптивні системи виявлення вторгнень, здатні ефективно функціонувати в реальному часі та забезпечувати високий рівень кіберзахисту сучасних інформаційних систем і мереж.

8. У результаті формалізації задачі виявлення вторгнень визначено основні компоненти системи: множину подій, набір ознак, механізм класифікації та критерії прийняття рішення. Задача виявлення вторгнень може бути представлена як задача бінарної класифікації мережевого трафіку на нормальний та аномальний.

Розглянуті математичні моделі дозволяють описати процес аналізу мережевих подій та створюють основу для застосування сучасних методів машинного навчання й інтелектуального аналізу даних. Використання формалізованого підходу забезпечує підвищення точності виявлення атак, зменшення кількості хибних спрацювань та підвищення рівня захищеності інформаційних систем.

Окрему увагу приділено гібридним системам виявлення вторгнень, які поєднують сигнатурні методи, методи аналізу аномалій та алгоритми машинного

навчання. Використання гібридного підходу дозволяє підвищити ефективність виявлення як відомих, так і нових типів атак, зменшити кількість хибних спрацювань та покращити адаптивність системи до змін мережевого середовища.

Метрики оцінювання є ключовим інструментом аналізу ефективності систем виявлення вторгнень. Вибір метрик залежить від конкретних вимог системи, однак у кібербезпеці особливу увагу приділяють мінімізації пропущених атак і контролю рівня хибних спрацювань. Застосування наведених метрик дає можливість комплексно оцінювати якість роботи моделей виявлення вторгнень та визначати їх придатність для практичного використання.

9. У результаті виконання роботи було розроблено гібридну модель адаптивної системи виявлення вторгнень (IDS), яка поєднує сигнатурний та поведінковий підходи до аналізу мережевого трафіку. Запропонована модель забезпечує підвищення точності виявлення атак за рахунок комплексного використання методів машинного навчання, адаптивного аналізу аномалій та механізмів оновлення правил безпеки в реальному часі.

10. У процесі дослідження було проаналізовано сучасні підходи до побудови IDS, визначено їх переваги та недоліки, а також обґрунтовано необхідність створення адаптивної гібридної архітектури. Реалізована модель дозволяє ефективно виявляти як відомі, так і нові типи кібератак, що особливо важливо в умовах постійної еволюції загроз інформаційній безпеці.

Отримані результати підтвердили, що використання гібридного підходу сприяє зменшенню кількості хибнопозитивних спрацювань та підвищує швидкість реагування системи на підозрілу активність. Крім того, адаптивний механізм навчання дозволяє IDS автоматично пристосовуватися до змін у структурі мережевого середовища та поведінці користувачів.

Практична цінність розробленої моделі полягає у можливості її інтеграції в корпоративні мережі та інформаційні системи для забезпечення більш надійного захисту від кіберзагроз. У подальших дослідженнях доцільно зосередити увагу на оптимізації продуктивності моделі, розширенні набору алгоритмів

машинного навчання та використанні технологій штучного інтелекту для прогнозування складних багатовекторних атак.

11. Запропонована архітектура гібридної моделі IDS забезпечує комплексний підхід до аналізу мережевого трафіку шляхом поєднання методів виокремлення ознак, кластеризації, класифікації та адаптивного навчання. Така послідовність етапів дозволяє ефективно виявляти аномалії, ідентифікувати типи атак та адаптувати систему до нових кіберзагроз. Використання гібридного підходу підвищує точність виявлення вторгнень, зменшує кількість хибних спрацювань та забезпечує більш гнучке функціонування IDS в умовах динамічного мережевого середовища.

12. Алгоритм функціонування розробленої адаптивної гібридної системи виявлення вторгнень забезпечує комплексний підхід до аналізу мережевого трафіку шляхом поєднання методів кластеризації, класифікації та адаптивного оновлення моделі. Використання гібридної архітектури дозволяє ефективно виявляти як відомі типи атак, так і нові аномальні загрози, що не були присутні у навчальній вибірці. Завдяки механізму автоматичного оновлення модель здатна адаптуватися до змін у мережевому середовищі та підтримувати високий рівень точності виявлення вторгнень у реальному часі. Це підвищує надійність системи кіберзахисту та забезпечує своєчасне реагування на потенційні загрози інформаційній безпеці.

13. Реалізація та налаштування гібридної моделі IDS передбачає поєднання сигнатурного аналізу з поведінковим методом виявлення аномалій на основі k-means. Такий підхід забезпечує більш комплексний аналіз мережевого трафіку, оскільки дозволяє одночасно виявляти як відомі атаки за наявними сигнатурами, так і потенційно нові загрози шляхом аналізу відхилень у поведінці мережевих потоків. Побудована архітектура охоплює всі ключові етапи роботи IDS: збір даних, попередню обробку, кластеризацію, сигнатурну перевірку, прийняття рішення та формування реакції системи.

Використання k-means у складі гібридної IDS підвищує здатність системи до виявлення невідомих або модифікованих атак, тоді як сигнатурний модуль забезпечує високу точність і швидкість ідентифікації вже відомих загроз.

Поєднання цих компонентів дає змогу зменшити кількість пропущених атак і підвищити загальну ефективність системи виявлення вторгнень. Таким чином, запропонована гібридна модель IDS є доцільним рішенням для захисту сучасних комп’ютерних мереж, оскільки поєднує переваги класичних методів виявлення з можливістю адаптації до нових типів мережевих загроз.

14. У результаті було сформовано експериментальне середовище для дослідження та тестування системи виявлення вторгнень на основі аналізу мережевого трафіку. Створена архітектура включає зовнішню мережу, демілітаризовану зону (DMZ), внутрішній захищений сегмент, генератори легітимного та шкідливого трафіку, IDS/IPS-систему, SIEM-компоненти, сервер зберігання даних і модуль машинного навчання. Запропонована структура дозволяє моделювати реальні сценарії мережевої взаємодії та кіберзагроз, забезпечуючи контрольовані умови для проведення експериментів.\n\nУ процесі підготовки даних мережевого трафіку було розглянуто основні етапи попередньої обробки даних, зокрема очищення, формування ознак, нормалізацію, кодування категоріальних параметрів та балансування класів. Використання як легітимного, так і шкідливого трафіку забезпечує формування репрезентативного набору даних для навчання та тестування моделей виявлення вторгнень. Реалізоване експериментальне середовище створює надійну основу для подальшого дослідження методів машинного навчання та оцінювання ефективності систем кібербезпеки в умовах реальних мережевих загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Янко А. С., Макаренко О. І. Концепція системи виявлення та запобігання вторгнень до мережі. – *Системи управління, навігації та зв'язку*. 2022. № 2. – С. 59-67. URL: https://reposit.nupp.edu.ua/bitstream/PoltNTU/12052/1/document%20%281%29-59-67.pdf
2. Anderson J. P. Computer Security Threat Monitoring and Surveillance [Електронний ресурс]. – 1980. – URL: https://csrc.nist.gov/csrc/media/publications/conferencepaper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cspapers/ande80.pdf.
3. Denning, Dorothy E., "An Intrusion Detection Model, "Proceedings of the Seventh IEEE Symposium on Security and Privacy, May 1986, pages 119-131. URL: https://www.academia.edu/8674514/An_Intrusion_Detection_Model
4. Haystack: An Intrusion Detection System [Електронний ресурс]. – 1988. – URL: http://people.scs.carleton.ca/~soma/id/readings/smahahaystack.pdf
5. DES: An Intelligent System for Detecting Intruders [Електронний ресурс]. – 1990. – URL: https://www.researchgate.net/profile/Teresa-Lunt-2/publication/242383334_Ides_an_intelligent_system_for_detecting_intruders/links/552dacae0cf29b22c9c4f95f/Ides-an-intelligent-system-for-detecting-intruders.pdf.
6. Detection of Anomalous Computer Session Activity [Електронний ресурс]. – 1989. – URL: http://people.scs.carleton.ca/~soma/id2007w/readings/vaccaro-wisdom+sense.pdf.
7. Lunt, Teresa F., "Detecting Intruders in Computer Systems, 1993 Conference on Auditing and Computer Technology, SRI International. [Електронний ресурс]. – 1993. – URL: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.43.7289.
8. Adaptive Real-time Anomaly Detection Using Inductively Generated Sequential Patterns [Електронний ресурс] – 1990. – URL: https://ieeexplore.ieee.org/abstract/document/63857
9. A Network Security Monitor [Електронний ресурс]. – 1990. – URL: http://seclab.cs.ucdavis.edu/papers/pdfs/th-gd-90.pdf.
10. Gorbatov V. S., Zhurba A. O. Оптимізація обробки правил у Snort 3. 2024. URL: https://journals.nmetau.edu.ua/index.php/st/article/view/1693/993. Дата звернення 22.02.2026
11. Afrah Gueriani et al. Deep Reinforcement Learning for Intrusion Detection in IoT: A Survey. 2024. URL: https://arxiv.org/abs/2405.20038?utm_source=chatgpt.com. Дата звернення 22.02.2026.
12. Yasir Ali Farrukh et al. *XG-NID: Heterogeneous GNN and LLM for NIDS*. 2024. URL: https://arxiv.org/abs/2408.16021?utm_source=chatgpt.com. Дата звернення 22.02.2026.
13. Richard Kimanzi et al. *Deep Learning Algorithms Used in IDS — A Review*. 2024. URL: https://arxiv.org/abs/2402.17020?utm_source=chatgpt.com. Дата звернення 22.02.2026.
14. Шпур О. та ін. *Розробка моделі IDS та IPS із ML-методами*. 2024. URL: https://science.lpnu.ua/uk/ictee/vsi-vypusky/vypusk-4-nomer-2-2024/rozroblennya-modeli-systemy-vyyavlennya-ta-protydiyi?utm_source=chatgpt.com. Дата звернення 22.02.2026.

15. National Institute of Standards and Technology. Guide to Intrusion Detection and Prevention Systems (IDPS) (NIST SP 800-94). Gaithersburg: NIST, 2007. 127 p. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf?utm_source=chatgpt.com.
16. Система виявлення вторгнень [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Система_виявлення_вторгнень.
17. Риков О., Олешко І. Порівняльний аналіз систем виявлення і запобігання вторгнень. «GLOBAL CYBER SECURITY FORUM 2019» 14 – 16 листопада 2019, ХАРЬКІВ, Україна. URL: https://openarchive.nure.ua/server/api/core/bitstreams/381a4953-9306-4362-a6d1-e7199f2f425a/content.
18. Гавриленко С.Ю., Кісь А.А. Аналіз методів виявлень вторгнень у комп'ютерні мережі. *Проблеми інформатики та моделювання (ПІМ-2023), Харків, 2023*. С. 36-37.
URL: https://repository.kpi.kharkov.ua/server/api/core/bitstreams/b89ef021-c4e1-4b6f-a747-8d1adc2cf305/content.
19. Chichkarev, E.,Zinchenko, O., Bondarchuk, A., & Aseeva, L. (2023). Feature selection method for intrusion detection system using ensemble approach and fuzzy logic. Cybersecurity: Education, Science, Technology, 1(21), 234–251.
20. Damasevicius, R., Venckauskas, A., Grigaliunas, S., Toldinas, J., Morkevicius, N., Aleliunas, T., Smuikys, P. (2020). LITNET-2020: An annotated real-world network flow dataset for network intrusion detection. Electronics, 9(5), 800. https://doi.org/10.3390/electronics9050800.
21. Мєшков В.І., Віролайнен В.О. Аналіз сучасних систем виявлення та запобігання вторгнень в інформаційно-телекомунікаційних системах. URL: https://ela.kpi.ua/server/api/core/bitstreams/2fc5d863-fb1a-4334-a33d-ceee718222ff/content
22. Sen Sevil. Power-Aware Intrusion Detection in Mobile Ad Hoc Networks – 2006. – 20 p.
23. Коробейнікова Т., Цар О. Аналіз сучасних відкритих систем виявлення та запобігання вторгнень. – Grail of Science, (27), 2023. с. 317–325.
24. Толюпа С.В., Кулько А.А. «Нейро-нечітка системи виявлення вторгнень у інформаційну мережу критичної інфраструктури», Кібербезпека: освіта, наука, техніка, № 3 (27), с. 233-247, 2025.
25. Teresa F. Lunt. Detecting intruders in computer systems // Proceedings of the 1988 IEEE Symposium on Security and Privacy. – Oakland, CA, 1988. – P. 22–46.
26. Ross Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. – 2nd ed. – Indianapolis: Wiley Publishing, 2008. – 1080 p.
27. Tom M. Mitchell. Machine Learning. – New York : McGraw-Hill, 1997. – 414 p.
28. Y. Wu et al. Adaptive Exploration-Exploitation Tradeoff for the UCB Algorithm // IEEE Transactions on Neural Networks and Learning Systems. – 2018. – DOI: https://ieeexplore.ieee.org/document/8264962.
29. P. Auer, N. Cesa-Bianchi, P. Fischer. Finite-time analysis of the multiarmed bandit problem // Machine Learning. – 2002. – Vol. 47(2–3). – P. 235–256. – DOI: https://ieeexplore.ieee.org/document/5504793.
30. S. Bubeck, N. Cesa-Bianchi. Regret Analysis of Stochastic and Nonstochastic Multi-armed Bandit Problems // Foundations and Trends in Machine Learning. – 2012. – Vol. 5(1). – P. 1–122. – DOI: https://ieeexplore.ieee.org/document/7307098.

31. L. Lattimore, Cs. Szepesvári. Bandit Algorithms – 2020. – URL: https://ieeexplore.ieee.org/document/9179240.
32. Gama et al. (concept drift) A Survey on Concept Drift Adaptation ACM Computing Surveys, 2014/ 46.4: 1-37. URL: https://www.researchgate.net/publication/261961254_A_Survey_on_Concept_Drift_Adaptation.
33. Modi C. et al. A survey of intrusion detection techniques in cloud. Journal of Network and Computer Applications. 2013.
34. Sommer R., Paxson V. Outside the Closed World: On Using ML for Network Intrusion Detection. IEEE S&P. 2010.
35. Mukkamala S., Sung A. Intrusion Detection Using Neural Networks and Support Vector Machines. 2003.
36. Cesa-Bianchi N., Lugosi G. Prediction, Learning, and Games. Cambridge University Press, 2006.
37. Breiman L. Random Forests. Machine Learning. 2001.
38. Aggarwal C. Data Streams: Models and Algorithms. Springer, 2007.
39. Shukla H.D., Jaiswal B. Adaptive machine learning algorithms for intrusion detection system in cybersecurity. – Journal of Information Systems Engineering and Management. – 2024. – URL: https://www.jisem-journal.com/index.php/journal/article/view/11550 (дата звернення: 01.02.2026).
40. Ogunbadejo M. та ін. Machine learning methods for intrusion detection: A comprehensive survey. – IJSRM. – 2025. – URL: https://www.ijsrm.net/index.php/ijsrm/article/view/6535 (дата звернення: 01.02.2026).
41. Головко М. С. Адаптивне виявлення кібератак у системах IDS з використанням методу багаторуких бандитів. URL: https://ela.kpi.ua/server/api/core/bitstreams/8120b797-1bb4-4426-8ff3-896ce04b5d33/content.
42. U. Islam, A. Muhammad, R. Mansoor, M. S. Hossain, I. Ahmad, E. T. Eldin, J. A. Khan, A. U. Rehman, and M. Shafiq, “Detection of Distributed Denial of Service (DDoS) Attacks in IoT Based Monitoring System of Banking Sector Using Machine Learning Models,” Sustainability, vol. 14, no. 14, p. 8374, Jul. 2022, doi: 10.3390/su14148374.
43. Megantara, A. A., et al. (2021). A hybrid machine learning method for increasing the performance of network intrusion detection systems. Journal of Big Data. URL: https://journalofbigdata.springeropen.com/articles/10.1186/s40537-021-00531-w
44. Messaouda, B., et al. (2026). Hybrid IDS Using Signature-Based and Anomaly-Based Detection. *arXiv preprint*. https://arxiv.org/abs/2601.11998.
45. Goodfellow I., Bengio Y., Courville A. *Deep Learning*. – Cambridge : MIT Press, 2016. – 775 p. – Режим доступу: Deep Learning Book – Дата звернення: 24.03.2026.
46. Bishop C. M. *Pattern Recognition and Machine Learning*. – New York : Springer, 2006. – 738 p. – Режим доступу: Springer – Дата звернення: 24.03.2026.
47. *Framework for Improving Critical Infrastructure Cybersecurity*. – Gaithersburg : NIST, 2018. – 55 p. – Режим доступу: NIST Cybersecurity Framework – Дата звернення: 24.03.2026.
48. *ENISA Threat Landscape 2023*. Brussels: European Union Agency for Cybersecurity, 2023. – 120 p. – Режим доступу: ENISA Report – Дата звернення: 24.03.2026.

49. Artificial intelligence and machine learning in cybersecurity, Knowledge and Information Systems (2025).URL: https://link.springer.com/article/10.1007/s10115-025-02429-y.
50. Коробейнікова Т., Метод аналізу даних від систем IDS/IPS на основі комбінування сигнатур і політик, Herald of Khmelnytskyi National University (2025). URL: file:///C:/Users/User/Downloads/(351)+VKNU-TS-2025-N3-26.pdf.
51. Wang Y., et al., Hybrid Model for Novel Attack Detection Using a Cluster Based Machine Learning Classification Approach, Future Internet (2025). URL: https://www.mdpi.com/1999-5903/17/6/251?utm_source=chatgpt.com.
52. AI огляд у сучасних IDS/IPS системах, Knowledge and Information Systems (2025).
53. Springer. (2025). A systematic literature study of machine learning techniques based intrusion detection. Journal of Big Data. https://link.springer.com/article/10.1186/s40537-025-01323-2.
54. Perháč J., Novitzká V., Steingartner W., Bilanová Z. Formal model of IDS based on BDI logic // Mathematics. – 2021. – Vol. 9, № 18. – P. 2290.
55. Al-Fuqaha A., et al. Intrusion detection systems for IoT-based smart environments: a survey // Journal of Cloud Computing. – 2018.
56. Ahmim A., et al. A novel hierarchical intrusion detection system based on decision tree and rules-based models // arXiv. – 2018.
57. Sokolova, M., & Lapalme, G. (2009). A systematic analysis of performance measures for classification tasks. Information Processing & Management, 45(4), 427–437. URL: A systematic analysis of performance measures for classification tasks - ScienceDirect
58. Chicco, D., & Jurman, G. (2020). The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation. BMC Genomics, 21(1), URL: MCC advantages paper.
59. Fawcett T. An introduction to ROC analysis // *Pattern Recognition Letters*. – 2006. – Vol. 27, № 8. – P. 861–874. – Режим доступу: https://www.sciencedirect.com/science/article/abs/pii/S016786550500303X?utm_source=chatgpt.com
60. Boutassetta M. et al. Hybrid IDS Using Signature-Based and Anomaly-Based Detection (Survey and Conceptual Model), 2026. URL: https://www.researchgate.net/publication/399931383_Hybrid_IDS_Using_Signature-Based_and_Anomaly-Based_Detection.
61. Xu, R., & Wunsch, D. (2005) Survey of clustering algorithms. IEEE Transactions on Neural Networks, 16(3), 645–678. https://doi.org/10.1109/TNN.2005.845141.
62. Шевченко С., Жданова Ю., Спасітєлєва С., Мазур Н., Складанний П., Негоденко В. Математичні методи в кібербезпеці: кластерний аналіз та його застосування в інформаційній та кібернетичній безпеці. Кібербезпека: освіта, наука, техніка, 3 (23), с. 258-273, 2024. URL: file:///C:/Users/User/Downloads/%D0%9A%D0%86%D0%91%D0%95%D0%A0%D0%91%D0%95%D0%97%D0%9F%D0%95%D0%9A%D0%90_2024_last+(1)-258-273.pdf.
63. K-Means Clustering Algorithm - Javatpoint [Електронний ресурс] //www.javatpoint.com. – Режим доступу: https://www.javatpoint.com/k-meansclustering-algorithm-in-machine-learning.

64. 2014 SIGKDD TEST OF TIME AWARD, 2014. https://www.kdd.org/news/view/2014-sigkdd-test-of-time-award
2.M. Ester, H-P. Kriegel, J. Sander, X. Xu. A density-based algorithm for discovering clusters in large spatial databases with noise // Proceedings of the Second International Conference on Knowledge Discovery and Data Mining (KDD-96) /Evangelos Simoudis, Jiawei Han, Usama M. Fayyad. - AAAI Press.
65. Shafronenko, A., Bodyanskiy, Y., & Rudenko, D. (2020). Neuro-fuzzy clustering of Distorted Data Using Cat Swarm Optimization. LAP LAMBERT Academic Publishing.
66. Головня С.А., Марчук Г.В. Кластерний аналіз: ієрархічна кластеризація. URL: https://conf.ztu.edu.ua/wp-content/uploads/2019/12/58-1.pdf.
67. Adaptive and online network intrusion detection system using clustering and Extreme Learning Machines // Journal of the Franklin Institute. – 2018. – DOI: 10.1016/j.jfranklin.2017.06.006. – Режим доступу: https://www.sciencedirect.com/science/article/pii/S0016003217302995 (дата звернення: 24.03.2026).
68. Scarfone K, Mell P. Guide to intrusion detection and prevention systems (IDPS). NIST special publication, 2007, 800(2007): 94. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf.
69. Otoum, Y., Nayak, A. AS-IDS: Anomaly and Signature Based Intrusion Detection System for IoT. Journal of Network and Systems Management, 2021. URL: https://doi.org/10.1007/s10922-021-09589-6.
70. MLflow Contributors. *MLflow*. — URL: https://mlflow.org/
71. Kubeflow Authors. *Kubeflow: Machine Learning Toolkit for Kubernetes*. – URL: https://www.kubeflow.org/
72. Chandola, V., Banerjee, A. & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, Vol. 41, Issue 3. Article No: 15, pp. 1-58. URL: https://doi.org/10.1145/1541880.1541882.
73. Al-Yaseen, W. L., Othman, Z. A., Nazri, M. Z. A. Hybrid Modified K-Means with C4.5 for Intrusion Detection Systems in Multiagent Systems. The Scientific World Journal, 2015. URL: https://doi.org/10.1155/2015/294761.
74. Stallings W. Network Security Essentials: Applications and Standards. – Pearson, 2020. URL: https://www.emgywomenscollege.ac.in/templateEditor/kcfinder/upload/files/Network-security-essentials.pdf.
75. Scarfone, K, & Mell, P. (2007, Feb.). Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication on Computer security, pp. 58–69.
76. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. Pearson Education, 2021. URL: https://ebooks.karbust.me/Technology/Computer%20Networking%20A%20Top-Down%20Approach,%208th%20Edition%20by%20James%20F.%20Kurose,%20Keith%20W.%20Ross-Pearson-9780136681557.pdf
77. Bejtlich R. The Practice of Network Security Monitoring. Michigan: No Starch Press, 2013. 465 c.
78. Sanders C., Smith J. Applied Network Security Monitoring. — Syngress, 2013. 496 c.
79. Singer P., Friedman A. Cybersecurity and Cyberwar: What Everyone Needs to Know. — Oxford University Press, 2014. 320 c.

80. Міщеряков А. Ю. Адміністрування та захист систем на базі ядра Linux, 2020. URL: https://openarchive.nure.ua/bitstreams/c896eb4e-b241-4f00-abee-10067476357c/download
81. Garcia Cordero C., Vasilomanolakis E., Wainakh A. et al. On generating network traffic datasets with synthetic attacks for intrusion detection. 2019. URL: file:///C:/Users/User/Downloads/OnGeneratingNetworkTrafficDatasetswithSyntheticAttacksforIntrusionDetection.pdf.
82. Що таке перехоплення пакетів? URL: https://nym.com/uk/blog/%D1%89%D0%BE-%D1%82%D0%B0%D0%BA%D0%B5-%D0%BF%D0%B5%D1%80%D0%B5%D1%85%D0%BE%D0%BF%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F-%D0%BF%D0%B0%D0%BA%D0%B5%D1%82%D1%96%D0%B2
83. Georgia Weidman «Penetration testing». Attacks. Розділ – 3, с.339.
84. Mumtaz M.Ali AL-Mukhtar. A Protocol Analyzer Using a Sockets Based Network Sniffer. Australian Journal of Basic and Applied Sciences. URL: http://www.ajbasweb.com/old/ajbas/2010/1632-1640.pdf. c.1634-1639.
85. Han J., Kamber M., Pei J. Data Mining: Concepts and Techniques. Morgan Kaufmann, 2011. – 744 с.
86. Bishop C. Pattern Recognition and Machine Learning. Springer, 2006. – 740 с.
87. Pekár A., Plný R., Hynek K. Tutorial on Flow-Based Network Traffic Classification Using Machine Learning. 2026. URL: https://www.researchgate.net/publication/399559247_Tutorial_on_Flow-Based_Network_Traffic_Classification_Using_Machine_Learning.
88. Messaoud M. Classification of Network Traffic Using Machine Learning Models on the NetML Dataset. 2025. URL: https://aircconline.com/ijcnc/V17N3/17325cnc07.pdf
89. Мєшков В. І. Методи машинного навчання для бінарної та багатокласової класифікації мережевого трафіку у системах виявлення атак. – Таврійський науковий вісник № 4, частина 1. – С. 182-196.
90. Горносталь О. А. Класифікація мережевих атак методами машинного навчання. Control, Navigation and Communication Systems. 2025. No. 32025.URL: https://repository.kpi.kharkov.ua/server/api/core/bitstreams/60de30c8-6c2d-41da-9ff6-df826a264101/content.
91. Scikit-learn: Cross-validation and model evaluation [Електронний ресурс]. – Режим доступу: https://scikit-learn.org/stable/modules/cross_validation.html.
92. Goodfellow I., Bengio Y., Courville A. Deep Learning [Електронний ресурс]. – Cambridge : MIT Press, 2016. – Режим доступу: https://www.deeplearningbook.org.

Метадані

ДОКУМЕНТ

Заголовок
КБР_Паранін І.Е.

Автор
Паранін І.Е.

Науковий керівник / Експерт
Кулініч О.М.

ІД документу
334235340

ОРГАНІЗАЦІЯ

Назва організації
Kyiv National Economic University named after Vadym Hetman KNEU

підрозділ
кафедра системного аналізу та кібербезпеки

ЗВІТ

Дата звіту
6/9/2026

Дата редагування

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.

12.92% 12.92% КП 1

8.83% 8.83% КП 2

0.35% 0.35% КЦ

25
Довжина фрази для коефіцієнта подібності 2

19388
Кількість слів

156222
Кількість символів

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв	ß	9
Інтервали	A→	0
Мікропробіли	·	5
Білі знаки	ß	0
Парафрази (SmartMarks)	a	90

Джерела

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз — Колір тексту

#	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)

1	2023_Б_ІНФ_ІТІНФ-19-2_Авлякулов_Т_Е [redacted] 5/30/2024 Kharkiv National University of Radio Electronics (Kharkiv National University of Radio Electronics)	361 (1.86 %)
2	http://eprints.zu.edu.ua/id/eprint/30511/contents	148 (0.76 %)
3	https://journals.duikt.edu.ua/index.php/dataprotect/article/download/3061/2950/	118 (0.61 %)
4	Створення системи виявлення вторгнень на основі архітектури штучної імунної системи [redacted] 12/19/2023 Ternopil Ivan Pul'uj National Technical University (кафедра кібербезпеки)	77 (0.4 %)
5	Спосіб кластерного аналізу [redacted] 3/15/2025 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute)	74 (0.38 %)
6	Климаш, Бальковський, Шпур (версія 3) [redacted] 4/17/2025 National University "Lviv Politechnika" (NULP2)	60 (0.31 %)
7	Методи глибинного навчання для конструювання ознакового простору та кластеризації кібератак [redacted] 3/15/2025 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute)	59 (0.3 %)
8	https://conf.ztu.edu.ua/wp-content/uploads/2019/12/tezy-dopovidej-kt2019_os.pdf	59 (0.3 %)
9	https://openarchive.nure.ua/bitstream/document/10522/1/GCS_FORUM_2019.pdf	57 (0.29 %)
10	Впровадження систем виявлення вторгнень атак на основі SURICAT [redacted] 6/10/2022 State University of Telecommunications (ННІЗІ)	56 (0.29 %)

База даних RefBooks (0.05 %)

#	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
джерело: Paperity		
1	Application of convolutional neural network for classification of ophthalmic diseases by fundus images Шегера Андрій, Ольга Величко, Олег Дацок;	10 (1) (0.05 %)

Домашня база даних (0.11 %)

#	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
2	КБР_Пяничук О.В. [redacted] 6/19/2025 Kyiv National Economic University named after Vadym Hetman KNEU (кафедра системного аналізу та кібербезпеки)	22 (2) (0.11 %)

Програма обміну базами даних (7.44 %)

#	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)

3	2023_Б_ІНФ_ІТІНФ-19-2_Авлякулов_Т_Е [redacted] 5/30/2024 **Kharkiv National University of Radio Electronics (Kharkiv National University of Radio Electronics)**	**361 (1) (1.86 %)**
4	Спосіб кластерного аналізу [redacted] 3/15/2025 **National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute)**	**326 (11) (1.68 %)**
5	Holovko_Bakalavr [redacted] 6/17/2025 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (ФТІ, К-ра інформаційної безпеки)	160 (15) (0.83 %)
6	Впровадження систем виявлення вторгнень атак на основі SURICAT [redacted] 6/10/2022 **State University of Telecommunications (HHI3I)**	**87 (2) (0.45 %)**
7	Методи глибинного навчання для конструювання ознакового простору та кластеризації кібератак [redacted] 3/15/2025 **National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute)**	**78 (3) (0.4 %)**
8	Програмний комплекс захисту мережевого периметру інформаційно-комунікаційної системи підприємства [redacted] 6/15/2021 **Sumy State University (Кафедра інформаційних технологій)**	**77 (3) (0.4 %)**
9	Створення системи виявлення вторгнень на основі архітектури штучної імунної системи [redacted] 12/19/2023 **Ternopil Ivan Pul'uj National Technical University (кафедра кібербезпеки)**	**77 (1) (0.4 %)**
10	Метод оцінки систем виявлення вторгнень [redacted] 3/15/2025 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute)	65 (6) (0.34 %)
11	Климаш, Бальковський, Шпур (версія 3) [redacted] 4/17/2025 **National University "Lviv Politechnika" (NULP2)**	**60 (1) (0.31 %)**
12	Кваліфікаційна_робота_Михайловський_Антон [redacted] 7/10/2024 **Ukrainian national aviation university (Ukrainian national aviation university)**	**59 (3) (0.3 %)**
13	Система виявлення вторгнень у мережі [redacted] 3/16/2025 **National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute)**	**58 (3) (0.3 %)**
14	ФКНТ_2025_125-24-1-СК_Кебкал Н.О. (1) [redacted] 12/17/2025 Ukrainian national aviation university (ФКНТ Кафедра технічного захисту інформації)	15 (3) (0.08 %)
15	Порівняльний аналіз підходів підвищення ефективності систем виявлення вторгнень [redacted] 12/21/2025 Ternopil Ivan Pul'uj National Technical University (кафедра кібербезпеки)	8 (1) (0.04 %)
16	Антоник Анастасії КНУС-22.docx [redacted] 12/20/2022 National University "Lviv Politechnika" (NULP2)	7 (1) (0.04 %)

17	МКР Купец Дмитро [redacted] 5/24/2026 National University "Lviv Politechnika" (NULP2)	5 (1) (0.03 %)

Інтернет (5.31 %)

#	ДЖЕРЕЛО URL	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
18	**http://eprints.zu.edu.ua/id/eprint/30511/contents**	**240 (3) (1.24 %)**
19	**https://journals.duikt.edu.ua/index.php/dataprotect/article/download/3061/2950/**	**146 (4) (0.75 %)**
20	http://ir.nmu.org.ua/bitstream/handle/123456789/151303/%D0%9C%D0%BE%D1%85%D0%BD%D1%96%D0%BD.pdf?sequence=1&isAllowed=y	118 (10) (0.61 %)
21	**https://www.ua-referat.com/uploaded/nacionalenij-tehnichnij-universitet-ukrayini/index5.html**	**96 (4) (0.5 %)**
22	**https://conf.ztu.edu.ua/wp-content/uploads/2019/12/tezy-dopovidej-kt2019_os.pdf**	**87 (3) (0.45 %)**
23	**https://csecurity.kubg.edu.ua/index.php/journal/article/download/568/454/1929**	**74 (2) (0.38 %)**
24	**https://openarchive.nure.ua/bitstream/document/10522/1/GCS_FORUM_2019.pdf**	**71 (2) (0.37 %)**
25	https://dspace.znu.edu.ua/jspui/bitstream/12345/12489/1/Kaminskiy_D_U.pdf	61 (4) (0.31 %)
26	**http://dspace.wunu.edu.ua/bitstream/316497/46657/1/%D0%93%D0%B0%D0%B2%D1%80%D0%B8%D0%BB%D1%8F%D0%BA.pdf**	**55 (2) (0.28 %)**
27	**https://calvarybaptisthsv.org/w/ids**	**39 (2) (0.2 %)**
28	https://www.h-x.technology/ua/blog-ua/trends-cyber-challenges-solutions-2024-ua	15 (2) (0.08 %)
29	https://duikt.edu.ua/repozitorii/ikb/2024/bak/%D0%94%D0%B8%D0%BF%D0%BB%D0%BE%D0%BC_%D0%91%D0%A1%D0%94-41_%D0%92%D0%B0%D1%81%D0%B8%D0%BB%D0%B5%D0%BD%D0%BA%D0%BE%D0%AF%D0%9E_PDF.pdf	12 (1) (0.06 %)
30	https://openarchive.nure.ua/server/api/core/bitstreams/8c31039b-6878-43a6-a54d-e38a69880896/content	10 (1) (0.05 %)
31	https://dut.edu.ua/repozitorii/sikz/2023/%D0%94%D0%B8%D0%BF%D0%BB%D0%BE%D0%BC%D0%9E%D0%B3%D0%BD%D1%94%D0%B2.pdf	6 (1) (0.03 %)

Список прийнятих фрагментів

#	ЗМІСТ	КІЛЬКІСТЬ ОДНАКОВИХ СЛІВ (ФРАГМЕНТІВ)