DOI: https://doi.org/10.32626/2309-9763.2026-40-177-187
УДК 378.004.056

Коновалов Олексій Юрійович,
кандидат технічних наук,
доцент кафедри кібербезпеки Національної академії СБ України,
Київ, Україна
ORCID ID: https://orcid.org/0000-0002-3772-3654
alex_metapost@meta.ua

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ SNORT, SURICATA ТА AI-IDS У ПРАКТИЧНІЙ ПІДГОТОВЦІ ЗДОБУВАЧІВ ОСВІТИ ЗА СПЕЦІАЛЬНІСТЮ «КІБЕРБЕЗПЕКА»

Анотація. У процесі дослідження автором проаналізовано можливості використання сучасних систем виявлення вторгнень Snort, Suricata та AI-IDS у практичній підготовці здобувачів освіти за спеціальністю «Кібербезпека». Особливу увагу приділено обґрунтуванню доцільності інтеграції сигнатурних та інтелектуальних систем аналізу мережевого трафіку в освітній процес з метою наближення професійної підготовки до реальних умов функціонування сучасних корпоративних інформаційних систем. Зазначено, що стрімкий розвиток цифрових технологій, поширення хмарних сервісів, Інтернету речей, штучного інтелекту та складних розподілених мережевих інфраструктур супроводжується постійним зростанням кількості кіберзагроз і висуває нові вимоги до професійної підготовки майбутніх спеціалістів з кібербезпеки. Актуальність дослідження зумовлена необхідністю вдосконалення практико-орієнтованої складової освітнього процесу та формування у здобувачів освіти сучасних професійних компетентностей, пов'язаних із виявленням, аналізом і запобіганням мережевим атакам. У роботі розглянуто роль систем виявлення вторгнень у структурі сучасної кібербезпеки, їх використання під час вивчення професійно орієнтованих дисциплін та виконання лабораторних робіт. Детально проаналізовано функціональні можливості систем Snort і Suricata, визначено їх переваги для формування практичних навичок аналізу мережевого трафіку, створення правил детектування атак та роботи із сучасними платформами моніторингу інформаційної безпеки. Окрему увагу приділено інтелектуальним системам AI-IDS, які використовують алгоритми машинного навчання та штучного інтелекту для виявлення поведінкових аномалій і невідомих кіберзагроз. За результатами проведеного дослідження встановлено, що використання Snort сприяє формуванню базових професійних компетентностей у сфері сигнатурного аналізу мережевого трафіку, Suricata забезпечує розвиток практичних навичок роботи з високопродуктивними багатопотоковими системами моніторингу, тоді як AI-IDS створює умови для опанування сучасних технологій машинного навчання та аналізу великих масивів даних у сфері кібербезпеки. Обґрунтовано доцільність комплексного використання зазначених програмних засобів у професійній підготовці майбутніх фахівців, оскільки їх інтеграція дозволяє сформувати цілісну

ISSN 2309-9763 https://doi.org/10.32626/2309-9763.2026-40

систему професійних компетентностей, необхідних для ефективної діяльності в умовах сучасного цифрового середовища.

Ключові слова: кібербезпека; професійна підготовка; Snort; Suricata; AI-IDS; системи виявлення вторгнень; машинне навчання; практико-орієнтоване навчання.

1. ВСТУП / INTRODUCTION

Постановка проблеми. У сучасних умовах ринок праці потребує не лише спеціалістів, які володіють теоретичними знаннями з інформаційної безпеки, але й фахівців, здатних працювати із сучасними системами моніторингу та аналізу мережевого трафіку, здійснювати виявлення кіберзагроз, аналізувати журнали подій безпеки та приймати оперативні рішення щодо реагування на інциденти. Саме тому особливої актуальності набуває інтеграція сучасних систем виявлення вторгнень (Intrusion Detection Systems, IDS) у процес професійної підготовки майбутніх спеціалістів з кібербезпеки. Сучасні корпоративні мережі стикаються зі зростаючою кількістю складних кіберзагроз, серед яких APT-атаки, експлуатація вразливостей нульового дня, фішингові кампанії та атаки на ланцюги постачання програмного забезпечення. Традиційні сигнатурні системи виявлення вторгнень забезпечують високу точність виявлення відомих атак, однак демонструють обмежену ефективність щодо нових або модифікованих загроз. У зв'язку з цим особливого значення набувають системи виявлення вторгнень на основі методів машинного навчання та штучного інтелекту, здатні виявляти аномалії та невідомі патерни поведінки мережевого трафіку. Стрімка цифровізація бізнес-процесів, активне впровадження хмарних технологій, концепцій Industry 4.0, Інтернету речей (IoT), штучного інтелекту та розподілених корпоративних інформаційних систем суттєво трансформували сучасний ландшафт кібербезпеки. Корпоративні мережі сьогодні виступають критично важливою інфраструктурою для функціонування державних установ, фінансового сектору, промислових підприємств та IT-компаній, що робить їх привабливою ціллю для різноманітних кіберзлочинних угруповань. За даними міжнародних аналітичних агентств, щороку кількість кібератак демонструє стійку тенденцію до зростання, а самі атаки стають дедалі складнішими, багаторівневими та менш помітними для традиційних засобів захисту.

Аналіз останніх досліджень і публікацій. Окремі аспекти професійної підготовки майбутніх фахівців за спеціальністю «Кібербезпека» знайшли відображення у працях вітчизняних науковців, зокрема Н. Котенко, Т. Жирової, О. Коновалова, Л. Харлай та інших дослідників. У їхніх роботах висвітлено питання формування професійних компетентностей, розвитку цифрової грамотності, практико-орієнтованої підготовки, використання сучасних інформаційно-комунікаційних технологій та впровадження компетентнісного підходу у процес професійної освіти майбутніх фахівців з кібербезпеки. Значний внесок у розвиток теоретичних і прикладних аспектів побудови інтелектуальних систем кіберзахисту

зробили В. Сталлінгс (W. Stallings), Б. Шнайєр (B. Schneier), Е. Скілліс (E. Skoudis), М. Роеш (M. Roesch), який є розробником системи Snort, а також дослідники у сфері штучного інтелекту та машинного навчання І. Гудфеллоу (I. Goodfellow), Й. Лекун (Y. LeCun) та Д. Сільвер (D. Silver). Їхні праці заклали наукове підґрунтя для створення сучасних засобів моніторингу мережевого трафіку, аналізу аномальної поведінки та автоматизованого реагування на кіберінциденти. Сучасні дослідження у сфері захисту інформації формують важливу теоретичну та практичну базу для подальшого вдосконалення систем виявлення вторгнень, розроблення інтелектуальних моделей аналізу мережевого трафіку та підвищення рівня кіберстійкості корпоративних мереж. Особливий інтерес викликають роботи, присвячені інтеграції методів машинного навчання та штучного інтелекту в архітектуру сучасних IDS та IPS. Зокрема, у праці «AI-driven Cybersecurity: An Overview, Security Analysis Modeling and Research Directions» автори Аліреза Могімі (Alireza Moghimi), Ян Віхельманн (Jan Wichelmann), Томас Айзенбарт (Thomas Eisenbarth) та Берк Сунар (Berk Sunar) здійснюють комплексний аналіз сучасних підходів до застосування технологій штучного інтелекту в кібербезпеці. У дослідженні розглядаються можливості використання алгоритмів машинного та глибокого навчання для автоматизованого аналізу подій інформаційної безпеки, виявлення мережевих аномалій, класифікації атак та прогнозування потенційних кіберзагроз.

Водночас аналіз сучасної наукової літератури свідчить, що недостатньо дослідженим залишається питання використання сучасних систем виявлення вторгнень, зокрема Snort, Suricata та AI-IDS, як засобу формування професійних компетентностей здобувачів освіти. Зокрема, потребують подальшого наукового обґрунтування педагогічні умови інтеграції зазначених програмно-апаратних комплексів у освітній процес, їхній вплив на розвиток практичних навичок аналізу мережевого трафіку, виявлення кіберзагроз, роботи із засобами моніторингу інформаційної безпеки та застосування технологій штучного інтелекту для розв'язання професійних завдань.

2. МЕТА ТА ЗАВДАННЯ / AIM AND TASKS

Метою дослідження є теоретичне обґрунтування та аналіз можливостей використання сучасних систем виявлення вторгнень Snort, Suricata та AI-IDS у процесі формування професійних компетентностей майбутніх фахівців з кібербезпеки, а також визначення їхнього дидактичного потенціалу для розвитку практичних навичок аналізу мережевого трафіку, виявлення кіберзагроз та застосування технологій штучного інтелекту в професійній діяльності.

Реалізація мети передбачає вирішення таких **завдань**: розкрити особливості функціонування та архітектурні принципи сучасних систем виявлення вторгнень Snort, Suricata та AI-IDS; дослідити можливості використання сигнатурних та інтелектуальних систем виявлення вторгнень як засобів формування професійних компетентностей здобувачів освіти; визначити роль технологій машинного навчання

ISSN 2309-9763 https://doi.org/10.32626/2309-9763.2026-40

та штучного інтелекту у розвитку практичних навичок майбутніх фахівців з кібербезпеки.

3. МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ / RESEARCH METHODOLOGY

Методологічну основу дослідження становлять положення компетентнісного, системного підходів до професійної підготовки майбутніх фахівців з кібербезпеки. У ході дослідження використано комплекс загальнонаукових теоретичних методів, зокрема аналіз, синтез, порівняння, узагальнення та систематизацію вітчизняних і зарубіжних наукових праць, присвячених проблемам професійної підготовки майбутніх фахівців з кібербезпеки, використанню сучасних систем виявлення вторгнень, а також застосуванню технологій машинного навчання та штучного інтелекту в освітньому процесі. Порівняльний аналіз функціональних можливостей систем Snort, Suricata та AI-IDS дозволив визначити їхній дидактичний потенціал та обґрунтувати доцільність використання зазначених програмних засобів для формування професійних компетентностей майбутніх фахівців з кібербезпеки.

4. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ / RESEARCH RESULTS

Стрімкий розвиток інформаційно-комунікаційних технологій, активна цифровізація всіх сфер суспільного життя та широке впровадження хмарних сервісів, штучного інтелекту й розподілених інформаційних систем суттєво змінюють вимоги до професійної підготовки майбутніх фахівців з кібербезпеки [1]. У сучасних умовах недостатньо володіти лише базовими теоретичними знаннями про принципи функціонування комп'ютерних мереж та засоби їх захисту. Ринок праці потребує висококваліфікованих спеціалістів, здатних оперативно виявляти та аналізувати кіберзагрози, здійснювати моніторинг мережевої інфраструктури й застосовувати сучасні технології протидії кібератакам. У зв'язку зі зростанням кількості цифрових сервісів та ускладненням сучасних інформаційних систем особливого значення набуває формування у здобувачів освіти практичних професійних компетентностей у сфері виявлення та аналізу мережевих загроз. Одним із найбільш ефективних засобів реалізації такого практико-орієнтованого підходу є використання систем виявлення вторгнень (Intrusion Detection Systems, IDS), які забезпечують моніторинг мережевого трафіку, аналіз подій інформаційної безпеки та своєчасне виявлення підозрілої активності. Інтеграція сучасних систем IDS у професійну підготовку майбутніх фахівців з кібербезпеки створює умови для розвитку їхніх аналітичних здібностей, критичного мислення, навичок роботи з мережевими журналами подій та формування готовності до практичного вирішення реальних завдань забезпечення кібербезпеки. Таким чином, використання систем виявлення вторгнень виступає не лише сучасним технологічним інструментом захисту інформаційних систем, а й ефективним засобом формування професійних компетентностей здобувачів освіти відповідно до вимог цифрового суспільства та сучасного ринку праці.

ISSN 2309-9763 https://doi.org/10.32626/2309-9763.2026-40

Сучасний кіберпростір характеризується значною різноманітністю атак, які використовують як технічні, так і соціально-інженерні методи проникнення. Одними з найбільш поширених залишаються атаки типу DoS (Denial of Service) та DDoS (Distributed Denial of Service) [5]. Їх метою є перевантаження серверів або мережевих ресурсів великою кількістю запитів, що призводить до відмови в обслуговуванні легітимних користувачів. Особливу небезпеку становлять розподілені DDoS-атаки, які здійснюються одночасно з тисяч заражених пристроїв ботнету. Іншим поширеним типом загроз є сканування портів (Port Scanning). Воно використовується для збору інформації про активні сервіси та відкриті порти корпоративної мережі. Отримані відомості часто стають основою для подальшої експлуатації вразливостей. Значну частку сучасних атак становлять спроби brute-force, під час яких зловмисник автоматизовано підбирає паролі або криптографічні ключі. Особливо вразливими є сервіси віддаленого доступу, VPN-шлюзи та SSH-сервери. Окрему категорію становлять експлойти, які використовують програмні помилки або вразливості нульового дня (Zero-Day). Саме вони дозволяють отримати несанкціонований доступ до інформаційних систем до моменту встановлення відповідних оновлень безпеки [4].

Після первинного проникнення до мережі кіберзлочинці часто здійснюють так званий lateral movement — горизонтальне переміщення між вузлами корпоративної мережі з метою підвищення привілеїв та пошуку цінної інформації. Заключним етапом багатьох сучасних APT-атак є встановлення каналів Command and Control (C2), які забезпечують приховане дистанційне керування зараженими пристроями та передачу викрадених даних [2].

Системи виявлення вторгнень є одним із ключових елементів сучасної багаторівневої архітектури інформаційної безпеки. Основним завданням IDS є аналіз мережевого трафіку та генерація повідомлень про потенційно небезпечні події. На відміну від IDS, системи IPS (Intrusion Prevention System) не лише виявляють атаки, але й автоматично блокують підозрілий трафік, запобігаючи розвитку кіберінциденту. Варто зазначити, що сучасні корпоративні мережі дедалі частіше використовують SIEM (Security Information and Event Management) – платформи централізованого збору, кореляції та аналізу подій безпеки. SIEM-системи отримують журнали подій від IDS, IPS, міжмережевих екранів та інших компонентів інфраструктури, що дозволяє формувати комплексну картину кіберзагроз [3].

Новим етапом розвитку систем кіберзахисту стали платформи XDR (Extended Detection and Response), які забезпечують інтегрований аналіз подій із мережевих пристроїв, серверів, робочих станцій, хмарних сервісів та кінцевих точок, використовуючи елементи штучного інтелекту для автоматизованого реагування.

Однією з найпоширеніших відкритих систем IDS є Snort, яка була викуплена компанією Cisco і широко використовується для моніторингу мережевого трафіку. Архітектура Snort складається з кількох основних модулів:

1. Першим є Packet Decoder, який виконує декодування мережевих пакетів різних протоколів (Ethernet, IP, TCP, UDP, ICMP).

ISSN 2309-9763 https://doi.org/10.32626/2309-9763.2026-40

2. Далі інформація передається до блоку Preprocessors, який здійснює нормалізацію трафіку, дефрагментацію пакетів та виявлення аномалій на початковому рівні.

3. Основним компонентом системи виступає Detection Engine. Саме він порівнює мережевий трафік із базою сигнатур та правил виявлення атак. У разі збігу формується повідомлення про інцидент.

4. Заключним є модуль Logging and Alerting, який забезпечує ведення журналів подій та передачу повідомлень адміністраторам або зовнішнім системам SIEM.

Перевагами Snort є велика база сигнатур, простота налаштування та широке використання у професійному середовищі. Недоліком залишається обмежена масштабованість та відсутність повноцінної багатопотокової архітектури.

Система Suricata була створена як сучасна альтернатива Snort із підтримкою високопродуктивної обробки мережевого трафіку. Головною особливістю Suricata є багатопотокова архітектура, яка дозволяє ефективно використовувати багатоядерні процесори та забезпечувати аналіз трафіку на високошвидкісних каналах передачі даних.

Suricata підтримує одночасне функціонування в режимах IDS та IPS, що робить її універсальним засобом кіберзахисту. Важливою перевагою системи є підтримка сучасних мережевих протоколів та можливість глибокого аналізу прикладного рівня (HTTP, TLS, DNS, SMB тощо). Крім того, Suricata легко інтегрується з платформами Zeek, Elastic Stack, Kibana та Elasticsearch, що дозволяє реалізувати централізований моніторинг та візуалізацію подій безпеки. Завдяки підтримці правил Snort та високій продуктивності Suricata дедалі частіше використовується у великих корпоративних мережах і центрах обробки даних. Традиційні сигнатурні системи демонструють високу точність лише щодо відомих атак. Саме тому останніми роками активно розвиваються системи AI-IDS, які використовують алгоритми машинного навчання для виявлення аномальної поведінки.

Одним із найпростіших методів є Decision Tree (дерево рішень), яке будує модель класифікації на основі послідовності логічних правил. Перевагою є висока швидкість роботи та простота інтерпретації результатів.

Більш складним є алгоритм Random Forest, який базується на побудові безлічі окремих дерев рішень, усереднюючи прогнози окремих дерев для отримання максимально точного та стабільного результату.

Також використовується Support Vector Machine (SVM), метод опорних векторів – це потужний алгоритм машинного навчання, який використовується для класифікації, регресії та виявлення викидів. Він працює шляхом знаходження оптимальної «гіперплощини» (межі прийняття рішення), яка розділяє різні класи даних у N-вимірному просторі з максимально можливим запасом. Метод дозволяє знаходити оптимальну межу між нормальним і аномальним трафіком навіть у багатовимірному просторі ознак.

Перспективним напрямом є використання Convolutional Neural Networks (CNN), які здатні автоматично виділяти складні закономірності в мережевих даних та демонструють високу ефективність при аналізі великих потоків інформації.

ISSN 2309-9763 https://doi.org/10.32626/2309-9763.2026-40

Для аналізу часових залежностей мережевого трафіку широко використовуються рекурентні нейронні мережі типу Long Short-Term Memory (LSTM). Вони дозволяють виявляти складні сценарії багатокрокових атак та моделювати поведінку користувачів у корпоративній мережі. Порівняльний аналіз сучасних систем виявлення вторгнень зведений у Таблицю 1.

Таблиця 1.

Порівняльний аналіз сучасних систем виявлення вторгнень

Критерій	Snort	Suricata	AI-IDS
Відомі атаки	Висока	Висока	Висока–середня
Zero-Day атаки	Низька	Низька	Висока
Пояснюваність результатів	Висока	Висока	Середня
Адаптація до нових загроз	Низька	Низька	Висока

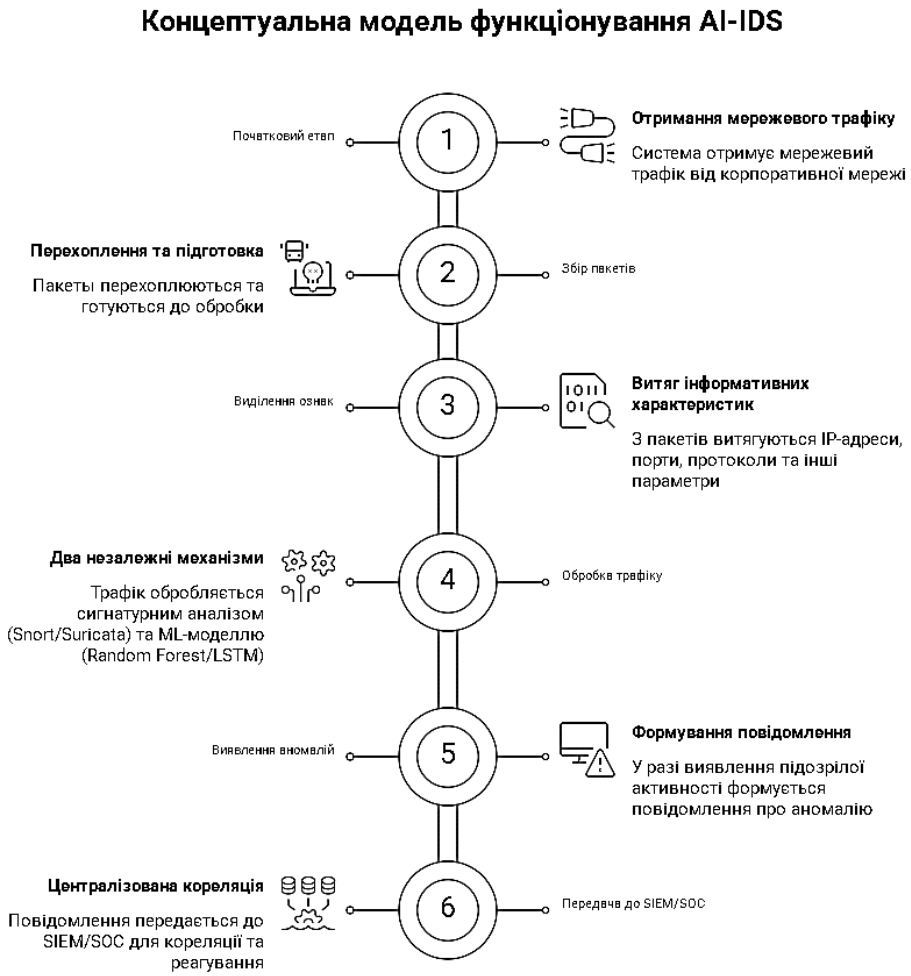

Рис.1. *Концептуальна модель AI-IDS*

ISSN 2309-9763 https://doi.org/10.32626/2309-9763.2026-40

Рисунок 1 ілюструє концептуальну модель функціонування інтелектуальної системи виявлення вторгнень (AI-IDS), побудованої на основі поєднання традиційного сигнатурного аналізу та алгоритмів машинного навчання. На початковому етапі система отримує мережевий трафік, який надходить від корпоративної мережевої інфраструктури. Далі відбувається збір пакетів, тобто їх перехоплення та підготовка до подальшої обробки. Наступним кроком є виділення ознак, під час якого з пакетів витягуються найбільш інформативні характеристики: IP-адреси, номери портів, типи протоколів, розміри пакетів, часові інтервали та інші параметри мережевого потоку. Після цього трафік обробляється двома незалежними механізмами. Перший передбачає використання класичних сигнатурних систем Snort або Suricata, які здійснюють пошук відомих шаблонів атак. Другий ґрунтується на застосуванні ML-моделі (Random Forest або LSTM), що виконує поведінковий аналіз і дозволяє виявляти аномалії та нові типи кіберзагроз. У разі виявлення підозрілої активності формується повідомлення про аномалію, яке передається до центру моніторингу SIEM/SOC. Саме цей модуль забезпечує централізовану кореляцію подій інформаційної безпеки, накопичення журналів та підтримку процесу прийняття рішень щодо реагування на інциденти. Запропонована модель поєднує переваги сигнатурного та інтелектуального аналізу, що дозволяє підвищити ефективність захисту сучасних корпоративних мереж від відомих і невідомих кібератак.

5. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ / CONCLUSIONS AND PROSPECTS FOR FURTHER RESEARCH

Проведений аналіз сучасних систем виявлення вторгнень дає підстави стверджувати, що в умовах стрімкого розвитку цифрових технологій та постійного ускладнення кіберзагроз особливого значення набуває практико-орієнтована підготовка майбутніх фахівців з кібербезпеки. Сучасне освітнє середовище повинно забезпечувати не лише засвоєння теоретичних знань про принципи функціонування інформаційних систем, а й формування професійних компетентностей, необхідних для аналізу, виявлення та запобігання сучасним кіберінцидентам. Порівняльний аналіз показав, що система Snort залишається одним із найбільш доступних і ефективних інструментів для формування базових професійних компетентностей майбутніх фахівців з кібербезпеки. Завдяки використанню сигнатурного аналізу здобувачі освіти отримують можливість ознайомитися з принципами роботи сучасних засобів моніторингу мережевого трафіку, створенням власних правил детектування та аналізом типових сценаріїв атак. Водночас встановлено, що використання Suricata має додатковий дидактичний потенціал завдяки підтримці багатопотокової архітектури, можливості функціонування в режимах IDS та IPS, а також інтеграції з платформами Zeek, Elastic Stack і сучасними SIEM-рішеннями. Робота із зазначеним програмним забезпеченням сприяє формуванню у здобувачів освіти комплексного бачення сучасної архітектури корпоративних систем кіберзахисту та розвитку навичок роботи із високошвидкісними мережевими середовищами. Особливу увагу в дослідженні приділено використанню інтелектуальних систем виявлення вторгнень (AI-IDS) як

інноваційного засобу професійної підготовки майбутніх фахівців з кібербезпеки. Використання алгоритмів машинного навчання та штучного інтелекту, зокрема Decision Tree, Random Forest, SVM, CNN та LSTM, дозволяє здобувачам освіти опановувати сучасні методи аналізу великих масивів даних, виявлення поведінкових аномалій та прогнозування потенційних кіберзагроз. Це, своєю чергою, сприяє розвитку критичного мислення, аналітичних здібностей та готовності до роботи в умовах швидкої трансформації цифрового середовища. Проведений аналіз дозволяє зробити висновок, що жодна із розглянутих систем окремо не забезпечує повного формування всього спектра професійних компетентностей майбутнього фахівця з кібербезпеки. Саме тому найбільш перспективним напрямом удосконалення освітнього процесу є комплексне використання Snort, Suricata та AI-IDS у межах практичної підготовки здобувачів освіти. Поєднання сигнатурних та інтелектуальних підходів створює умови для формування інтегрованих професійних компетентностей, розвитку навичок аналізу кіберзагроз та підготовки конкурентоспроможних спеціалістів, здатних ефективно діяти в умовах сучасних викликів інформаційної безпеки.

Перспективу подальших досліджень убачаються у розробленні методичних моделей інтеграції систем Snort, Suricata та AI-IDS у практичну підготовку здобувачів спеціальності «Кібербезпека та захист інформації».

6. СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ТРАНСЛІТЕРАЦІЯ / REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Єсін, В., Вілігура, В., Сватовський, І., 2023. Забезпечення безпеки у розподілених інформаційних системах: основні аспекти. Радіотехніка, *3*(214), 32–64.

2. Коробейнікова, Т.І., Журавель, І.М., Бодак, А.О., Бороденко, Д.В., 2024. Концепція нульової довіри: сучасні методи забезпечення кібербезпеки в корпоративних мережах. *Вісник Львівського державного університету безпеки життєдіяльності*, 30, 67-77.

3. Опанович, М., 2024. Аналіз кібератак та діяльності APT груп в Україні. *Кібербезпека: освіта, наука, техніка, 4*(24), 172–184.

4. Шкітов, А., 2024. Синтез типових алгоритмів захисту інформації в корпоративних мережах. *Управління розвитком складних систем*, 60, 129-135.

5. Pooja, S., & Chandrakala, C., 2024. Secure Reviewing and Data Sharing in Scientific Collaboration: Leveraging Blockchain and Zero TrustArchitecture. *IEEE Access*, 12, 92386–92399.

Під час написання окремих фрагментів статті застосовувалися інструменти генеративного штучного інтелекту з метою стилістичної перевірки й удосконалення мовного оформлення тексту. Автор самостійно здійснювad добір джерел, аналіз наукової літератури, інтерпретацію результатів дослідження та формулювання висновків.

ISSN 2309-9763 https://doi.org/10.32626/2309-9763.2026-40

THE USE OF SNORT, SURICATA AND AI-IDS TECHNOLOGIES IN THE PRACTICAL TRAINING OF STUDENTS STUDYING «CYBERSECURITY»

Oleksiy Konovalov,
Candidate of Technical Sciences,
Associate Professor of Cybersecurity,
National Academy of the Security Service of Ukraine,
Kyiv, Ukraine
ORCID ID: https://orcid.org/0000-0002-3772-3654
alex_metapost@meta.ua

Abstract. In this study, the author analyses the potential for using modern intrusion detection systems – Snort, Suricata and AI-IDS – in the practical training of students specialising in 'Cybersecurity'. Particular attention is paid to justifying the feasibility of integrating signature-based and intelligent network traffic analysis systems into the educational process, with the aim of bringing professional training closer to the real-world conditions of modern corporate information systems. It is noted that the rapid development of digital technologies, the proliferation of cloud services, the Internet of Things, artificial intelligence and complex distributed network infrastructures is accompanied by a constant increase in the number of cyber threats and places new demands on the professional training of future cybersecurity specialists. The relevance of the study stems from the need to improve the practice-oriented component of the educational process and to equip students with modern professional competencies related to the detection, analysis and prevention of network attacks. The paper examines the role of intrusion detection systems within the framework of modern cybersecurity, and their use in the study of professionally oriented disciplines and the completion of laboratory work. The functional capabilities of the Snort and Suricata systems have been analysed in detail, and their benefits have been identified in terms of developing practical skills in network traffic analysis, creating attack detection rules, and working with modern information security monitoring platforms. Particular attention is paid to AI-IDS systems, which use machine learning and artificial intelligence algorithms to detect behavioural anomalies and unknown cyber threats. The results of the study indicate that the use of Snort facilitates the development of basic professional competencies in the field of signature-based network traffic analysis, whilst Suricata enables the development of practical skills in working with high-performance multi-threaded monitoring systems, whilst AI-IDS creates the conditions for mastering modern machine learning technologies and the analysis of large datasets in the field of cybersecurity. The feasibility of the comprehensive use of these software tools in the professional training of future specialists is substantiated, as their integration allows for the formation of a holistic system of professional competencies necessary for effective work in the modern digital environment.

Keywords: cybersecurity; professional training; Snort; Suricata; AI-IDS; intrusion detection systems; machine learning; practice-oriented learning.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Lesin, V., Vilihura, V., & Svatovskyi, I., 2023. Zabezpechennia bezpeky u rozpodilenykh informatsiinykh systemakh: osnovni aspekty [Security in distributed information systems: key aspects]. *Radiotekhnika, 3*(214), *32–64.*

2. Korobeinikova, T.I., Zhuravel, I.M., Bodak, A.O., & Borodenko, D.V., 2024. Kontseptsiia nulovoi doviry: suchasni metody zabezpechennia kiberbezpeky v korporatyvnykh merezhakh [The zero-trust concept: modern methods of ensuring cybersecurity in corporate networks]. *Visnyk Lvivskoho derzhavnoho universytetu bezpeky zhyttiediialnosti, 30,* 67-77.

3. Opanovych, M., 2024. Analiz kiberatak ta diialnosti APT hrup v Ukraini [Analysis of cyberattacks and the activities of APT groups in Ukraine]. *Kiberbezpeka: osvita, nauka, tekhnika, 4*(24), 172–184.

4. Shkitov, A., 2024. Syntez typovykh alhorytmiv zakhystu informatsii v korporatyvnykh merezhakh [Synthesis of typical information protection algorithms in corporate networks]. *Upravlinnia rozvytkom skladnykh system, 60,* 129-135*.*

5. Pooja, S., & Chandrakala, C., 2024. Secure Reviewing and Data Sharing in Scientific Collaboration: Leveraging Blockchain and Zero Trust. *Architecture. IEEE Access,* 12, 92386–92399*.*

Дата першого подання статті до публікації: 03.03.2026
Дата прийняття статті до публікації після рецензування: 04.04.2026
Дата публікації: 29.05.2026

DOI: https://doi.org/10.32626/2309-9763.2026-40-187-200
УДК 37.011.3-051(377.36)+37.091.12:78.071.2+781.65

Лабунець Віктор Миколайович,
доктор педагогічних наук, професор, професор кафедри музичного мистецтва,
Кам'янець-Подільський національний університет імені Івана Огієнка,
Кам'янець-Подільський, Україна
ORCID ID: https://orcid.org/0000-0002-9154-0955
gitaraclassic@gmail.com

Карташова Жанна Юріївна,
кандидат педагогічних наук, доцент, доцент кафедри музичного мистецтва,
Кам'янець-Подільський національний університет імені Івана Огієнка,
Кам'янець-Подільський, Україна
ORCID ID: https://orcid.org/0000-0001-7368-9249
lab_ioanna@ukr.net

ПСИХОЛОГО-ПЕДАГОГІЧНІ ОСОБЛИВОСТІ РОЗВИТКУ ІМПРОВІЗАЦІЙНИХ УМІНЬ СТУДЕНТА-ІНСТРУМЕНТАЛІСТА В ПРОЦЕСІ ФАХОВОЇ ПІДГОТОВКИ

Анотація. У статті здійснено комплексний аналіз психолого-педагогічних особливостей розвитку імпровізаційних умінь студентів-інструменталістів у