https://doi.org/10.31891/2307-5732-2025-351-26
УДК 004.056.53

КОРОБЕЙНІКОВА ТЕТЯНА
Національний університет «Львівська політехніка»
https://orcid.org/0000-0003-2487-8742
e-mail: tetianakorobeinikova@gmail.com

МЕТОД АНАЛІЗУ ДАНИХ ВІД СИСТЕМ IDS/IPS НА ОСНОВІ КОМБІНУВАННЯ СИГНАТУР І ПОЛІТИК

У статті проаналізовано сучасні IDS/IPS системи та їх спільні недоліки. Запропоновано вдосконалений метод аналізу даних, що поєднує сигнатурний і політиковий підходи. На його основі розроблено програмний засіб у середовищі Ubuntu з використанням Suricata та Python. Серед інших, показано алгоритми налаштування політик і формування рекомендацій. Чільна увага приділяється програмній реалізації запропонованих алгоритмів та методу аналізу даних від систем виявлення та запобігання вторгнень.

Ключові слова: IDS/IPS, мережева безпека, аналіз сигнатур, аналіз політик, виявлення аномалій, правила безпеки.

KOROBEINIKOVA TETIANA
Lviv National Technical University

METHOD FOR ANALYZING DATA FROM IDS/IPS SYSTEMS BASED ON A COMBINATION OF SIGNATURES AND POLICIES

Prevention Systems (IDS/IPS). We review widely used solutions such as Snort, Suricata, McAfee Network Security Platform, and Zeek, highlighting their strengths and weaknesses in network security applications. Our proposed approach aims to improve threat detection by combining signature-based and policy-based techniques. Specifically, Suricata is leveraged for real-time traffic monitoring, while a Python-based software tool streamlines rule configuration, event logging, and the generation of actionable recommendations. We present an improved method for analyzing IDS/IPS data that processes known threat signatures and user-defined policies concurrently. In doing so, it enables more accurate detection of malicious activity, unauthorized access attempts, and suspicious behavior beyond documented vulnerabilities. A central aspect of this study is the development of algorithms for policy customization (e.g., defining trusted hosts, blocked IP addresses, and specific port/protocol restrictions) and automated assessment of security events. Experimental validation was conducted on an Ubuntu 18.04 platform, demonstrating a notable decrease in false positives, better adaptability to evolving network conditions, and streamlined management of security incidents. The system promptly identifies potential anomalies and provides relevant recommendations by correlating JSON-formatted Suricata outputs with user-configured policies. These include creating or adjusting firewalls and IDS/IPS rules to restrict traffic or block suspicious hosts. The findings confirm that integrating signature-based and policy-based detection offers a scalable, effective defense mechanism for organizations of various sizes. Such an approach accelerates threat mitigation processes, reduces the overhead of manual rule management, and enhances overall cybersecurity posture. This research contributes to the ongoing evolution of IDS/IPS solutions, addressing common limitations related to system complexity, performance bottlenecks, and the persistent challenge of detecting previously unknown attacks.

Keywords: IDS/IPS, network security, signature analysis, policy analysis, anomaly detection, security rules.

Стаття надійшла до редакції / Received 11.04.2025
Прийнята до друку / Accepted 26.04.2025

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Кожна сучасна організація зустрічається з проблемою захисту своїх даних та мереж від несанкціонованого доступу. За даними статистики, збитки, які можуть завдати кібератаки компанії, у середньому становлять 2,4 мільйона доларів [1]. Однією з найпоширеніших помилок, яку допускають організації, є використання лише одного рівня захисту від загроз [2, 3]. З кожним днем зловмисники стають все більш обізнаними та досвідченими, тому необхідністю стає використання комплексного захисту, який включає в себе IDS/IPS системи [3, 4, 5]. Ці системи стрімко розвиваються пропонуючи захист від сучасних загроз [4, 6, 7]. Зокрема очікується, що до 2025 року система IDS/IPS на базі хоста буде розвиватися із середньорічним темпом зростання понад 15% [8]. Ця система має можливість відстежувати критично важливі системні файли хоста, аналізувати запущені процеси, дії користувача, цілісність даних та інші пов'язані з цим вторгнення в систему. Загалом, використання IDS/IPS систем для захисту інформаційних систем та мереж є необхідністю у сучасному світі. Таким чином, існує потреба у вдосконалені методів та засобів аналізу даних отриманих від систем IDS/IPS.

Аналіз досліджень та публікацій

Тема вдосконалення систем виявлення та запобігання вторгнень активно досліджується впродовж останніх років [9, 10]. Науковці пропонують різноманітні підходи, зокрема використання штучних нейронних мереж, алгоритмів машинного навчання та евристичних методів для виявлення аномалій [11–13]. У дослідженнях, присвячених Snort і Suricata [14], на перший план виходять підвищення продуктивності та точності при розпізнаванні загроз. Роботи, що стосуються McAfee та Zeek [14–15], акцентують увагу на комплексній обробці мережевого трафіку, зокрема на гнучкому модульному принципі та покращеній сумісності з іншими програмними рішеннями. Проте залишається

проблема великої кількості хибних спрацювань і недостатньої адаптивності існуючих систем. Окремі автори наголошують на доцільності комбінованого підходу, що поєднує сигнатурний метод [16] (для відомих загроз) і політиковий чи аномалійний метод [17] (для виявлення невідомих атак). Такий підхід здатен знизити ризики пропуску нових загроз і підвищити результативність IDS/IPS за умов динамічних змін у мережевому середовищі, що й визначає актуальність подальших досліджень у цьому напрямі.

Формулювання мети роботи

Метою роботи є підвищення рівня безпеки та захисту мережі від несанкціонованого доступу за рахунок застосування вдосконаленого методу аналізу даних від систем виявлення та запобігання вторгнень.

Виклад основного матеріалу

Відомо, що служби виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS) постійно відстежують мережу, виявляють можливі інциденти та фіксують інформацію про них, зупиняють інциденти та повідомляють про них адміністраторів служби безпеки. Мережі використовують служби виявлення вторгнень та системи запобігання вторгненням для виявлення проблем із політикою безпеки та захисту фізичних осіб від порушення політики безпеки. Таким чином, IDS та IPS стали невід'ємною частиною інфраструктури безпеки: можуть зупинити зловмисників та одночасно зібрати інформацію про мережу [18]. Між IPS та IDS-системами є відмінності, зумовлені місцем інтеграції інструментів у ланцюжок обробки трафіку, та особливості, що визначають спектр завдань та обмежень. Саме тому функціонал мережевих екранів (МЕ) краще доповнювати функціоналом систем IDS/IPS, підвищуючи рівень захисту.

Метою дослідження є підвищення рівня безпеки та захисту мережі від несанкціонованого доступу за рахунок застосування вдосконаленого методу аналізу даних від систем виявлення та запобігання вторгнень.

1. Поняття IDS/IPS та їх роль в сучасних комунікаційних системах

IDS, Intrusion Detection System – система виявлення вторгнень. IPS, Intrusion Prevention System, – система запобігання вторгненням. У порівнянні з традиційними засобами захисту – антивірусами, спам-фільтрами, фаєрволами – IDS/IPS забезпечують високий рівень захисту мережі. Сьогодні МЕ у взаємодії з IPS та IDS-системами є одним із ключових засобів виявлення та захисту від дій зловмисників. Системи IPS та IDS відносно легко налаштовуються, просто управляються та можуть забезпечити високу точність моніторингу мереж. IPS та IDS-системи мають ряд корисних можливостей:

1) Виявлення сигнатур – трафік перевіряється на відповідність профілю відомих атак (шаблонів). Це дозволяє виявити атаки, шкідливі коди, рух хибного трафіку та інші ризики. Застосовується для виявлення та блокування відомих атак.
2) Виявлення на основі аномальної поведінки в даних – системи можуть використовувати не лише шаблони, але й розпізнавати нові (нешаблонні) варіанти атак. Як правило, для цього задіюється штучний інтелект та моделі машинного навчання.
3) Спостереження за користувачами в реальному часі – алгоритми збирають дані про трафік та комплексно аналізують його. Це дозволяє не лише знаходити проблеми, а й точно ідентифікувати їх: звідки була загроза, коли та яким чином.

IDS відстежує трафік, порівнюючи його з власною базою даних можливих мережевих атак та базовою мережевою активністю. Такий механізм роботи дозволяє виявляти: мережеві атаки; неавторизований доступ до даних; дії шкідливих скриптів та програм; функціонування сканерів портів; порушення політик безпеки; звернення до центрів управління бот-мережами та майнінг-пулами; аномальну активність. Виявити порушення політик безпеки можна за рахунок написання власних патернів детектування. Це допомагає відстежувати певну поведінку у мережі. Важливо помітити, що IDS-система не відображає атаки, а лише виявляє їх і повідомляє адміністратора, допомагаючи знайти причину та усунути її [10]. Інструменти IDS можуть використовуватися окремо або у складі МЕ.

IPS виконує співставлення трафіку відомим патернам мережевих атак для виявлення: зміни тенденцій мережевого трафіку; спроб несанкціонованого доступу; спроб звернення до небезпечних ресурсів із мережі організації. IPS здатна виявляти ризики на різних рівнях, автоматично відповідати на них: блокувати небезпечний трафік; генерувати подію безпеки для адміністратора. Таким чином, IPS є інструментом активного захисту. Фактично IPS виступає другим рубежом захисту, що знаходиться за МЕ або входить до його складу [12].

Основна відмінність систем полягає у методі реагування на порушення інформаційної безпеки. По своїй суті, IDS є інструментом моніторингу: може розпізнати небезпечні дії та попередити про них. А IPS-система – механізм ширшого застосування: виявляє проблему, запускає процеси протидії їй. Наприклад, скидання з'єднання або блокування IP-відправника. Крім відмінностей у способі реагування на атакуючий або підозрілий трафік, IPS та IDS відрізняються способом розташування в інфраструктурі мережі та по відношенню до мережевого трафіку. Як правило, IDS системи встановлюються «збоку» від мережевих потоків, обробляючи копію трафіку, що проходить через мережу, а IPS зазвичай встановлюються «в розрив» і стоять на проході трафіку через активне мережеве обладнання [12].

Порівняльний аналіз IPS/IDS систем та виявлення їх недоліків відображено у таблиці 1.

Таблиця 1

Порівняльний аналіз сучасних систем виявлення та запобігання вторгнень

Система	*Переваги*	*Недоліки*	*Спосіб вирішення*
Snort	визначає атаки «під прикриттям»; здатна виявляти і блокувати широкий спектр атак	сповільнення роботи через однопотоковість; сканування лише за вказаним номером порту	модернізація системи; оптимізація використання ресурсів; реалізація багатопотоковості
Suricata	багатопотоковість та висока продуктивність; полегшене інтегрування зі сторонніми програмами; обробка даних 7-го рівня OSI	великий обсяг налаштувань; недостатня (в деяких питаннях) документація	використання сторонніх програм (напр. Kibana) для полегшення спілкування з системою
McAfee Network Security Platform	можливість виявляти невідомі раніше атаки завдяки використанню сигнатур; забезпечення максимального захисту мережі	висока вартість; уповільнення роботи мережі через «тяжкий» функціонал	доцільно використовувати у випадках, коли необхідність максимального захисту виправдовує затрати на встановлення і пітримку системи
Zeek	підтримка різних режимів роботи; гнучкий функціонал; можливість створення власних скриптів політик та спеціальних аналізаторів протоколів	складність спілкування з інтерфейсом, складність налаштувань	високий фаховий рівень користувача; система призначена для використання в мережах, де необхідна гнучкість та велика кількість налаштувань

Серед спільних недоліків сучасних систем виявлення та запобігання вторгнень можна виокремити такі: уповільнення роботи системи або мережі; велика кількість налаштувань; складність роботи з інтерфейсом; складність налаштувань системи для недосвідчених користувачів.

2. Формування задач у сучасних системах виявлення та запобігання вторгнень

Виділивши конкретні завдання, що виконуються IPS/IDS можна сформулювати головні вимоги до таких систем. Системи виявлення атак мають дві основні функції: збирають доказову базу для розслідування інцидентів (наприклад, коли зловмисник довго користується ресурсами організації); здійснюють моніторинг шкідливої активності. Отже, основні вимоги до IDS – це повнота охоплення відомих експлойтів та вразливостей (актуальність бази сигнатур); а також «живучість» системи, щоб вона постійно збирала необхідну інформацію. В ідеалі система повинна бути здатною виявляти також і невідомі раніше вразливості та атаки, тобто працювати без сигнатур.

Системи запобігання атак займаються «нормалізацією» трафіку, блокуванням атак та мінімізацією завданих збитків. Вимоги до IPS: надійність, тобто не повинно перериватись функціонування системи (збої можуть призвести до таких неприємних наслідків, як обрив каналу та відмова в обслуговуванні); низький рівень хибних спрацювань.

Окрім надійності однією з основних вимог до систем IPS/IDS є забезпечення високої швидкості роботи мережі; гнучкість налаштувань; зрозуміле виведення результатів. Водночас велика кількість налаштувань не повинна призводити до складнощів роботи з програмою, а інтерфейс повинен залишатися зрозумілим для користувача [].

3. Методи виявлення атак при роботі з IDS/IPS системами

IDS/IPS системи є гнучким інструментом для забезпечення захисту мережі і здатні перехоплювати трафік та аналізувати його згідно попередньо налаштованих правил, виявляти підозрілу чи аномальну активність та порушення попередньо налаштованих політик. Для роботи систем виявлення та запобігання вторгнень потрібно попередньо налаштовувати правила та політики, система повинна розуміти яка активність є нормальною, а яка може сигналізувати про порушення, зрештою необхідна певна база сигнатур, яка допомагає розпізнавати вторгнення. Загалом методи виявлення атак можна розділити на три основні категорії: метод аномалій; метод аналізу сигнатур; метод політик.

Метод аномалій допомагає виявляти підозрілу активність в мережі та на окремих хостах. Спочатку збираються дані про нормальну роботу системи, які зберігаються у профілях. Їх потім використовують детектори для аналізу подій та порівняння поточної активності із нормальною. Тут не потрібно зберігати велику базу сигнатур і це є очевидною перевагою. Але потрібно бути готовим до обробки великої кількості помилкових сигналів про загрози.

Під час використання методу аналізу сигнатур весь трафік аналізується шляхом порівняння з існуючими сигнатурами, тобто шукаються ознаки, які б вказували на конкретну атаку. В порівнянні з попереднім методом цей метод має досить малу кількість помилкових спрацювань, але для забезпечення захисту потрібна велика база сигнатур, яка б охоплювала якомога більше відомих атак.

Для методу політик потрібні попередньо налаштовані чіткі правила мережевої безпеки, згідно яких буде аналізуватись трафік. Такі правила можуть містити принципи взаємодії окремих хостів чи мереж, дозволені порти, протоколи, визначати у який час дозволено доступ і т.д. Метод є доволі гнучким, адже правила можна налаштовувати індивідуально для кожної організації, проте таке налаштування потребує певного досвіду та аналізу роботи конкретної організації [10].

4. Обробка та аналіз даних за допомогою комбінованого методу сигнатур та політик

Системи IDS/IPS є гнучким інструментом, і для роботи з ними можна використовувати комбіновані методи виявлення атак. Хорошим рішенням є поєднання методу аналізу сигнатур та методу політик. При такому підході система зможе виявляти та блокувати підозрілий трафік за допомогою сигнатур, а також проводити порівняння результату такого аналізу на відповідність наперед визначеним політикам. Розглянемо цей метод детальніше. На рис. 1 зображена схема комбінованого методу аналізу даних від систем виявлення та запобігання вторгнень.

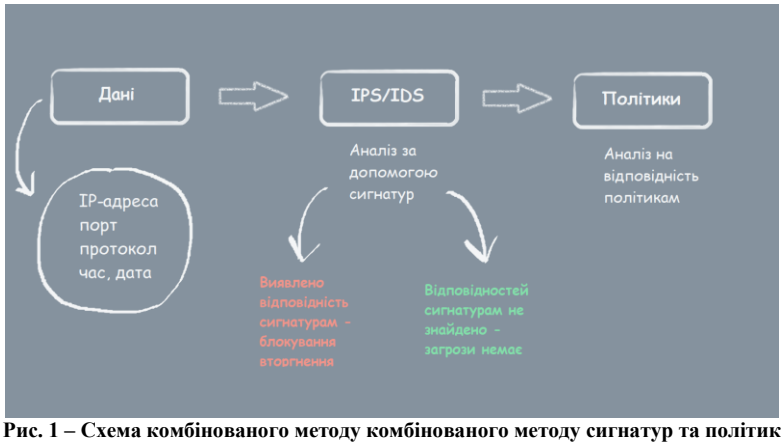


Рис. 1 – Схема комбінованого методу комбінованого методу сигнатур та політик

На першому етапі IDS/IPS система збирає дані про події (IP відправника та отримувача, їх порти, протоколи та час події) і аналізує їх за допомогою наперед визначених сигнатур; на основі аналізу приймає рішення чи відбувається вторгнення. Якщо вторгнення є – тоді трафік блокується і формується сповіщення, якщо вторгнення немає – трафік дозволяється і подія передається на наступний етап аналізу – аналіз на відповідність політикам. Тут відбувається перевірка події на відповідність наперед визначених політикам. До прикладу, може бути визначено певний діапазон IP-адрес з'єднання з якими дозволено чи заборонено; визначено хости чи мережі, які можуть встановлювати з'єднання тільки по певним портам або протоколам чи в певний час. Така схема аналізу допоможе забезпечити не тільки надійний захист за допомогою аналізу сигнатур, але і можливість налаштувати систему індивідуально за допомогою політик, проте це потребує кропіткої роботи з визначення особливостей конкретної організації і формування політик.

5. Метод аналізу даних від систем виявлення та запобігання вторгнень

Під аналізом даних від систем IDS/IPS розуміємо всі дані, якими вони оперують та/або ті, що вони обробляють та продукують спільно, в процесі суміжної роботи у єдиній системі (табл. 2).

Таблиця 2

Дані від систем IDS/IPS

Дані, що отримано від IDS/IPS	*Дані, що отримано у результаті налаштувань безпеки*
d_1 – чи було встановлено з'єднання; d_2 – IP-адреса відправника; d_3 – IP-адреса отримувача; d_4 – порт відправника; d_5 – порт отримувача; d_6 – протокол;	d_7 – IP-адреси домашньої мережі; d_8 – дружні IP-адреси та дозволені для них порти, протоколи; d_9 – заблоковані IP-адреси.

Множина цих даних $D = \{d_1, d_2, \dots, d_9\}$ використовуються задачами з множини $T = \{t_1, t_2, \dots, t_5\}$, для подальшого формування рекомендацій $R = \{r_1, r_2, \dots, r_5\}$. Перелік задач T наведено у таблиці 3. У результаті виконання задач формуються рекомендації R (табл. 4). Схема методу аналізу даних від систем виявлення та запобігання вторгнень зображена на рис. 2.

Таблиця 3

Перелік задач *T*

Задача	*Розшифровка*	*Дані, що використовуються*
t_1	якщо з'єднання не було встановлено, визначаємо, чи відправник та отримувач належать до домашньої мережі	d_1, d_2, d_3, d_7
t_2	якщо з'єднання було встановлено та отримувач належить до домашньої мережі, визначаємо, чи відправник належить до заблокованих	d_1, d_2, d_3, d_7, d_9
t_3	якщо з'єднання було встановлено, отримувач належить до домашньої мережі та відправник належить до дружніх, визначаємо, чи відправник використав дозволений порт для встановлення з'єднання	$d_1, d_2, d_3, d_5, d_7, d_8$
t_4	якщо з'єднання було встановлено, отримувач належить до домашньої мережі та відправник належить до дружніх, визначаємо, чи відправник використав дозволений протокол для встановлення з'єднання	$d_1, d_2, d_3, d_6, d_7, d_8$
t_5	якщо після перевірки не знайдено загроз, визначаємо, чи налаштування безпеки заповнені повністю	d_7, d_8, d_9

Таблиця 4

Формування рекомендацій *R*

Задача	*Рекомендація*	*Рівень загрози*	*Рекомендація*
t_1	r_1	немає	заблоковано з'єднання між хостами домашньої мережі, рекомендовано переглянути налаштування правил та налаштувань безпеки
t_2	r_2	високий	заблокований хост отримав доступ до домашньої мережі, рекомендовано негайно створити правило, що обмежувало б доступ
t_3	r_3	середній_1	дружній хост отримав доступ до домашньої мережі через заборонений порт, рекомендовано налаштувати правила, щоб обмежити доступ
t_4	r_4	середній_2	дружній хост отримав доступ до домашньої мережі через заборонений протокол, рекомендовано налаштувати правила, щоб обмежити доступ
t_5	r_5	низький	налаштування безпеки не заповнені повністю, рекомендовано заповнити налаштування безпеки, щоб отримувати актуальні рекомендації

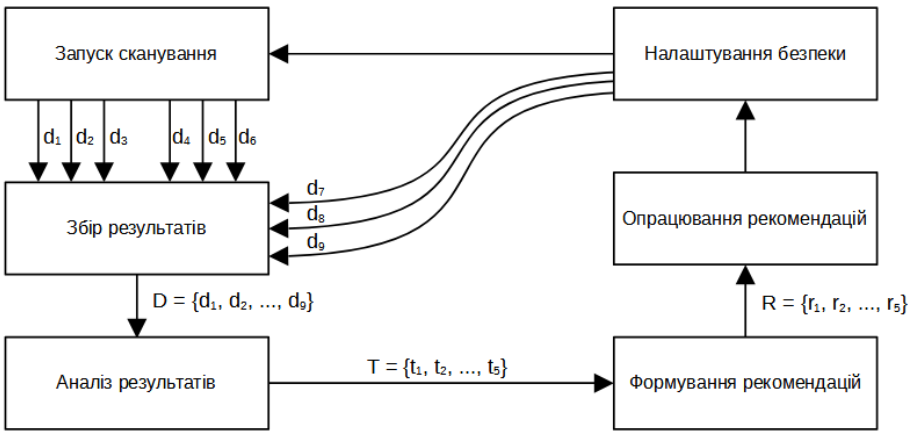


Рис. 2 – Схема методу аналізу даних від систем виявлення та запобігання вторгнень

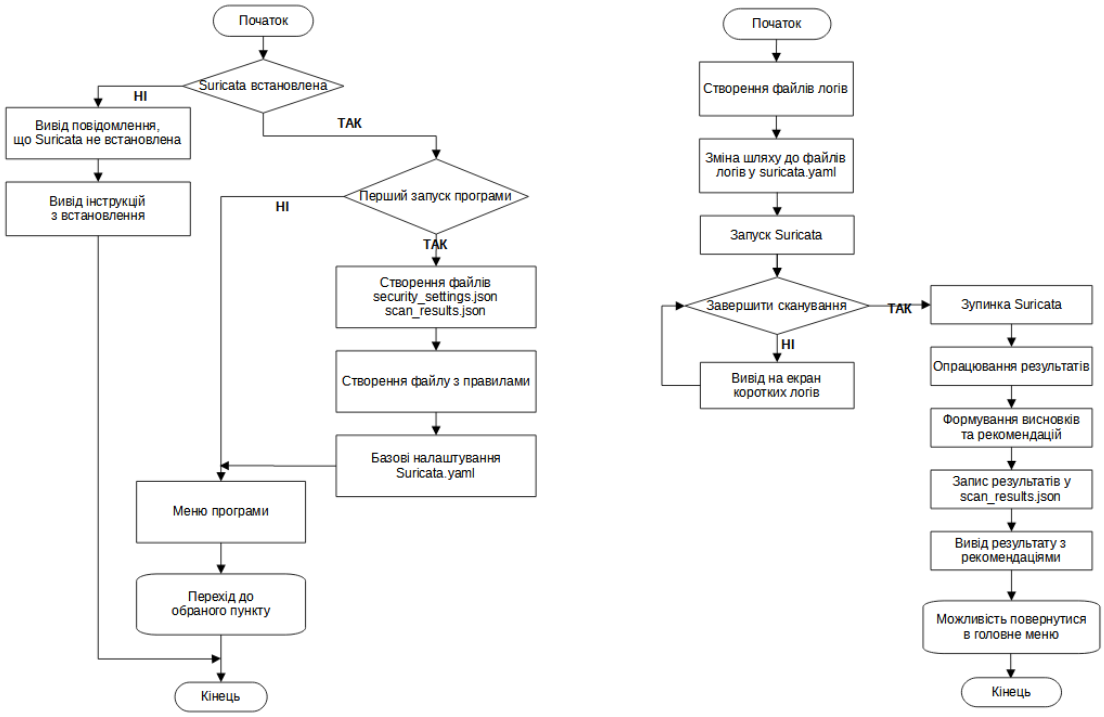
Відомо, що системи IDS/IPS для аналізу роботи мережі використовують три методи виявлення атак: метод аномалій, метод аналізу сигнатур та метод політик. Згідно результатів такого аналізу системи здатні розпізнати загрози чи підозрілі активності. Для забезпечення більш надійного захисту можна поєднати метод аналізу сигнатур та метод політик. Таким чином IDS/IPS система аналізує

трафік, порівнюючи його з сигнатурами, а для обробки даних отриманих від IDS/IPS системи використовується метод політик.

6. Вибір IDS/IPS системи, та середовища програмування

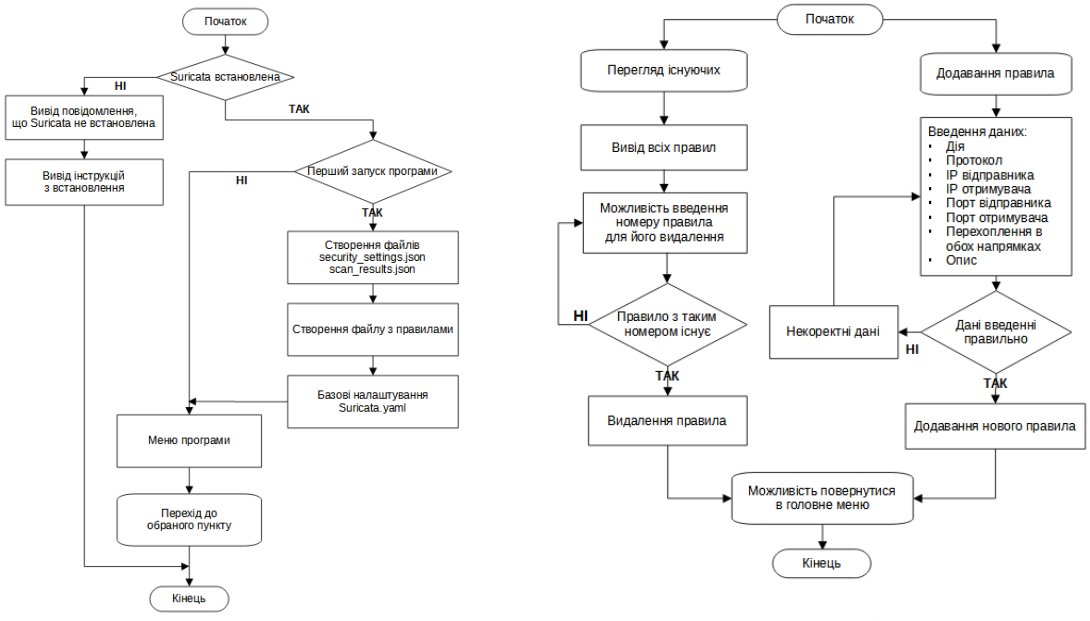
Для реалізації програми доцільно використовувати систему, яка може працювати в режимах і IDS, і IPS; взаємодія з програмою відбувається через термінал, а отримувати дані можна в зручному для обробки форматі JSON (RFC 4627) [20]. Suricata оперує JSON, є безкоштовною і може працювати на різних ОС. Програма буде реалізована на ОС Ubuntu версії 18.04 мовою програмування Python 3 (Python 3.6).

Алгоритм роботи програми. Під час запуску програми виконується перевірка, чи встановлена Suricata, та перевіряються її базові налаштування. Алгоритм запуску програми зображено на рис. 3, а. Після успішного запуску відкривається головне меню програми, звідки є можливість перейти до запуску сканувань, перегляду попередніх сканувань, налаштування правил та налаштувань безпеки (політик). Алгоритм запуску сканування зображено на рис. 3, б. Алгоритм перегляду попередніх сканувань зображено на рис. 4, а. Алгоритм налаштування правил зображено на рис. 4, б.



а) б)

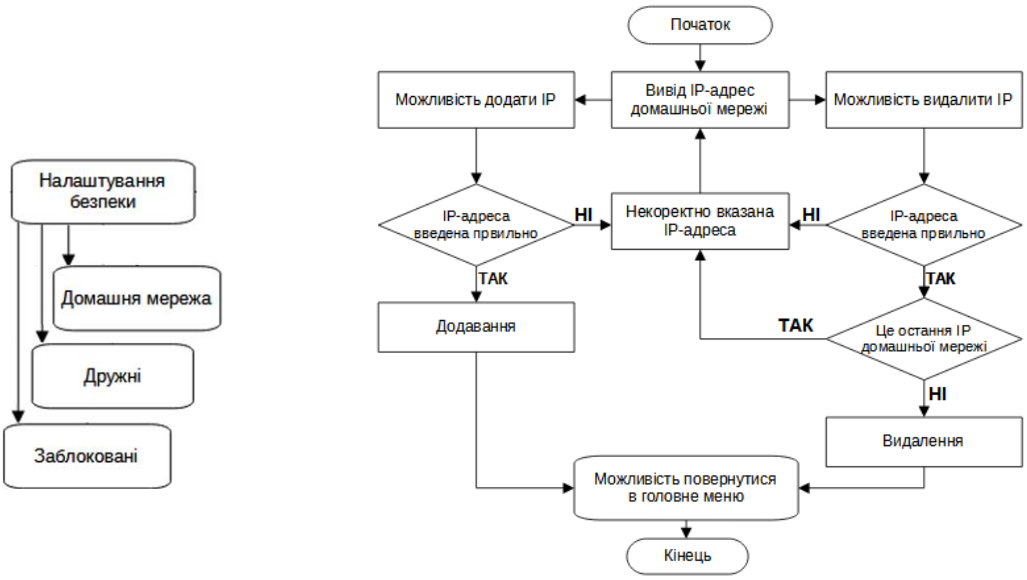
Рис. 3 – Алгоритми: запуску програми (а) та запуску процесу сканування (б)



а) б)

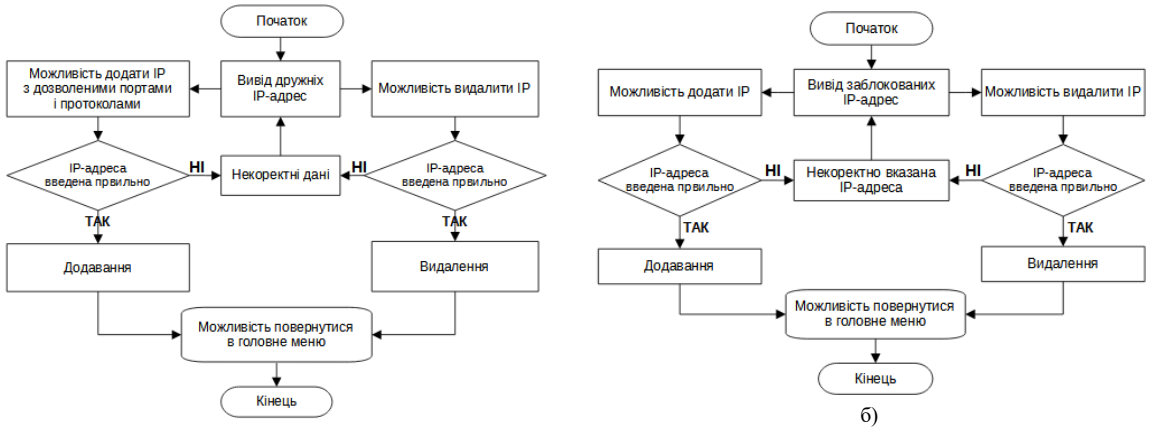
Рис. 4 – Алгоритми: перегляду попередніх сканувань (а) та налаштування правил (б)

Налаштування безпеки складається з налаштування домашньої мережі, дружніх IP-адрес та заблокованих (рис. 5, а). Алгоритм налаштування домашньої мережі зображено на рис. 5, б. Алгоритм налаштування дружніх IP-адрес зображено на рис. 6, а. Алгоритм налаштування заблокованих IP-адрес зображено на рис. 6, б.



а) б)

Рис. 5 – Алгоритми: налаштування безпеки (а) та налаштування домашньої мережі (б)



а) б)

Рис. 6 – Алгоритми налаштування: дружніх IP-адрес (а) та заблокованих IP-адрес (б)

Алгоритм формування висновків та рекомендацій після сканування. Після завершення сканування інформація про всі події зберігаються у файлі `eve`[*номер_сканування*]`.json`. Формування висновків та рекомендацій відбувається на основі політик (налаштувань безпеки), на рис. 7 зображено алгоритм формування висновків та рекомендацій. Для формування висновків та рекомендацій переглядається кожна подія та опрацьовується згідно наведеного алгоритму. Висновки сигналізують рівні загрози, які можуть бути чотирьох типів: загрози немає; низький рівень; середній рівень; високий рівень.

За умови наявності загроз, рекомендації належать до 5 типів (від r_2 до r_5):

1) З'єднання між хостами $[host\_1]$ та $[host\_2]$, що належать до домашньої мережі заблоковано існуючим правилом. Рекомендовано переглянути налаштування правил/політик.

2) Хост $[host\_1]$ (порт $[port\_1]$), що позначено як заблокований, встановив з'єднання з $[host\_2]$ (порт $[port\_2]$). Протокол $[protokol]$. Рекомендовано негайно створити правило, що обмежувало б доступ.

3) Хост $[host\_1]$, що позначено як дружній, встановив з'єднання з $[host\_2]$ через порт $[port\_p]$, за умови $p \notin n{:}m$ і дозволені порти: $[port\_n{:}m]$. Рекомендовано налаштувати правила, щоб обмежити доступ.

4) Хост $[host\_1]$, що позначено як дружній, встановив з'єднання з $[host\_2]$ через протокол $[protokol\_p]$, за умови $p \notin l{:}k$ і дозволені протоколи: $[protokol\_l{:}k]$. Рекомендовано налаштувати правила, щоб обмежити доступ.

5) Рекомендовано заповнити налаштування безпеки, щоб отримувати актуальні рекомендації.

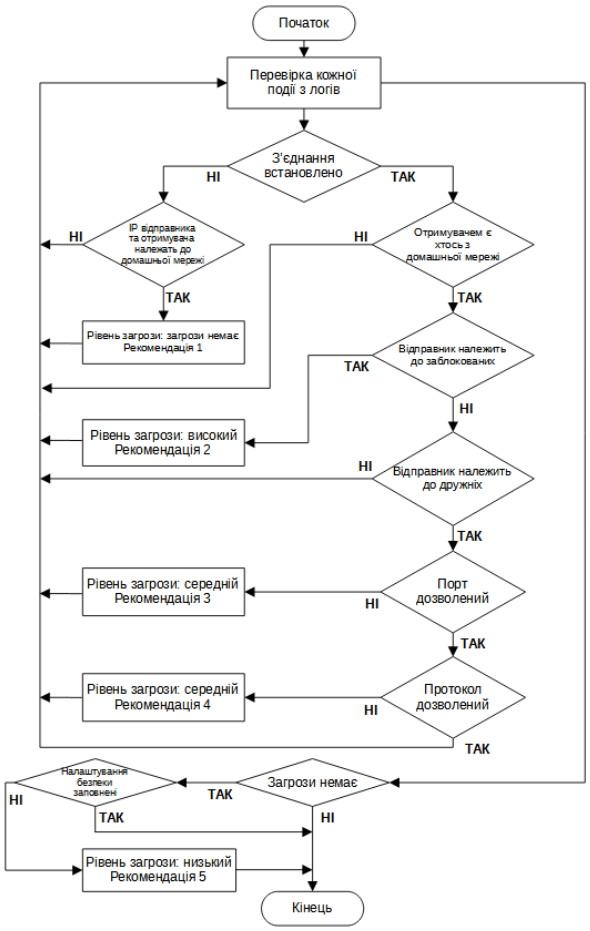
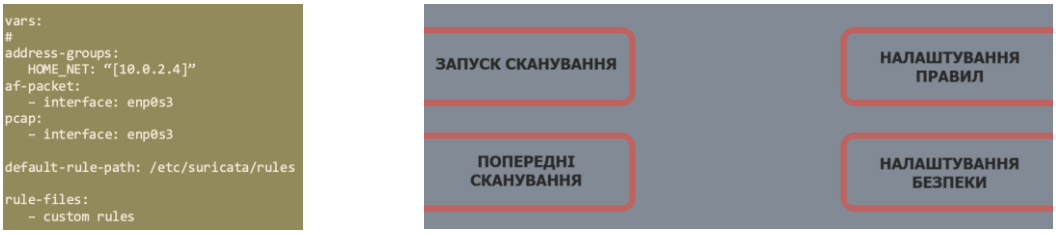


Рис. 7 – Алгоритм формування висновків та рекомендацій

7. Тестування програмного засобу

Програма розроблена для ОС Ubuntu, тестування відбувається за допомогою віртуальної машини з встановленою Ubuntu версії 18.04. Під час запуску відбувається перевірка чи встановлена Suricata. Якщо Suricata не встановлена – виводиться відповідне повідомлення з командами для її встановлення. Якщо Suricata встановлена і це перший запуск програми – виконуються базові налаштування, зокрема налаштовується конфігураційний файл suricata.yaml (рис. 8, а). Під час запуску відкривається головне меню програми (рис. 8, б). Звідти є можливість перейти до запуску сканувань, перегляду результатів попередніх сканувань, налаштування правил та налаштування безпеки.



а) б)

Рис. 8 – Налаштування першого запуску (а) та зовнішній вигляд головного меню програми (б)

З метою тестування створимо перше правило, яке б перехоплювало весь трафік, для цього переходимо до пункту меню щодо налаштування правил – додати правило `alert ip any any <> 10.0.2.4 any (msg; "test.rule"; sid:1;)` (рис. 9, а та 9, б), щоб заповнити інформацію про правило.

Виберемо дію `alert` (створення сповіщення); всі протоколи (по IP); IP відправника; порти відправника та отримувача виберемо будь-які; в IP отримувача запишемо власну IP-адресу; оберемо перехоплення пакетів в обох напрямках. Після додавання правила з'являються у списку правил, звідки їх можна видалити за їхнім номером (рис. 9, б).

Перейдемо до результатів першого сканування. З метою перевірити роботу правила, відкриємо сторінку браузера. Під час сканування виводяться логи про перехоплені пакети (рис. 9, в). Після завершення сканування виводиться результат з рівнем загрози та відповідними рекомендаціями (рис. 9, г). Так як не було знайдено порушень налаштувань безпеки, рівень загрози є низьким.

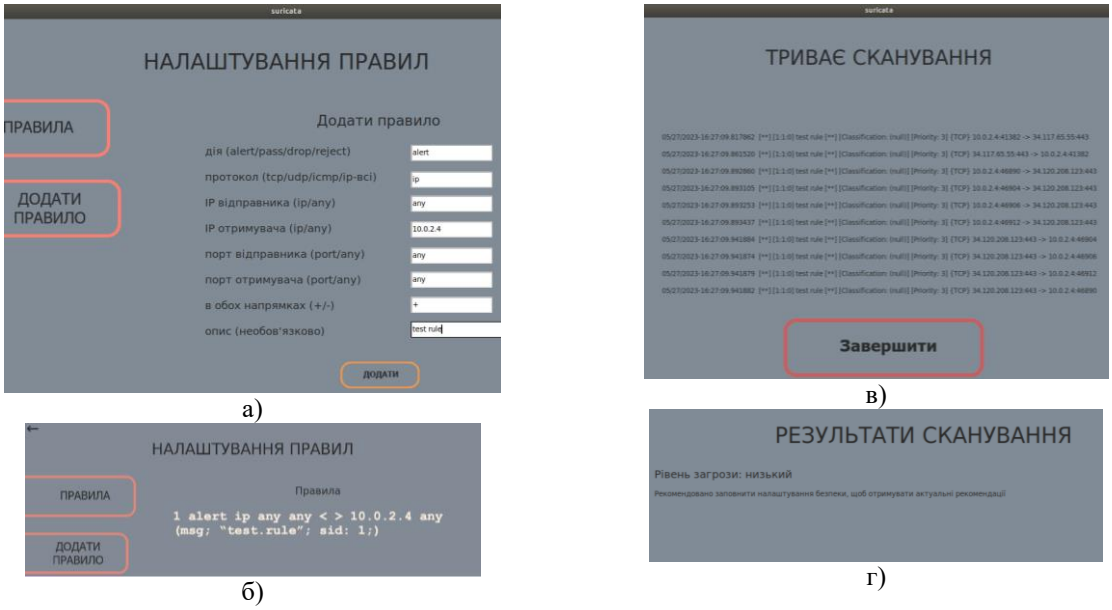


Рис. 9 – Створення правила (а), його візуалізація (б), процес сканування (в) та його результат (г)

Для подальшого тестування програми об'єднаємо тестову віртуальну машину (10.0.2.4) в одну локальну мережу з іншою віртуальною машиною (10.0.2.15). Тепер додаємо нові налаштування безпеки, а саме додаймо дружній хост – 10.0.2.15, і дозволимо йому доступ лише за протоколом TCP через порти 80 і 443, всі решта протоколи заборонені (рис. 10).

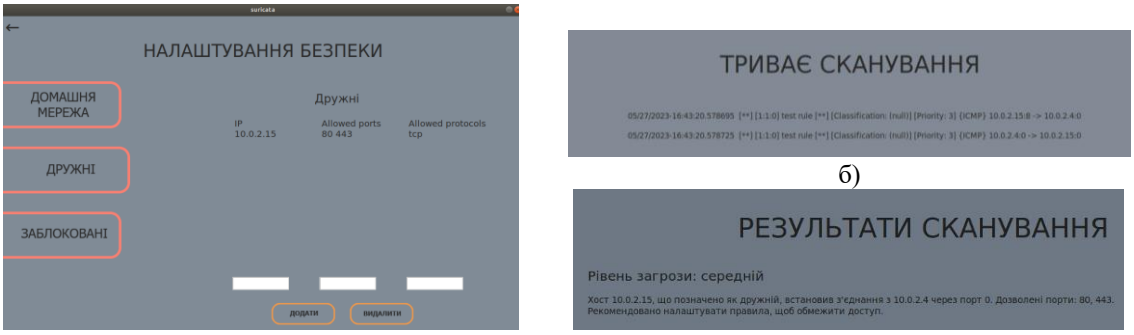


Рис. 10 – Налаштування дружніх хостів (а), перехоплення ping (б) та результат сканування (в)

Запустимо сканування і спробуємо виконати ping із іншої віртуальної машини. На рис. 11, а показано процес сканування, де видно що пінг пройшов. На рис. 11, б показано результати сканування. Рівень загрози визначено як середній, адже, згідно налаштувань безпеки, хосту 10.0.2.15 можна встановлювати з'єднання лише через порти 80 або 443, а відповідного правила яке б обмежувало доступ створено не було.

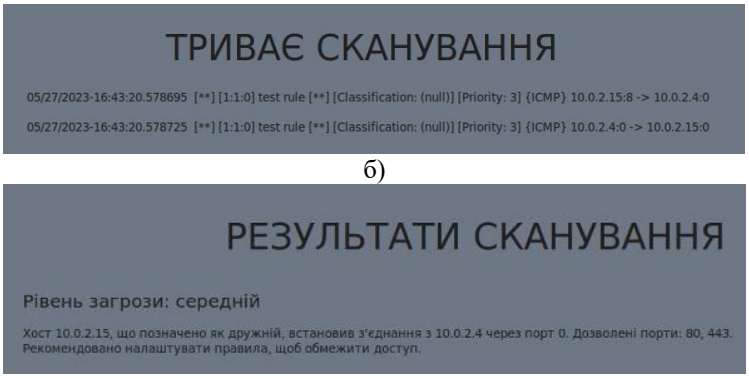
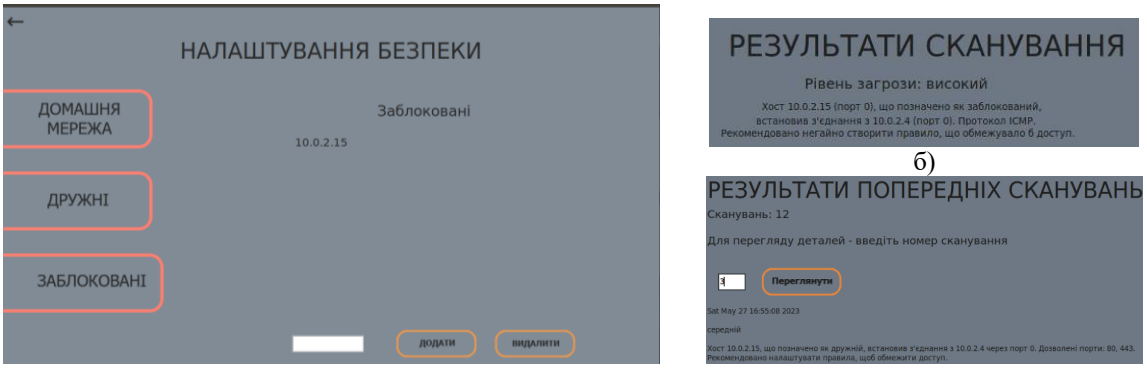


Рис. 11 – Перехоплення ping під час сканування (а) та результат сканування (б)

Завершимо налаштування безпеки, вказавши заблокований хост 10.0.2.15, попередньо видаливши його з дружніх (рис. 12, а). Знову запустимо сканування і виконаємо ping(на рис. 12, б зображено результати цього сканування).

Рівень загрози є високим, адже хост належить до заблокованих і немає правила, яке б обмежувало доступ. Результати попередніх сканувань також доступні для перегляду (рис. 12, в).



а) б) в)

Рис. 12 – Додавання заблокованої адреси (а), результати сканування з високим рівнем загрози (б) та перегляд результату третього сканування (в)

Таким чином, реалізовано програму обробки даних отриманих від системи виявлення та запобігання вторгнень Suricata. При обробці даних використано комбінування методів сигнатур та політик, що дозволило сформувати висновки про рівень загрози та відповідні рекомендації. Створена програма полегшує взаємодію з Suricata завдяки зручному інтерфейсу для створення правил, запуску сканування та перегляду логів.

Висновки

Потреба у вдосконалені методів та засобів аналізу даних отриманих від IDS/IPS систем для збільшення ефективності їх використання стала підставою для даного дослідження. У статті досягнуто підвищення рівня безпеки та захисту мережі від несанкціонованого доступу за рахунок застосування вдосконаленого методу аналізу даних від систем виявлення та запобігання вторгнень. Зокрема, в роботі виконано такі завдання: проаналізовано відомі системи виявлення та запобігання вторгнень та алгоритми їх роботи шляхом їх порівняння та виявлення їх спільних недоліків; проведено аналіз задач та проблем у сучасних системах виявлення та запобігання вторгнень; наведено основні методи виявлення атак при роботі з IDS/IPS системами; розглянуто обробку та аналіз даних від систем IDS/IPS за допомогою комбінованого методу сигнатур та політик. Запропоновано вдосконалений метод аналізу даних від систем виявлення та запобігання вторгнень, який, на відміну від відомих, використовує поєднання методу сигнатур для виявлення атак та методу політик для аналізу даних отриманих від систем IDS/IPS. Розроблено програмний засіб аналізу даних від систем IDS/IPS, що використовує вдосконалений метод аналізу даних отриманих від систем IDS/IPS.

Наукова цінність: вдосконалено існуючі методи аналізу даних у системах виявлення та запобігання вторгнень, за рахунок поєднання їх із засобом аналізу, що обробляє дані, отримані від систем IDS/IPS; запропоновано схему комбінованого методу аналізу даних від систем IDS/IPS, що поєднує методи сигнатур та політик.

Практична цінність: розроблено алгоритм формування політик, що враховує налаштування домашньої мережі, дружніх та заблокованих IP-адрес; розроблено алгоритм налаштування правил, що використовуються IDS/IPS системою для сканування мережі; розроблено алгоритм формування висновків та рекомендацій на основі результату роботи IDS/IPS системи та попередньо налаштованих політик; розроблено ПЗ, що дозволяє користувачеві налаштовувати політики безпеки та правила для IDS/IPS системи, таким чином полегшуючи взаємодію з нею, а також здатне проводити сканування та аналізувати його результати на основі сформованих користувачем політик.

Загалом розширено методологічну базу методів та засобів аналізу даних отриманих від систем виявлення та запобігання вторгнень, що може стати поштовхом для подальшого застосування комбінованого методу аналізу даних для реалізації програмного забезпечення, що взаємодіє з системами IDS/IPS та обробляє отримані від них дані.

Література

1. IDS проти IPS. Https://instagalleryapp.com. 13.12.2024. URL: https://instagalleryapp.com/chistij-administrator-2/ids-proti-ips-2/ (дата звернення: 01.03.2025).

2. Стасєв, Ю. В. Дослідження систем виявлення та попередження вторгнень у комп'ютерні мережі / Ю. В. Стасєв // Інформаційні технології та комп'ютерна інженерія : зб. тез доп. наук.-практ. конф., 4 груд. 2014 р., м. Кіровоград / М-во освіти і науки України, Кіровоград. нац. техн. ун-т . – Кіровоград: КНТУ, 2014. – С. 185.

3. Рондалєв Д., Мелкозьорова О., Нарєжній О. Особливості функціонування корпоративного міжмережевого екрану та питання взаємодії з системою IDS // Комп'ютерні науки та кібербезпека.

2019. № 3. С. 11-21.

4. Риков О. Порівняльний аналіз систем виявлення і запобігання вторгнень / О. Риков, І. В. Олешко // Global Cyber Security Forum : матеріали Першого міжнародного науково-практичного форуму, 14 – 16 листопада 2019 р. – Харьков : ХНУРЭ, 2019. – С. 88–89.

5. Корзаченко О. В. Методологічні засади щодо вибору IDS/IPS для організацій / О. В. Корзаченко, В. І. Полторак // Моделювання та інформаційні системи в економіці. - 2019. - № 98. - С. 135-146. - Режим доступу: http://nbuv.gov.ua/UJRN/Mise_2019_98_16.

6. Chumachenko K. Study of Snort performance in counteracting port scanning techniques / K. Chumachenko, D. Chumachenko // Безпека інформації. - 2017. - Т. 23, № 1. - С. 15-18. - Режим доступу: http://nbuv.gov.ua/UJRN/bezin_2017_23_1_4.

7. Мостовий М. Е. Аналіз ефективності використання систем виявлення вторгнень для аудиту безпеки : пояснювальна записка до атестаційної роботи здобувача вищої освіти на другому (магістерському) рівні, спеціальність 125 Кібербезпека / М. Е. Мостовий ; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. – Харків, 2020. – 79 с.

8. Ankita Bhutani. Industry Trends. Intrusion Detection System / Intrusion Prevention System (IDS / IPS) [Електронний ресурс] / Ankita Bhutani, Preeti Wadhwani // Global Market Insights. – 2019. – Режим доступу до ресурсу: https://www.gminsights.com/industry-analysis/intrusion-detection-prevention-system-ids-ips-market.

9. Мєшков В. (2023). Аналіз систем інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак. Information Technology: Computer Science, Software Engineering and Cyber Security, (1), 85-92.

10. Калюга, В. В. (2021, December). Моделі виявлення вторгнень в комп'ютерну мережу. In The 7th International scientific and practical conference "Modern directions of scientific research development"(December 22-24, 2021) BoScience Publisher, Chicago, USA. 2021. 880 p. (p. 261).

11. Фесоха, В. (2024). Особливості протистояння оборонного та наступального штучного інтелектів у кіберпросторі. International Science Journal of Engineering & Agriculture, 3(4), 105-114.

12. Кравчук Н. В. Безпечний доступ до серверів інформаційних систем, забезпечений ML-моделлю для блокування шкідливих запитів / Н.В. Кравчук, Т.І. Коробейнікова // Вісник Хмельницького національного університету. – 2024. – Том 341, №5. – С. 327–333.

13. Коробейнікова Т. І. Огляд питання безпечного доступу до ресурсів системи доменних імен / Т.І. Коробейнікова, А. Б. Федчук // Інформаційні технології та комп`ютерна інженерія. – 2024. – № 59(1). – С. 40-53.

14. Waleed, A., Jamali, A. F., & Masood, A. (2022). Which open-source ids? snort, suricata or zeek. Computer Networks, 213, 109116.

15. Wala, F. B., & Cotton, C. (2022). "Off-Label" Use of DNS. Digital Threats: Research and Practice, 3(3), 1-13.

16. Савіцький, Л., Безносенко, С., & Горбач, Р. (2024). Концептуальні погляди на побудову системи захисту від кібератак із застосуванням методів штучного інтелекту в інформаційно-комунікаційних системах. Сучасні інформаційні технології у сфері безпеки та оборони, 49(1), 77-85.

17. Бідюк, О., & Марценко, С. (2025). Методи та засоби інформаційної безпеки іт інфраструктур. Herald of Khmelnytskyi National University. Technical sciences, 347(1), 47-58.

18. Коробейнікова Т.І. Аналіз сучасних відкритих систем виявлення та запобігання вторгнень. / Коробейнікова Т.І., Цар О.О. // International scientific journal «Grail of Science» – 2023. – № 27. – С. 317–325.

19. Коробейнікова Т., Журавель І., Бодак А., & Бороденко Д. (2024). Концепція нульової довіри: сучасні методи забезпечення кібербезпеки в корпоративних мережах. Вісник Львівського державного університету безпеки життєдіяльності, 30, 67-77.

20. Bourhis, P., Reutter, J. L., Suárez, F., & Vrgoč, D. (2017, May). JSON: data model, query languages and schema specification. In Proceedings of the 36th ACM SIGMOD-SIGACT-SIGAI symposium on principles of database systems (pp. 123-135).

References

1. IDS proty IPS. Https://instagalleryapp.com. 13.12.2024. URL: https://instagalleryapp.com/chistij-administrator-2/ids-proti-ips-2/ (data zvernennia: 01.03.2025).

2. Stasiev, Yu. V. Doslidzhennia system vyiavlennia ta poperedzhennia vtorhnen u kompiuterni merezhi / Yu. V. Stasiev // Informatsiini tekhnolohii ta kompiuterna inzheneriia : zb. tez dop. nauk.-prakt. konf., 4 hrud. 2014 r., m. Kirovohrad / M-vo osvity i nauky Ukrainy, Kirovohrad. nats. tekhn. un-t . – Kirovohrad: KNTU, 2014. – S. 185.

3. Rondaliev D., Melkozorova O., Nariezhnii O. Osoblyvosti funktsionuvannia korporatyvnoho mizhmerezhevoho ekranu ta pytannia vzaiemodii z systemoiu IDS // Kompiuterni nauky ta kiberbezpeka. 2019. № 3. C. 11-21.

4. Rykov O. Porivnialnyi analiz system vyiavlennia i zapobihannia vtorhnen / O. Rykov, I. V. Oleshko // Global Cyber Security Forum : materialy Pershoho mizhnarodnoho naukovo-praktychnoho forumu, 14 – 16 lystopada 2019 r. – Kharkov : KhNURЭ, 2019. – S. 88–89.

5. Korzachenko O. V. Metodolohichni zasady shchodo vyboru IDS/IPS dlia orhanizatsii / O. V. Korzachenko, V. I. Poltorak // Modeliuvannia ta informatsiini systemy v ekonomitsi. - 2019. - № 98. - S. 135-146. - Rezhym dostupu: http://nbuv.gov.ua/UJRN/Mise_2019_98_16.

6. Chumachenko K. Study of Snort performance in counteracting port scanning techniques / K. Chumachenko, D. Chumachenko // Bezpeka informatsii. - 2017. - T. 23, № 1. - S. 15-18. - Rezhym dostupu: http://nbuv.gov.ua/UJRN/bezin_2017_23_1_4.

7. Mostovyi M. E. Analiz efektyvnosti vykorystannia system vyiavlennia vtorhnen dlia audytu bezpeky : poiasniuvalna zapyska do atestatsiinoi roboty zdobuvacha vyshchoi osvity na druhomu (mahisterskomu) rivni, spetsialnist 125 Kiberbezpeka / M. E. Mostovyi ; M-vo osvity i nauky Ukrainy, Kharkiv. nats. un-t radioelektroniky. – Kharkiv, 2020. – 79 s.

8. Ankita Bhutani. Industry Trends. Intrusion Detection System / Intrusion Prevention System (IDS / IPS) [Elektronnyi resurs] / Ankita Bhutani, Preeti Wadhwani // Global Market Insights. – 2019. – Rezhym dostupu do resursu: https://www.gminsights.com/industry-analysis/intrusion-detection-prevention-system-ids-ips-market.

9. Mieshkov V. (2023). Analiz system intelektualnoho monitorynhu trafiku kompiuternoi merezhi dlia system vyiavlennia atak. Information Technology: Computer Science, Software Engineering and Cyber Security, (1), 85-92.

10. Kaliuha, V. V. (2021, December). Modeli vyiavlennia vtorhnen v kompiuternu merezhu. In The 7th International scientific and practical conference "Modern directions of scientific research development"(December 22-24, 2021) BoScience Publisher, Chicago, USA. 2021. 880 p. (p. 261).

11. Fesokha, V. (2024). Osoblyvosti protystoiannia oboronnoho ta nastupalnoho shtuchnoho intelektiv u kiberprostori. International Science Journal of Engineering & Agriculture, 3(4), 105-114.

12. Kravchuk N. V. Bezpechnyi dostup do serveriv informatsiinykh system, zabezpechenyi ML-modelliu dlia blokuvannia shkidlyvykh zapytiv / N.V. Kravchuk, T.I. Korobeinikova // Visnyk Khmelnytskoho natsionalnoho universytetu. – 2024. – Tom 341, №5. – S. 327–333.

13. Korobeinikova T. I. Ohliad pytannia bezpechnoho dostupu do resursiv systemy domennykh imen / T.I. Korobeinikova, A. B. Fedchuk // Informatsiini tekhnolohii ta komp`iuterna inzheneriia. – 2024. – № 59(1). – S. 40-53.

14. Waleed, A., Jamali, A. F., & Masood, A. (2022). Which open-source ids? snort, suricata or zeek. Computer Networks, 213, 109116.

15. Wala, F. B., & Cotton, C. (2022). "Off-Label" Use of DNS. Digital Threats: Research and Practice, 3(3), 1-13.

16. Savitskyi, L., Beznosenko, S., & Horbach, R. (2024). Kontseptualni pohliady na pobudovu systemy zakhystu vid kiberatak iz zastosuvanniam metodiv shtuchnoho intelektu v informatsiino-komunikatsiinykh systemakh. Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony, 49(1), 77-85.

17. Bidiuk, O., & Martsenko, S. (2025). Metody ta zasoby informatsiinoi bezpeky it infrastruktur. Herald of Khmelnytskyi National University. Technical sciences, 347(1), 47-58.

18. Korobeinikova T.I. Analiz suchasnykh vidkrytykh system vyiavlennia ta zapobihannia vtorhnen. / Korobeinikova T.I., Tsar O.O. // International scientific journal «Grail of Science» – 2023. – № 27. – S. 317–325.

19. Korobeinikova T., Zhuravel I., Bodak A., & Borodenko D. (2024). Kontseptsiia nulovoi doviry: suchasni metody zabezpechennia kiberbezpeky v korporatyvnykh merezhakh. Visnyk Lvivskoho derzhavnoho universytetu bezpeky zhyttiediialnosti, 30, 67-77.

20. Bourhis, P., Reutter, J. L., Suárez, F., & Vrgoč, D. (2017, May). JSON: data model, query languages and schema specification. In Proceedings of the 36th ACM SIGMOD-SIGACT-SIGAI symposium on principles of database systems (pp. 123-135).