DOI: 10.18372/2310-5461.67.20036
УДК 004.056.53:681.3.06 (045)

В. А Стороженко,
Державний університет «Київський авіаційний інститут», Київ
orcid.org/0009-0007-3210-2174
E-mail: 6920103@stud.kai.edu.ua;

Б. А. Дем'янчук,
Державний університет «Київський авіаційний інститут», Київ
orcid.org/0009-0009-3731-9764
E-mail: 6915495@stud.kai.edu.ua;

Д. В. Козловська,
Державний університет «Київський авіаційний інститут», Київ
orcid.org/0009-0004-6223-0319
E-mail: 8542876@stud.kai.edu.ua;

А. О. Фесенко
Державний університет «Київський авіаційний інститут», Київ
orcid.org/0000-0001-5154-5324
E-mail: andrii.fesenko@npp.kai.edu.ua

ОГЛЯД МОЖЛИВОСТЕЙ IDS ДЛЯ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ

Вступ

У сучасних умовах кібербезпеки загрози інформаційним системам постійно еволюціонують, що вимагає вдосконалення механізмів їхнього виявлення та протидії. Зростаюча складність атак та їхня спрямованість на критичну інфраструктуру потребують адаптивних методів аналізу мережевого трафіку та моніторингу загроз.

Традиційні системи виявлення вторгнень (IDS) та засоби кореляції подій (SIEM) забезпечують базовий рівень захисту, однак їхня ефективність може знижуватися через велику кількість помилкових спрацьовувань та обмежену здатність розпізнавати нові типи атак.

Фахівці та дослідники постійно працюють над створенням ефективних систем кіберзахисту, які забезпечують конфіденційність, цілісність та доступність інформації, захищаючи комп'ютерні мережі від хакерських атак.

Аналіз досліджень і публікацій

У цьому розділі ми висвітлимо деякі дослідження, виконані науковою спільнотою для розвитку галузі виявлення вторгнень.

Кілька досліджень систем виявлення вторгнень були проведені фахівцями з кібербезпеки. Зокрема, S. Smys та ін. [1] запропонували IDS для виявлення вторгнень в IoT-мережах на основі гібридної нейронної мережі. За словами автора, його система може давати задовільні результати у високовимірних IoT-мережах. Sydney та ін. [2] запропонували метод на основі глибинного навчання для розробки бездротової IDS. Автор використав Wrapper Based Feature Extraction Unit (WFEU) для зменшення розмірності датасетів UNSW-NB15 та AWID. Hadeel Alazzam та ін. [3] запропонували метод на основі алгоритму Pigeon Inspired Optimizer для зменшення розмірності датасету, зберігаючи лише найбільш релевантні ознаки. Оцінювання їхнього підходу було проведено на датасетах KDDCUP99, NLS-KDD та UNSW-NB15. Ferrag та ін. [4] запропонували IDS під назвою Rules and Decision Tree-based Intrusion Detection System (RDTIDS) для виявлення вторгнень, що можуть бути спрямовані на IoT-мережі. Його підхід поєднує різні класифікаційні техніки: Decision Tree, JRip algorithm, Forest PA та REP Tree. Kumar та ін. [5] запропонували сигнатурну IDS, здатну виявляти п'ять категорій мережевого трафіку: Exploit, Probe, Generic, DOS та Normal. Запропонована система діє як «сторожовий пес», що здатен контролювати мережу від підозрілої активності. Автор використав датасет UNSW-NB15 та згенерував власний тестовий датасет під назвою Real-Time dataset у лабораторії NIT Patna CSE (RTNITP18). S. Jin та ін. [6] запропонували легку сигнатурну IDS, здатну виявляти вторгнення, спрямовані на In-Vehicle Controller Area Network Bus Network. Дослідження підтверджує, що цей тип мереж усе ще не має достатніх механізмів захисту від кіберзлочинності і потребує максимально легкої IDS, оскільки такі мережі відомі обмеженими обчислювальними ресурсами. A. N. Cahyo та ін. [7]

підтвердили, що гібридні NIDS, запропоновані науковою спільнотою, ще не досягли зрілості й потребують вдосконалення для практичного використання в реальних мережах. Відтак дослідник здійснив огляд літератури щодо гібридних NIDS за останні п'ять років, представляючи різні архітектури, що були запропоновані.

H. Gajjar та ін. [8] обрали аналіз і порівняння різних підходів, які ґрунтуються на приватній хмарі OpenStack для виявлення вторгнень на основі сигнатурного або аномалійного аналізу. Dinesh Goyal та ін. [9] запропонували рішення для зменшення кількості хибних тривог, які генеруються NIDS на основі виявлення аномалій. Автор розробив IDS, що ґрунтується на виявленні аномалій і здатна виявляти вторгнення з нижчим рівнем хибних спрацювань. Для досягнення цього дослідник зосередився на трьох основних компонентах: компоненті попередньої обробки, рушії детекції та модулі обробки тривог. Said OUIAZZANE та ін. [10] запропонували NIDS для виявлення вторгнень, які можуть бути спрямовані на мережі БПЛА. Автор використав мультиагентні системи та методи машинного навчання для моделювання NIDS. Відтак було застосовано й оцінено набір методів класифікації для вибору найбільш надійного. Автор роботи [11] запропонував механізм виявлення вторгнень у мережах, що генерують великі обсяги даних. Дослідник поєднав використання двох класифікаційних технік – Long Short-Term Memory (LSTM) та Convolutional Neural Network (CNN). Крім того, автор застосував балансування датасету CIDDS-001 для зменшення впливу дисбалансу даних на результати класифікації. За словами дослідника, результати виявилися переконливими як для багатокласової класифікації (99,83 % точності), так і для бінарної класифікації (99,17 % точності)

Наукова спільнота справді почала зосереджуватися на різних типах NIDS, і дослідники постійно пропонують нові підходи для підвищення ефективності. Проте сфера виявлення вторгнень ще не досягла зрілості й потребує додаткових зусиль для створення більш ефективних і продуктивних NIDS.

Швидкий розвиток кіберзлочинності через появу нових, більш складних і цілеспрямованих атак «0-day» ставить під загрозу безпеку мереж як малих, так і великих компаній. Крім того, традиційні механізми безпеки вже не здатні захистити мережі від сучасних кібератак, оскільки вони здебільшого базуються на відомих сигнатурах атак, розроблених експертами.

Більшість підходів, запропонованих у літературі, є незадовільними та охоплюють дуже обмежені проблеми. З одного боку, кілька дослідників зосередилися лише на механізмах сигнатурного виявлення. Проте класичні SNIDS більше не здатні ефективно виявляти невідомі атаки «0-day». Крім того, SNIDS більше не можуть гарантувати безпеку сучасних комп'ютерних мереж і потребують частих оновлень сигнатур для нових атак. З іншого боку, більшість досліджень намагалася вдосконалити механізми виявлення, які застосовуються ADNIDS, пропонуючи високоефективні методи класифікації на основі алгоритмів машинного та глибинного навчання. Однак ADNIDS генерують дуже високий рівень хибних спрацювань, що ускладнює видимість адміністраторів щодо безпеки їхньої IT-інфраструктури. До того ж, небагато досліджень запропонували гібридні підходи, які поєднують обидва типи NIDS (SNIDS та ADNIDS). Водночас підходи на основі гібридного виявлення зосереджуються лише на класифікаційних техніках і не враховують архітектурний аспект запропонованих NIDS, що заважає повному розумінню моделей.

У нашій теперішній науковій роботі ми пропонуємо просту й ефективну архітектуру для виявлення як відомих, так і невідомих атак. Наша модель ґрунтується на поєднанні двох механізмів виявлення: SNIDS та ADNIDS. SNIDS у нашій моделі здійснює первинну фільтрацію для виявлення відомих атак, сигнатури яких уже відомі експертам, тоді як ADNIDS використовується для виявлення відхилень від базової поведінки мережі. Базова поведінка мережі полягає у формуванні еталонного профілю роботи мережі за нормальних умов, у відсутності будь-яких слідів кібератак.

Постановка проблеми

У сучасних умовах стрімкого розвитку цифрових технологій та зростання обсягів мережевого трафіку питання забезпечення ефективного моніторингу та захисту інформаційних систем набуває особливої актуальності. Традиційні засоби безпеки, що базуються на периметровому захисті та статичних правилах фільтрації, не здатні своєчасно реагувати на складні та динамічні кіберзагрози, зокрема атаки типу «zero-day» та багаторівневі APT-атаки.

Системи виявлення вторгнень (IDS) відіграють ключову роль у виявленні аномальної активності в мережі, однак їх ефективність часто обмежується низкою проблем:

– сигнатурні методи не здатні виявляти нові або модифіковані загрози без попереднього оновлення баз даних;

– аномалійні підходи генерують велику кількість хибних спрацювань, що ускладнює оперативне реагування;

– обробка великих обсягів трафіку в реальному часі потребує високої продуктивності та масштабованості систем;

– нові архітектури, такі як мікросервіси, контейнеризація та edge-обчислення, вимагають адаптації IDS до динамічних середовищ.

У цьому контексті постає необхідність комплексного огляду сучасних IDS-рішень, їхніх технічних можливостей, підходів до аналізу трафіку та здатності інтегруватися в гетерогенні інфраструктури. Такий огляд дозволяє визначити перспективні напрямки розвитку систем виявлення вторгнень та сформувати рекомендації щодо побудови ефективних багаторівневих моделей захисту.

Кілька досліджень систем виявлення вторгнень були проведені фахівцями з кібербезпеки. Зокрема, S. Smys та ін. [1] запропонували IDS для виявлення вторгнень в IoT-мережах на основі гібридної нейронної мережі. За словами автора, його система може

Метою статті є проведення комплексного аналізу сучасних систем виявлення вторгнень (IDS) для аналізу мережевого трафіку, дослідження їхніх можливостей, переваг та обмежень у контексті забезпечення кібербезпеки. Особливу увагу приділено порівнянню відкритих та комерційних рішень, оцінці їх ефективності при виявленні актуальних мережевих атак, а також визначенню перспективних напрямів розвитку IDS, зокрема інтеграції з технологіями машинного навчання та гібридними архітектурами.

Основна частина

Системи IDS забезпечують конфіденційність, цілісність та доступність інформації, захищаючи комп'ютери та мережі від хакерських атак[1]. Традиційні рішення у сфері кібербезпеки протидіють широкому спектру цифрових загроз, серед яких віруси, трояни, черв'яки, спам та ботнети. Захист реалізується на двох ключових рівнях: мережевому та локальному. На рівні мережі здійснюється моніторинг інформаційних потоків із застосуванням мережевих фаєрволів, фільтрів спаму, антивірусного програмного забезпечення та інструментів виявлення вторгнень. На рівні кінцевих пристроїв забезпечується контроль вхідних даних за допомогою локальних засобів захисту: брандмауерів, антивірусних програм та механізмів детектування вторгнень, інстальованих безпосередньо на робочих станціях[2]. Приклад такої системи зображено на рис. 1

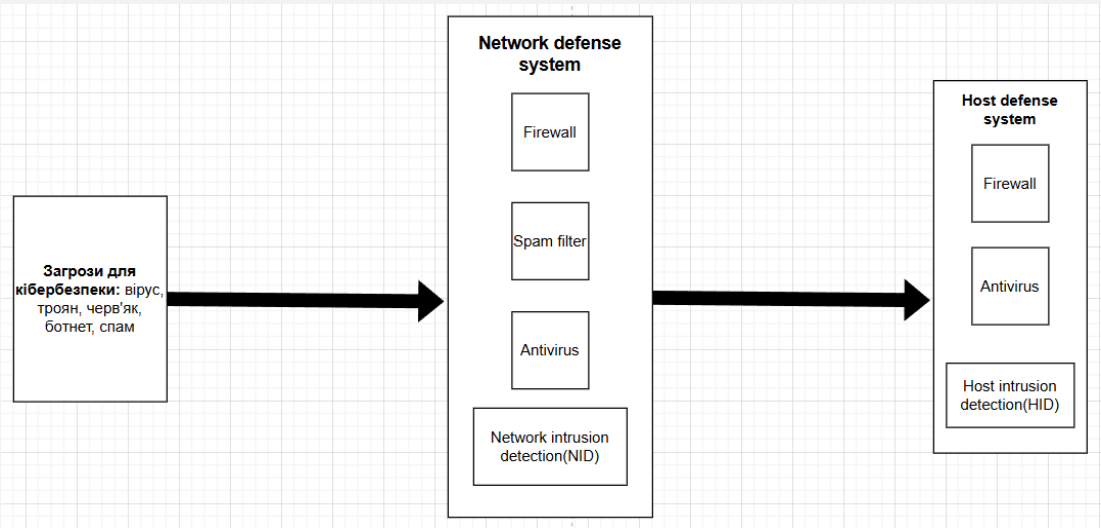

Рис. 1. Типова архітектура системи кіберзахисту

На обох рівнях безпеки впроваджено додатковий рівень захисту у вигляді мережевих систем виявлення вторгнень (NIDS) [3] та систем виявлення вторгнень на рівні хостів (HIDS), які є основними різновидами Intrusion Detection System (IDS). Основним завданням IDS є ідентифікація загроз та інформування адміністраторів безпеки про потенційні інциденти, такі як несанкціонований доступ, зараження шкідливим програмним забезпеченням або підозріла активність у мережевому трафіку. Аналізуючи пакети даних, журнали подій, активність системи та поведінкові патерни, IDS допомагає виявляти загрози безпеці та оперативно реагувати на них у реальному часі.

Серед найбільш популярних IDS-систем на сьогодні можна виділити наступні (табл. 1):

1. Zeek (раніше Bro) – потужний інструмент для аналізу мережевого трафіку, що поєднує сигнатурний та поведінковий аналіз. Відмінною особливістю Zeek є глибокий аналіз протоколів і подій, що дозволяє виявляти невідомі загрози та складні атаки, які неможливо ідентифікувати виключно на основі сигнатур [4].

2. Snort – одна з найвідоміших відкритих IDS-систем, яка використовує правила сигнатурного аналізу, що описують характерні ознаки відомих атак. Snort також підтримує модулі аналізу аномалій, що розширює її можливості у виявленні загроз, які не мають чітких сигнатур [5].

3. Suricata – високопродуктивна IDS/IPS-система, розроблена Open Information Security Foundation (OISF). Вона підтримує багатопотокову обробку трафіку, що робить її ефективною для великих корпоративних мереж. Suricata використовує глибокий аналіз пакетів (DPI) та механізм контекстного розпізнавання мережевих протоколів, що підвищує точність виявлення загроз [6].

4. Security Onion – це комплексне рішення, що об'єднує різні інструменти для моніторингу мережевої безпеки, аналізу журналів та розслідування інцидентів. Завдяки інтеграції з такими системами, як Zeek, Snort та Suricata, Security Onion забезпечує багаторівневий аналіз загроз та централізований контроль безпеки [7].

5. Wazuh – це агентська система виявлення вторгнень (HIDS), що базується на OSSEC. Вона спеціалізується на аналізі логів, контролі цілісності файлів, виявленні руткітів та поведінковому моніторингу активності системи. Wazuh також має можливість інтеграції з Elastic Stack, що дозволяє реалізувати функціональність SIEM-системи для кореляції подій та глибокого аналізу загроз [8].

6. Cisco Secure IDS – комерційне рішення від компанії Cisco, яке використовує аналіз трафіку на основі сигнатур та поведінкових моделей. Це рішення добре інтегрується з іншими продуктами Cisco, що дозволяє ефективно контролювати мережеву інфраструктуру та автоматизувати реагування на інциденти [9].

7. IBM QRadar – це потужна SIEM-платформа, яка включає вбудовані функції IDS для аналізу загроз. QRadar проводить кореляцію подій з різних джерел, застосовуючи методи поведінкового аналізу та машинного навчання. Це рішення використовується для моніторингу складних корпоративних мереж та аналізу кіберзагроз у режимі реального часу [10].

Таблиця 1

Порівняння різних IDS систем

Система	Переваги	Недоліки
Zeek	– висока масштабованість завдяки розподіленій обробці трафіку; – висока розширюваність через використання скриптової мови (можливість створення власних правил); – підтримка детального аналізу поведінки – безкоштовна	– складне налаштування через необхідність знання скриптової мови – вимагає великої обчислювальної потужності при аналізі об'ємного трафіку
Suricata	– висока продуктивність завдяки багатопотоковості та апаратному прискоренню; – гнучкість завдяки підтримці правил Snort та Lua-скриптів; – вбудована підтримка протоколів високого рівня; – безкоштовна	– певна складність налаштування через велику кількість конфігурацій; – вимагає оптимізації правил для зменшення спрацьовувань false positive
Security Onion	– гібридна платформа, що об'єднує можливості різних інструментів (Zeek, Snort, Suricata, Wazuh); – висока масштабованість для моніторингу великих мереж; – безкоштовна та активно підтримується спільнотою	– складне налаштування через велику кількість конфігурацій; – потребує значних ресурсів для ефективного функціонування
Wazuh	– висока масштабованість завдяки підтримці агентів на багатьох пристроях; – інтеграція з Elastic Stack для централізованого аналізу безпеки(фактично SIEM-система); – автоматизований аналіз подій; – безкоштовна та активно підтримується спільнотою	– вимагає встановлення агентів на кожен пристрій, що може ускладнити адміністрування; – необхідність додаткових налаштувань для ефективного виявлення загроз

Закінчення табл. 1

Система	Переваги	Недоліки
Cisco Secure IDS	– висока продуктивність, оскільки оптимізоване для обладнання Cisco; – глибока інтеграція з іншими продуктами Cisco; – професійна технічна підтримка; – висока точність виявлення загроз	– висока вартість ліцензій та необхідність використання Cisco–обладнання; – менш гнучка розширюваність через закриту екосистему Cisco
IBM QRadar	– висока масштабованість, підходить для великих підприємств; – використання AI для кореляції подій та аналітики загроз; – потужні можливості інтеграції з іншими системами; – підтримка SIEM–функцій; – частково безкоштовна	– висока вартість ліцензій та супроводу; – вимагає високого рівня експертних знань для налаштування та ефективного використання
Snort	– безкоштовна; – гнучка конфігурація через можливість створення та редагування правил; – спільнота користувачів та підтримка; – широке використання в мережах різного масштабу	– помірна масштабованість (потребує оптимізації при великих навантаженнях) – вимагає оптимізації правил для зменшення спрацьовувань false positive

Експериментальна частина дослідження передбачає тестування функціоналу SIEM-системи Security Onion, що інтегрує такі компоненти: Suricata (IDS/IPS), Zeek (мережевий аналізатор), ELSA (лог-менеджмент) та Squil (кореляція подій). Вибір саме цієї системи зумовлений її відкритою архітектурою та можливістю розгортання повноцінного середовища для виявлення та аналізу загроз. Security Onion поєднує в собі провідні інструменти інформаційної безпеки в одному дистрибутиві, що забезпечує зручність інтеграції, масштабованість та ефективність проведення досліджень. Основна увага у рамках тестування приділяється компоненту Suricata, оскільки він забезпечує високу швидкість і точність виявлення атак, підтримує багатопотокову обробку трафіку, має гнучкий механізм роботи з правилами виявлення та підтримує сучасні мережеві протоколи. Крім того, сумісність Suricata з правилами Snort дає змогу використовувати вже існуючі бази сигнатур без необхідності їх доопрацювання. Такий підхід дозволяє більш глибоко проаналізувати ефективність функціонування системи в умовах, наближених до реального мережевого середовища. У межах Security Onion використання Suricata є доцільним з огляду на її гнучкість налаштувань, високу продуктивність і можливість інтеграції з іншими аналітичними модулями платформи. Основні об'єкти дослідження:

- Робота модуля виявлення вторгнень Suricata
- Ефективність комплексного рішення Security Onion як платформи моніторингу безпеки

1. Технічні характеристики тестування:

Таблиця 2

Технічні характеристики тестування

Апаратне забезпечення	Процесор: Intel Core i5–9500T; ОЗУ: 32 ГБ;Мережевий адаптер: 1 Gbps
Тип платформи	Ubuntu Server 24.04
Програмне забезпечення	Security Onion на основі Ubuntu Server 24.04
Методика тестування	Генерація трафіку за допомогою Scapy та датасетів (CIC–IDS2017, UNSW–NB15); Емуляція атак: DDoS, SQL–ін'єкції, сканування портів

2. Конфігурація Suricata

Конфігурація Suricata базувалася на двох рівнях правил детекції:

- *Стандартні правила* (ET Open Ruleset) – забезпечують покриття типових векторів атак з високою точністю виявлення
- *Спеціалізовані правила* – розроблені експериментальні шаблони для:

1) Тестування адаптивності системи до нових загроз.

2) Оцінки роботи з аномальними мережевими паттернами.

3) Вимірювання продуктивності при обробці складних поліморфних атак.

4) Використані набори даних.

Для оцінки точності виявлення загроз та мінімізації помилкових спрацьовувань було застосовано такі набори даних:

- KDD Cup 1999 [11].

Один з перших і найбільш відомих наборів даних для завдань виявлення вторгнень. Містить численні приклади мережевих атак, зокрема DoS та зондувальних атак (probe). Через застарілість даних використовувався лише для базового тестування.

- NSL–KDD [12].

Вдосконалена версія KDD Cup 1999, в якій усунено дублюючі записи та забезпечено збалансованіший розподіл класів атак. Цей набір даних дозволяє отримати більш репрезентативні результати тестування.

• CIC–IDS2017 [13].

Сучасний набір даних, створений на основі реального мережевого трафіку. Включає актуальні типи атак, такі як DDoS, ботнети та фішинг, що робить його особливо корисним для оцінки ефективності сучасних систем виявлення вторгнень.

• UNSW–NB15 [14].

Набір даних, який охоплює широкий спектр сучасних атак та відрізняється більш різноманітним мережевим трафіком порівняно з KDD Cup 1999. Це дозволяє провести більш глибокий аналіз здатності системи до виявлення складних та нових загроз.

5) Результати дослідження

• Проведене тестування виявило високий рівень ефективності системи Suricata у протидії сучасним мережевим загрозам (табл. 3). Аналіз отриманих даних дозволяє зробити такі висновки:

Протидія DDoS–атакам

Система продемонструвала надійний захист, ідентифікувавши та нейтралізувавши 98% шкідливих запитів. Прицьому рівень помилкових спрацьовувань становив лише 2%, що свідчить про високу точність детекції.

Виявлення SQL-ін'єкцій

Точність виявлення цього типу атак становила 94 %. Система ефективно ідентифікувала більшість спроб несанкціонованого доступу до баз даних, зберігаючи мінімальний рівень помилкових спрацьовувань.

Детектування сканування портів

Suricata виявила 98,3 % спроб несанкціонованого сканування мережевої інфраструктури. Такий результат підтверджує здатність системи оперативно реагувати на підозрілу мережеву поведінку.

Таблиця 3

Ефективність виявлення загроз (Detection Rate) за типами атак

Тип атаки	Рівень виявлення	Помилкові спрацювання	Рівень захисту
DDoS–атаки	98 %	2 %	Високий
SQL–ін'єкції	94 %	6 %	Високий
Сканування портів	98,3 %	1,7 %	Високий
Фішинг	90,7 %	9,3 %	Середній

6) Аналіз ефективності роботи системи

Проведено комплексну оцінку роботи Suricata за двома ключовими критеріями (табл. 4):

• Точність детекції – здатність ідентифікувати реальні загрози

• Частота помилкових спрацьовувань – кількість хибних тривог

Таблиця 4

Результати тестування Suricata: статистика виявлення атак

Тип атаки	Рівень виявлення	Реальні загрози	Помилкові спрацювання	Відсоток хибних спрацьовувань
DDoS-таки	1250	1125	25	2,0 %
SQL-ін'єкції	1440	1355	85	5,9 %
Сканування портів	2350	2310	40	1,7 %
Шкідливе ПЗ	1600	1510	90	5,6 %
Фішинг	1120	1015	105	9,3 %

7) Аналіз результатів на основі наборів даних

Проведене тестування на різних наборах даних виявило такі показники ефективності Suricata:

Таблиця 3

Показники точності виявлення атак та рівня помилкових спрацьовувань

Набір даних	Точність	Помилкові спрацьовування	Основні типи атак
CIC–IDS2017	96 %	3,5	DDoS, Ботнети, Фішинг
UNSW–NB15	93 %	4,0	Експлойти, Брутфорс–атаки, Аналіз
NSL–KDD	89 %	5,2	DoS, Зондування (Probe)

Висновки

Результати аналізу показали, що кожна IDS-система має свої переваги та недоліки, які визначають її ефективність у певних умовах. Відкриті рішення, такі як Zeek, Suricata та Snort, забезпечують високу гнучкість і можливість адаптації, але потребують складного налаштування. Комерційні продукти, наприклад, Cisco Secure IDS та IBM QRadar, пропонують комплексні рішення з розширеними функціями аналізу загроз, проте вимагають значних фінансових вкладень.

Отже, Отримані результати підтверджують, що сучасні IDS досягли значного прогресу у виявленні загроз, проте їх ефективність суттєво залежить від правильного вибору з урахуванням специфіки інфраструктури, наявності експертних ресурсів та бюджетних обмежень. Найбільш перспективними напрямами розвитку є інтеграція машинного навчання для автоматизації оновлення правил та розробка гібридних архітектур, що поєднують переваги відкритих і комерційних рішень. Особливу увагу

варто приділити оптимізації продуктивності для роботи з високошвидкісним мережевим трафіком, що стає особливо актуальним у сучасних умовах зростання кіберзагроз.

У рамках проведеного дослідження було здійснено комплексний аналіз сучасних систем виявлення вторгнень, що поєднував теоретичне вивчення методів детекції з практичним тестуванням на реальних наборах даних. Експериментальна частина, зокрема тестування Suricata, продемонструвала високу ефективність системи з середнім рівнем виявлення атак на рівні 92,6 % при помилкових спрацьовуваннях не більше 4,2 %. Такі відкриті рішення як Suricata та Zeek довели свою конкурентноздатність у порівнянні з комерційними аналогами, пропонуючи гнучкість налаштувань та відкриту архітектуру, хоча й вимагають кваліфікованого адміністрування.

ЛІТЕРАТУРА

[1] Smys S., Basar A., Wang H. Hybrid intrusion detection system for Internet of Things (IoT). *Journal of ISMAC*. 2020. Vol. 2, No. 4. P. 190–199. (дата звернення: 09.09.2025).

[2] Kasongo S. M., Sun Y. A deep learning method with wrapper based feature extraction for wireless intrusion detection system. *Computers & Security*. 2020. Vol. 92. Article ID 101752. https://doi.org/10.1016/j.cose.2020.101752

[3] Alazzam H., Sharieh A., Kannan A. A feature selection algorithm for intrusion detection system based on Pigeon Inspired Optimizer. *Expert Systems with Applications*. 2020. Vol. 148. Article ID 113249. https://doi.org/10.1016/j.eswa.2020.113249

[4] Ferrag M. A., Maglaras L., Ahmim A., Derdour M., Janicke H. RDTIDS: Rules and Decision Tree–Based Intrusion Detection System for Internet-of-Things Networks. *Future Internet*. 2020. Vol. 12, No. 3. P. 44. https://doi.org/10.3390/fi12030044

[5] Kumar V., Sinha D., Das A. K., et al. An integrated rule based intrusion detection system: analysis on UNSW-NB15 data set and the real time online dataset. *Cluster Computing*. 2020. Vol. 23. P. 1397–1418. https://doi.org/10.1007/s10586–019–03008–x

[6] Jin S., Chung J.–G., Xu Y. Signature–Based Intrusion Detection System (IDS) for In–Vehicle CAN Bus Network. 2021 IEEE International Symposium on Circuits and Systems (ISCAS). 2021. P. 1–5. https://doi.org/10.1109/ISCAS51556.2021.9401087

[7] Cahyo A. N., Sari A. K., Riasetiawan M. Comparison of Hybrid Intrusion Detection System. 2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE). 2020. P. 92–97. https://doi.org/10.1109/ICITEE49829.2020.9271727

[8] Gajjar H., Malek Z. A Survey of Intrusion Detection System (IDS) using Openstack Private Cloud. 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4). 2020. P. 162–168. https://doi.org/10.1109/WorldS450073.2020.9210313

[9] Goyal D., Balamurugan S., Peng S.-L., Verma O. P. Soft Computing–Based Intrusion Detection System With Reduced False Positive Rate. *Journal of Intelligent & Fuzzy Systems*. 2020. Vol. 39, No. 5. P. 6229–6241. https://doi.org/10.3233/JIFS–189254

[10] Ouiazzane S., Barramou F., Addou M. Towards a Multi–Agent based Network Intrusion Detection System for a Fleet of Drones. *International Journal of Advanced Computer Science and Applications* (IJACSA). 2020. Vol. 11, No. 10. P. 390–398. http://dx.doi.org/10.14569/IJACSA.2020.0111044

[11] Al S., Dener M. STL–HDL: A new hybrid network intrusion detection system for imbalanced dataset on big data environment. *Computers & Security*. 2021. Vol. 103. Article ID 102435. https://doi.org/10.1016/j.cose.2021.102435

[12] Черник О. А. Системи виявлення вторгнень // *Матеріали міжнародної науково–технічної конференції «Інформаційні моделі, системи та технології» (IMSTT–2023)*. Тернопіль: ТНТУ, 2023. С. 126. URL: https://elartu.tntu.edu.ua/bitstream/lib/44254/2/IMSTT_2023_Chernyk_O_A–Intrusion_detection_systems_126.pdf (дата звернення 13.03.2025)

[13] Столяр А. Л. Аналіз сучасних методів виявлення аномалій в комп'ютерних мережах. 2023, URL: https://doi.org/10.18372/2073–4751.74.17888.

[14] Kumar KN, Sukumaran S. A survey on network intrusion detection system techniques. International *Journal of Advanced Technology and Engineering Exploration*. 2018. 5(47). 385–393

[15] Zeek. URL: https://github.com/zeek/zeek (дата звернення 13.03.2025)

[16] Snort. URL: https://www.snort.org (дата звернення 13.03.2025)

[17] Suricata URL: https://suricata.io (дата звернення 13.03.2025)

[18] Security Onion URL: https://securityonionsolutions.com/ software (дата звернення 13.03.2025)

[19] Wazuh. URL: https://github.com/wazuh/wazuh (дата звернення 13.03.2025)

[20] Intrusion Detection: Cisco IDS Overview. URL: https://www.ciscopress.com/articles/article.asp?p=24696 (дата звернення 13.03.2025)

[21] IBM QRadar URL: https://www.ibm.com/qradar (дата звернення (дата звернення 13.03.2025)

[22] KDD Cup 1999 URL: https://www.kaggle.com/datasets/galaxyh/kdd-cup-1999-data (дата звернення 13.03.2025)

[23] NSL–KDD URL: https://www.kaggle.com/datasets/hassan06/nslkdd (дата звернення 13.03.2025)

[24] CIC–IDS2017: https://www.kaggle.com/datasets/chethuhn/network–intrusion–dataset (дата звернення 13.03.2025)

[25] UNSW–NB15: https://www.kaggle.com/datasets/mrwellsdavid/unsw-nb15 (дата звернення 13.03.2025)

Стороженко В. А., Дем'янчук Б. А., Козловська Д. В., Фесенко А. О.

ОГЛЯД МОЖЛИВОСТЕЙ IDS ДЛЯ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ

Системи виявлення вторгнень (IDS) відіграють ключову роль у сучасній кібербезпеці, забезпечуючи оперативне виявлення та попередження несанкціонованого доступу, атак, спроб проникнення та інших форм зловмисної активності в комп'ютерних мережах. Рішення IDS застосовуються як на мережевому рівні (NIDS), здійснюючи аналіз трафіку в реальному часі, так і на рівні окремих хостів (HIDS), здійснюючи моніторинг локальних подій, поведінки процесів та змін у файловій системі. Такий підхід дозволяє досягти комплексного захисту інформаційних систем і оперативного реагування на загрози.

У межах дослідження розглянуто існуючі підходи до реалізації IDS, зокрема сигнатурні, аномалійні та гібридні моделі виявлення загроз. Проведено порівняльний аналіз найпоширеніших відкритих та комерційних рішень, серед яких Zeek, Snort, Suricata, Security Onion, Wazuh, Cisco Secure IDS та IBM QRadar. Акцент зроблено на технічних характеристиках, продуктивності, точності виявлення загроз, рівні хибнопозитивних спрацьовувань, можливостях масштабування та інтеграції з іншими системами безпеки. Особливу увагу приділено питанням обробки великих обсягів даних у режимі реального часу та автоматизації реагування на інциденти.

Дослідження підкреслює важливість розвитку інтегрованих систем безпеки, де IDS виступають основним інструментом попереднього виявлення загроз. У роботі також акцентовано на потребі в адаптивності та інтелектуалізації таких систем шляхом застосування алгоритмів машинного навчання та кореляції подій у складних інформаційних середовищах. Результати аналізу можуть бути використані для побудови ефективної архітектури кіберзахисту організацій різного масштабу.

Ключові слова: система виявлення вторгнень, IDS, NIDS, HIDS, кібербезпека, аналіз мережевого трафіку, виявлення загроз, моніторинг безпеки.

Storozenko V., Demianchuk B., Kozlovska D., Fesenko A.

OVERVIEW OF IDS CAPABILITIES FOR NETWORK TRAFFIC ANALYSIS

Intrusion Detection Systems (IDS) play a crucial role in modern cybersecurity by providing timely detection and prevention of unauthorized access, intrusion attempts, and other forms of malicious activity within computer networks. IDS solutions are implemented at both the network level (NIDS), enabling real–time traffic inspection, and the host level (HIDS), where they monitor local events, process behavior, and file system changes. This comprehensive approach allows for efficient protection of information systems and rapid incident response.

This study examines the principal approaches to IDS implementation, including signature–based, anomaly–based, and hybrid threat detection models. A comparative analysis of widely adopted open–source and commercial IDS solutions—such as Zeek, Snort, Suricata, Security Onion, Wazuh, Cisco Secure IDS, and IBM QRadar—is presented. The analysis focuses on technical features, detection accuracy, false positive rates, scalability, integration capabilities with other security systems, and overall performance under high network loads. Special attention is given to the challenges of real–time data processing and the need for automation in incident response workflows.

The research highlights the importance of developing integrated security architectures in which IDS function as the core component for proactive threat detection. Additionally, the need for adaptability and system intelligence is emphasized, particularly through the integration of machine learning algorithms and event correlation mechanisms in complex, distributed IT environments. The findings of this work can serve as a foundation for designing effective cybersecurity infrastructures for organizations of various scales.

Keywords: intrusion detection system, IDS, NIDS, HIDS, cybersecurity, network traffic analysis, threat detection, security monitoring.

Стаття надійшла до редакції 28.05.2025 р.
Прийнято до друку 10.09.2025 р.