КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1034
УДК 004.8:004.421

Чернящук Наталія Леонідівна
д.пед.н., професор
Волинський національний університет імені Лесі Українки, Луцьк, Україна
ORCID: 0000-0002-3178-8377
cherniashchuk.nataliia@vnu.edu.ua

ВИКОРИСТАННЯ ІНДИКАТОРІВ КОМПРОМЕТАЦІЇ ДЛЯ ВИЯВЛЕННЯ КІБЕРАТАК

Анотація. У роботі проведено всебічний аналіз систем виявлення та запобігання вторгненням (IDS та IPS), що дозволило оцінити їх ефективність у виявленні різних типів кібератак, включаючи ті, що здійснюються через приховані канали зв'язку. Особлива увага приділена вивченню природи стеганографічних каналів, які ускладнюють детекцію атак, а також факторів, що впливають на їхнє виявлення, таких як динаміка мережевого трафіку та особливості поведінки атакуючих. Досліджено індикатори атак, сформовані за допомогою методів штучного інтелекту на основі аналізу мережевого трафіку, що дозволяє підвищити точність та швидкість виявлення шкідливої активності.

Оцінено можливості платформи Splunk Machine для побудови моделей виявлення атак та аналізу аномальної поведінки у мережах, а також розроблено класифікатори для створення системи виявлення вторгнень на основі методів машинного навчання. У рамках дослідження запропоновано архітектуру системи, обрано оптимальний набір даних для навчання моделі, усунуто дисбаланс класів, визначено та відібрано найбільш значущі ознаки, а також здійснено зменшення простору ознак для підвищення ефективності та швидкодії моделі. Проведено налаштування та тестування моделі, оцінено її ефективність на основі отриманих результатів, що підтверджує практичну застосовність підходу для виявлення реальних кібератак.

Мета дослідження полягає у вивченні потенціалу застосування штучного інтелекту для виявлення вразливостей у мережевій інфраструктурі на основі індикаторів компрометації, враховуючи специфіку прихованих каналів зв'язку, динаміку поведінки атакуючих та обмеження традиційних статистичних методів. Отримані результати можуть бути використані для вдосконалення існуючих систем кібербезпеки та створення ефективних засобів раннього виявлення складних атак.

Ключові слова: системи виявлення вторгнень (IDS), системи запобігання вторгненням (IPS), методи машинного навчання штучного інтелекту, інструмент Splunk для аналітики подій безпеки – основні компоненти сучасних рішень у галузі кібербезпеки.

ВСТУП

У сучасних умовах швидкого зростання кількості та складності кіберзагроз особливо важливим стає застосування технологій для виявлення та прогнозування атак на мережеву інфраструктуру. Сучасні атаки є надзвичайно динамічними, адаптують свою поведінку в реальному часі, маскуються під легітимну активність і часто здійснюються через приховані канали зв'язку, включаючи стеганографічні канали. Це значно ускладнює їхнє виявлення за допомогою традиційних засобів, що базуються на статичних сигнатурах або простому порівнянні статистики трафіку з еталонними шаблонами [1; 2; 3].

Більш того, ідеальні моделі виявлення, які ґрунтуються на відхиленнях статистики переданих повідомлень від середніх характеристик порожніх контейнерів, неефективні у реальних системах приховування інформації. Атакуючі можуть використовувати

© Н. Л. Чернящук, 2026

нестійкі джерела, спеціально сформовані контейнери або вводити шум у канал зв'язку для імітації нормальної активності, що робить надійне виявлення передачі прихованої інформації неможливим із застосуванням традиційних засобів.

Водночас мережеві системи генерують великі обсяги даних, створюючи сприятливі умови для застосування сучасних методів аналізу. Технології аналізу трафіку можуть автоматично обробляти дані, виявляти аномалії, розпізнавати характерні шаблони поведінки атак і визначати індикатори компрометації (IoC) – артефакти, що залишаються в системі після шкідливої діяльності.

Отже, дослідження методів виявлення атак на основі IoC є надзвичайно актуальним, оскільки дозволяє ефективно ідентифікувати загрози, що залишаються непоміченими традиційними засобами захисту [4, 5, 6].

Завдання дослідження включають аналіз принципів роботи систем виявлення та запобігання вторгненням (IDS/IPS) та їхніх обмежень у контексті прихованих атак; вивчення природи стеганографічних каналів та факторів, що впливають на їхнє виявлення; оцінку ефективності використання платформи Splunk Machine для виявлення аномалій; а також проєктування та оптимізацію моделі машинного навчання.

Постановка проблеми. В умовах швидкої цифрової трансформації в різних економічних секторах, активної цифровізації державного управління, охорони здоров'я, освіти та науки, а також зростання популярності інтернет-сервісів і мобільних пристроїв, захист мобільних мереж стає дедалі більш актуальним.

Сучасне суспільство все більше залежить від безперебійної роботи мобільного зв'язку, який забезпечує доступ до критично важливих послуг, банківських операцій, обміну конфіденційною інформацією та підтримки життєво важливої інфраструктури. У зв'язку з цим атакуючі все частіше націлюються на мобільні мережі, використовуючи як відомі вразливості, так і нові, менш вивчені вектори атак.

З поширенням джерел атак і зростанням складності методів кіберзагроз своєчасне виявлення різноманітних кіберзагроз стає все складнішим. Кібернапади стають більш таргетованими, багаторівневими та прихованими, що ускладнює їхнє виявлення традиційними методами. Наприклад, атакуючі можуть поєднувати соціальну інженерію, шкідливе програмне забезпечення, експлойти протоколів та навіть атаки на основі штучного інтелекту. Такі методи дозволяють обходити системи безпеки та залишатися непоміченими протягом тривалого часу.

Традиційні підходи до виявлення атак у мережі, що здебільшого базуються на статичних правилах, таких як аналіз сигнатур, чорні списки або регулярні вирази, є недостатньо гнучкими та неефективними для раннього виявлення аномалій і швидкого реагування на інциденти. Вони часто не можуть адаптуватися до нових або змінених форм атак, які ще не внесені до баз даних сигнатур, і генерують велику кількість хибнопозитивних та хибнонегативних спрацьовувань, перевантажуючи аналітиків із кібербезпеки та знижуючи загальну ефективність захисту. У результаті зростає інтерес до розробки інтелектуальних систем виявлення вторгнень на основі машинного навчання, поведінкового аналізу, індикаторів компрометації (IoC) та індикаторів атак (IoA). Такі підходи дозволяють створювати більш адаптивні та ефективні системи виявлення, здатні своєчасно реагувати на нові, раніше невідомі загрози, виявляти аномальну активність на ранніх стадіях та зменшувати ризик компрометації критично важливих ресурсів [7, 8].

Для подолання цих обмежень застосовуються алгоритми машинного навчання, що відкриває нові можливості для точнішого виявлення шкідливої активності в інформаційних мережах. У цьому дослідженні була застосована платформа аналітики

даних Splunk, що дозволила створювати, навчати, тестувати та оцінювати класифікатори для виявлення мережевих атак.

Ефективність моделі оцінювалася за допомогою чотирьох популярних алгоритмів машинного навчання – дерева рішень, методу опорних векторів (SVM), випадкового лісу та подвійного випадкового лісу. Експериментальні результати показали, що всі алгоритми ефективно виявляли мережеві атаки, при цьому метод подвійного випадкового лісу досяг найвищої точності у розпізнаванні атак типу відмова в обслуговуванні (DoS).

Отже, у сучасних умовах розширення цифрових просторів та зростання кіберзагроз оператори мобільних мереж стикаються з новими викликами безпеки, що потребують впровадження інтелектуальних аналітичних рішень на основі машинного навчання. Мобільні мережі продовжують розвиватися, що відображається у вдосконаленні архітектури мережі, модернізації інтерфейсів і протоколів та збільшенні пропускної здатності передачі даних. Одночасно технічний прогрес створює нові вразливості, які атакуючі можуть використовувати як на рівні мереж доступу, так і в ядрі мережі.

Аналіз останніх досліджень і публікацій. У працях M. Hristov та ін. [1], J. D. Gadze та ін. [2] та M. J. Awan та ін. [3] представлено сучасні підходи до виявлення DDoS-атак. Автори підкреслюють ключову роль великих даних, потокової аналітики та інтелектуальних систем у реальному часі.

У роботі [1] продемонстровано інтеграцію платформи Splunk Enterprise у систему виявлення DDoS-атак в IoT-середовищі. Стаття актуалізує використання платформ SIEM як джерела та агрегатора IoC, що дозволяє поєднувати сигнатурні та поведінкові методи.

Стаття [2] досліджує застосування глибокого навчання для виявлення та пом’якшення DDoS-атак у SDN-мережах, підкреслюючи ефективність нейронних мереж для виявлення складних патернів, характерних для IoC (аномалії у трафіку, аномальні послідовності пакетів тощо).

Робота [3] демонструє систему виявлення в режимі реального часу, яка використовує методи аналізу великих даних. У ній підкреслюється важливість масштабованості та точності під час обробки великих потоків мережевої телеметрії.

Ці три роботи підтверджують, що IoC можуть бути інтегровані у високопродуктивні інфраструктури машинного навчання, а їх ефективність зростає при використанні великих наборів даних та потокової аналітики.

Дослідження S. Han, H. Kim та Y. S. Lee [4], присвячене алгоритму Double Random Forest, робить внесок у підвищення точності класифікації атак. Алгоритм поєднує кілька моделей Random Forest і показує покращені результати у порівнянні з традиційними методами.

Це дослідження є важливим у контексті IoC, оскільки деталізований відбір характеристик і багаторівнева ансамблева обробка позитивно впливають на якість формування індикаторів компрометації та зменшують кількість хибних спрацьовувань.

У статті [5] здійснено узагальнений огляд сучасних методів ШІ у кібербезпеці. Підкреслено, що сучасні моделі здатні автономно виявляти аномалії, аналізувати поведінкові IoC, використовувати методи глибокого навчання для виявлення прихованих зв’язків.

У роботі наголошено на зростанні ролі адаптивних моделей у виявленні zero-day атак, що є важливою складовою побудови IoC нового покоління.

Публікація Fidelis Security [6] пояснює сутність аномаліє-орієнтованого підходу, який лежить в основі поведінкових IoC та більшості сучасних систем виявлення вторгнень. Автори вказують, що поведінкові індикатори дозволяють виявляти

відхилення від нормальної поведінки, фіксувати складні атаки без використання сигнатур, інтегрувати ризик-орієнтовану оцінку активності.

Цей підхід є ключовим у сучасних системах виявлення атак, які працюють із IoC у динамічному середовищі.

Матеріали [7], [8] та [9] підкреслюють важливість використання MITRE ATT&CK при аналізі атак та формуванні IoC/IoA.

У [7] розглянуто використання ШІ для передбачення zero-day атак на основі поведінкових IoA та телеметричних IoC.

Публікації [8] та [9] докладно пояснюють роль MITRE ATT&CK у структуризації технік, тактик та процедур (TTPs), що дозволяє формалізувати індикатори компрометації та інтегрувати їх у системи моніторингу.

Таким чином, MITRE ATT&CK виступає універсальною моделлю для інтерпретації, класифікації та агрегування IoC.

У статті PuppyGraph [10] описано значення аналітики великих даних у виявленні кіберзагроз. Підкреслено, що великі обсяги телеметрії (логи, мережевий трафік, події аутентифікації) потребують графових методів пошуку IoC, потокової обробки, кореляції подій з різних джерел.

Публікація [11] визначає роль Hadoop та Spark у побудові масштабованих систем аналізу трафіку, що є важливим для інфраструктур, де формуються та обробляються IoC у великих обсягах.

Матеріал [12] присвячено проекту Apache Spot – платформі з відкритим кодом, орієнтованій на виявлення аномалій у великих масивах даних. У ній розглядається можливість використання Spot як джерела автоматизованого формування IoC.

Публікації Microsoft [13] та LogPoint [14] обґрунтовують важливість UEBA у створенні високорівневих поведінкових індикаторів. У роботах розглядаються виявлення інсайдерських загроз, моделювання профілю поведінки користувача, автоматичне формування IoC на основі неявних аномалій.

UEBA доповнює традиційний SIEM і дозволяє формувати більш точні IoC на рівні користувачів, процесів та пристроїв.

Мета статті. вивчити можливості застосування штучного інтелекту для виявлення вразливостей у мережевій інфраструктурі на основі індикаторів компрометації, враховуючи специфіку прихованих каналів зв’язку, динаміку поведінки атакуючих та обмеження традиційних статистичних методів.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Розроблена система виявлення атак призначена не для заміни, а для доповнення аналізатора на основі сигнатур з метою підвищення загальної ефективності, особливо при виявленні раніше невідомих атак. Основні етапи проєктування системи виявлення вторгнень на основі машинного навчання включають вибір набору даних для навчання системи виявлення атак; попередню обробку даних; вибірку для вирішення проблеми незбалансованості класів; оцінку значущості ознак та їх відбір; зменшення розмірності простору ознак; вибір моделі, налаштування параметрів та навчання моделі; тестування та валідацію.

Нижче наведена базова схема навчання з учителем, проілюстрована на рисунку 1.

ISSN 2663 – 4023

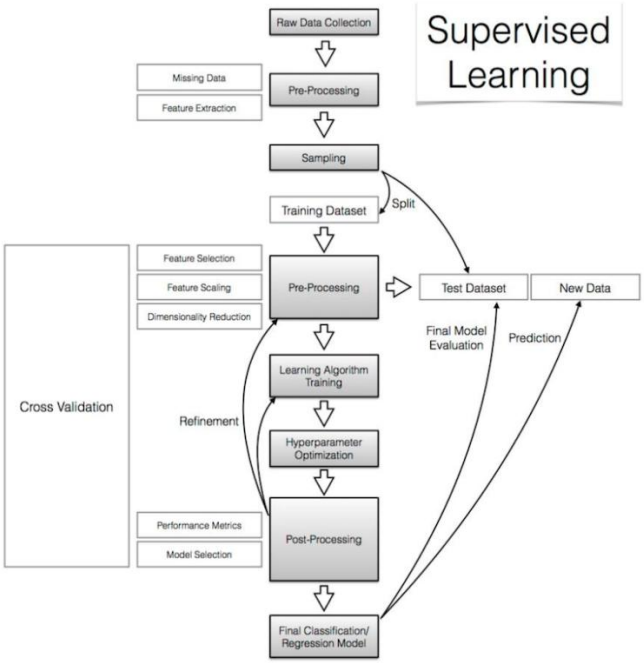

Рис. 1. Базова схема навчання з учителем

Для навчання системи серед публічно доступних наборів даних (таких як DARPA1998, KDD1999, ISCX2012, ADFA2013 та інші) було обрано один із найактуальніших на момент проведення дослідження – Intrusion Detection Evaluation Dataset CICIDS2017. Цей набір даних був розроблений Канадським інститутом кібербезпеки (CIC) [5].

CICIDS2017 створено на основі аналізу мережевого трафіку в контрольованому середовищі, що імітує дії 25 легітимних користувачів, а також різні типи шкідливих атак, здійснених зловмисниками.

Набір даних містить понад 50 ГБ сирих даних у форматі PCAP та включає 8 попередньо оброблених CSV-файлів із позначеними сесіями та витягнутими ознаками, зібраними протягом кількох днів спостережень.

В результаті для моделі RandomForestClassifier були отримані такі підсумкові параметри:

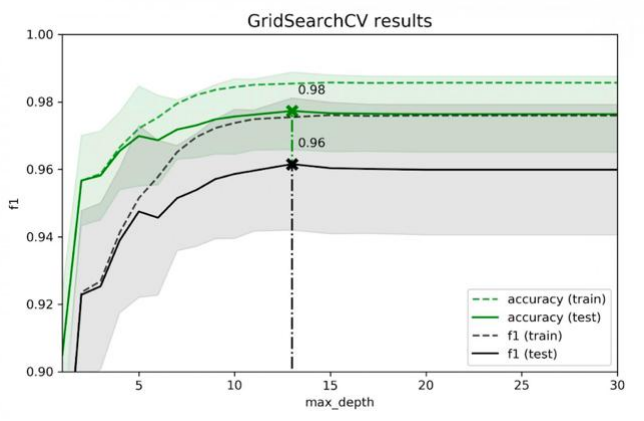

Рис. 2. Демонстрація процесу налаштування RandomForestClassifier

ISSN 2663 – 4023

Нижче наведено приклад налаштування одного з гіперпараметрів – max_depth – при фіксованих інших параметрах (n_estimators, min_samples_leaf, max_features). На рисунку показано залежність показника ефективності (F1-score) від різних значень параметра max_depth.

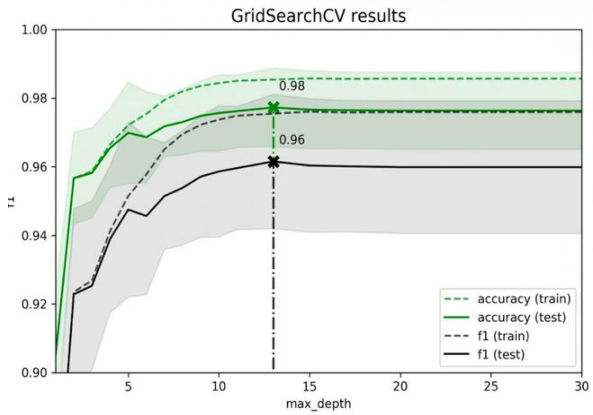

Рис. 3. Зміна F1-метрики моделі при варіюванні параметра max_depth

Навчена та налаштована модель RandomForestClassifier на тестовому наборі досягла показника recall 0,961 та F1-score 0,971 (перша прогонка згідно з протоколом експерименту; див. таблицю нижче).

Досягнуті результати свідчать про можливість подальшого підвищення точності моделі шляхом квазіоптимального налаштування гіперпараметрів (для порівняння, у дослідженні Кахрамана Костаса recall був 0,94, а F1 – 0,94, тоді як у роботах авторів CICIDS2017 recall складав 0,97, а F1 – 0,97).

Для валідації моделі в реальній мережевій інфраструктурі був розроблений мережевий аналізатор – сніффер – на мові C#. Цей інструмент дозволяє перехоплювати мережевий трафік та, використовуючи алгоритми реконструкції TCP-сесій із широко застосовуваних інструментів, таких як Wireshark та TCP Session Reconstruction Tool, виділяти окремі сесії.

Для кожної збереженої сесії сніффер формує набір ознак на основі алгоритму CICFlowMeter. В якості веб-застосунку, що піддавався атаці, використовувалася власноруч створена консоль адміністратора безпеки на PHP з єдиним активним модулем авторизації, який працював під веб-сервером Apache [11, 12, 13, 14]. Конфігурація тестового середовища наведена на рисунку 4.

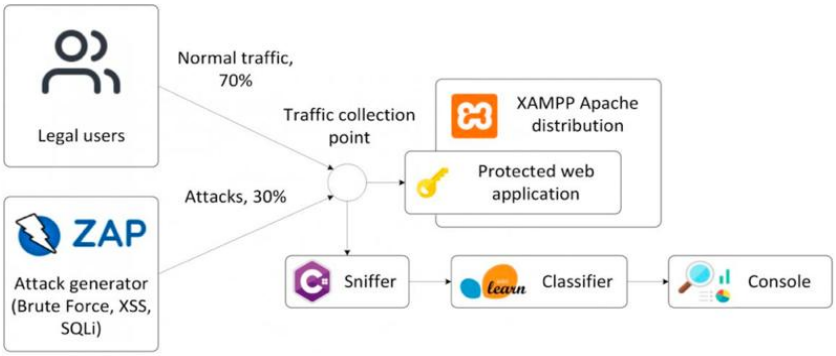

Рис. 4. Конфігурація тестового стенду

ISSN 2663 – 4023

Нормальний трафік генерувався запитами легітимних користувачів для доступу до консолі адміністратора та проходження аутентифікації. Аномальний (шкідливий) трафік імітувався за допомогою інструменту OWASP ZAP і включав три типи атак Brute Force, XSS та SQL Injection. Співвідношення нормального та аномального трафіку в реальному тестовому наборі даних становило 70% до 30% (див. рисунок 5).

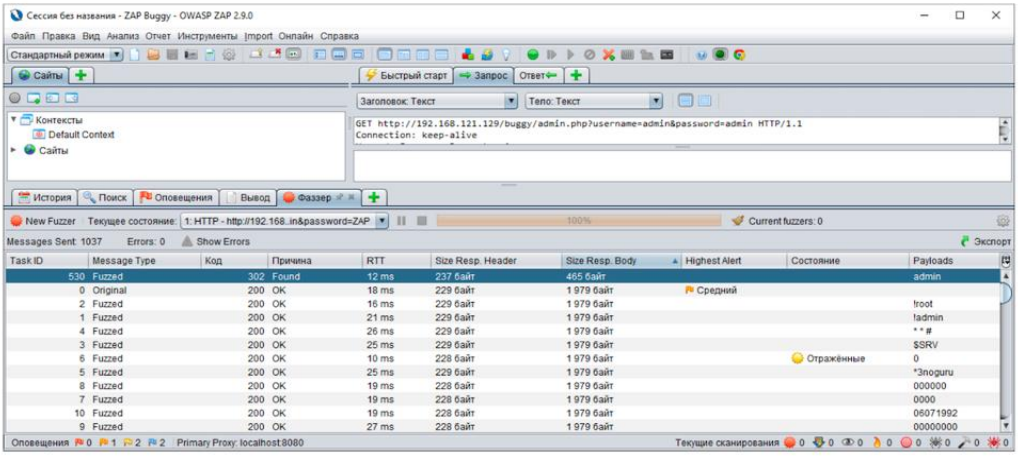

Рис. 5. Результати експериментів, проведених із використанням розробленого набору даних

Експерименти, проведені на зібраному наборі даних (прогін №2 та №3 у журналі експериментів), показали, що застосування моделі, натренованої на наборі CICIDS2017, є недоцільним з наступних причин:

Аналіз навчальної вибірки показав, що характер атак, змодельованих авторами CICIDS2017, відрізняється від реальної ситуації. Зокрема, атаки Brute Force у сесіях демонструють максимальну пропускну здатність до 10 Кбіт/с, що не відповідає реальним випадкам автоматизованого підбору паролів.

З десяти найважливіших ознак чотири – Flow Bytes/s (швидкість потоку даних), Fwd IAT Min(мінімальний час прибуття пакета в прямому потоці), Flow IAT Std (стандартне відхилення часу прибуття пакета) та Flow IAT Mean (середній час прибуття пакета) – безпосередньо залежать від фізичної топології мережі, де збирається трафік, та конфігурації мережевого обладнання.

У навчальному наборі сесії з веб-атаками характеризуються низькими швидкостями потоків та великими інтервалами між пакетами, що не відповідає характеристикам реальної мережі Ethernet 100 Мбіт/с.

Якісний набір даних має відповідати певним вимогам. Автори CICIDS2017 виділяють 11 таких критеріїв. Найважливішими серед них є забезпечення різноманітності мережевого обладнання, комп’ютерів та операційних систем у тестовій інфраструктурі; різноманітність напрямків трафіку; використання різних протоколів та типів атак; чітке маркування атак та чистого трафіку. Ми поставили додаткове завдання – оцінити доцільність створення евристичного аналізатора та приблизну точність його роботи. План збору набору даних:

Етап. Захоплення pcap-файлів та їх очищення. Під час збору «брудного» трафіку варіювати параметри фазування та вставляти паузи між фазами, щоб розбити сесії та збільшити їх кількість у наборі даних. Для «чистого» трафіку емулювати різноманітні дії легітимних користувачів.

Етап. Передача pcap-файлів до сніфера для вилучення ознак і об'єднання всіх маркованих записів в один набір даних.

Прогін №2. Модель була натренована на підмножині WebAttacks з CICIDS2017 (трафік зібраний у одній мережі). Потім модель тестували на реальному трафіку з іншої мережі з іншими характеристиками, зокрема пропускною здатністю. Результат був незадовільним – F1 score становив лише 0.064.

Обчислювальна складність оцінювалася опосередковано: прототип системи виявлення веб-атак, розроблений у Jupyter Notebook, було запущено на ПК з процесором Intel Core i5-2300 @ 2.3 GHz та 8 ГБ ОЗП у режимі виявлення. Тестовий набір містив близько 70 000 сесій, час виявлення становив 0.74669 секунди. Таким чином, пропускна здатність системи виявлення веб-атак оцінюється приблизно в 100 000 сесій на секунду.

Експеримент/Характеристика	Запуск 1	Запуск 2	Запуск 3
Етап навчання моделі			
Використовуваний набір даних	Збалансована та передопрацьована подібірка веб-атак WebAttacks набору даних CICIDS2017. 7267 записів, з них 5087 екземплярів класу «немає атаки» та 2180 екземплярів класу «є атака».		Сформований набір даних, що відповідають реальному мережному трафіку
Навчальна моель	70% записів використовуваного набору даних		70% записів набору даних
Ознаковий простір	1. Average Packet Size 2. Flow Bytes/s 3. Max Packet Length 4. Fwd Packet Length Mean 5. FwdIATMin 6. Total Length of Fwd Packets 7. FwdIATStd 8. Flow IAT Mean 9. Fwd Packet Length **Max** 10. Fwd Header Length		1. Flow Packets/s 2. Flow IAT Max 3. Bwd Packet Length Min 4. Flow Duration 5. Flow IAT Mean 6. Flow IAT Std 7. Average Packet Size 8. Fwd Packet Length Max 9. Total Packets 10. Fwd Header Length
Етап тестування моделі			
Тестова вибірка	30% записів використовуваного набору даних. Тестова і навчальна вибірка немає перетинів.	100% записів сформованого набору даних, що відповідають реальному мережевому трафіку	30% записів використовуваного набору даних. Тестова та навчальна вибірка не мають перетинів.
Значення метрик якості			
Accuracy	0.983	0.456	0.858
Precision	0.982	0.812	0.812
Recall	0.961	0.033	0.966
Fl	0.971	0.064	0.882

Рис. 6. Журнал експериментів

Експеримент зі створення моделі Random Forest для виявлення комп'ютерних атак завершено. Модель була натренована на публічному наборі даних CICIDS2017 і протестована в реальних умовах. Налаштування параметрів RandomForestClassifier із пакету scikit-learn дозволило досягти recall 0.961 та F1 score 0.971 на тестовому наборі CICIDS2017, а на власному наборі даних – 0.966 та 0.882 відповідно.

Основний висновок експерименту полягає в тому, що методи машинного навчання є практично застосовними для виявлення комп'ютерних атак.

Характер атак, змодельованих у навчальному наборі, відрізнявся від реальних атак.

Деякі ключові ознаки тісно пов'язані з фізичною топологією мережі, де збиралися дані, а також із конфігурацією мережевого обладнання.

Оптимальне навчання моделі має виконуватися на наборі даних, промаркованому на основі аналізу трафіку конкретної мережі, що захищається. При використанні моделі, натренованої на одній мережі, в іншій (проблема transfer learning), критично важливо,

щоб фізична структура мережі та конфігурації обладнання відповідали умовам оригінального навчання.

Розроблена система доповнює традиційний аналізатор на основі сигнатур і підвищує ефективність виявлення раніше невідомих атак. Ядром системи є модель RandomForestClassifier, натренована на публічному наборі даних CICIDS2017, що включає мережевий трафік легітимних користувачів та різні типи атак.

Для тестування в реальних умовах було розроблено sniffer на C#, який перехоплює TCP-сесії, виділяє ознаки за алгоритмом CICFlowMeter і надає їх для аналізу. Тестування продемонструвало високу продуктивність: на тестовому наборі CICIDS2017 recall = 0.961 та F1 = 0.971, а на власному наборі даних recall = 0.966 та F1 = 0.882. Обчислювальна швидкість оцінюється приблизно в 100 000 сесій за секунду.

Експерименти підтвердили, що ефективність моделі залежить від особливостей мережі оптимально навчати систему на даних тієї ж мережі, що захищається, через залежність ключових ознак від фізичної структури мережі та конфігурації обладнання. Розробка демонструє практичну застосовність методів машинного навчання для виявлення комп'ютерних атак і забезпечує основу для подальшого вдосконалення системи.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У дослідженні проведено всебічний аналіз систем IDS/IPS та їхніх обмежень у виявленні прихованих атак через стеганографічні канали. Було досліджено природу таких атак і визначено, що для ефективного виявлення необхідний розширений набір індикаторів компрометації (IoC), згенерованих за допомогою методів штучного інтелекту. Оцінювалась платформа Splunk Machine для побудови моделей виявлення аномалій, а також були розроблені класифікатори на основі IoC із використанням алгоритмів машинного навчання. Попередня обробка даних, балансування класів та відбір ознак підвищили здатність моделей до узагальнення. Тестування показало високу ефективність у виявленні як типових, так і складних атак. Отримані результати можуть бути використані для підвищення рівня кібербезпеки та покращення виявлення прихованих атак у комп'ютерних мережах.

Подальші дослідження можуть зосередитися на розширенні набору індикаторів компрометації (IoC) для виявлення нових типів атак, включаючи стеганографічні канали та інші методи прихованої передачі даних, а також на інтеграції системи з сучасними аналітичними платформами для обробки великих обсягів мережевого трафіку. Перспективними напрямками є застосування гібридних алгоритмів машинного навчання та глибокого навчання, адаптивного навчання та transfer learning для підвищення точності та швидкості виявлення складних атак. Важливим є також розвиток механізмів автоматизованого реагування, вивчення моделей поведінки користувачів та атакуючих, а також моделювання складних сценаріїв у контрольованих тестових середовищах. Крім того, перспективним підходом є впровадження систем виявлення вторгнень між мережами та організаціями для підвищення загальної стійкості кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Hristov, M., et al. (2021). Integration of Splunk Enterprise SIEM for DDoS attack detection in IoT. In *2021 IEEE 20th International Symposium on Network Computing and Applications (NCA)* (pp. 1–5). IEEE.
2. Gadze, J. D., et al. (2021). An investigation into the application of deep learning in the detection and mitigation of DDoS attack on SDN controllers. *Technologies, 9*(1), 14. https://doi.org/10.3390/technologies9010014

3. Awan, M. J., et al. (2021). Real-time DDoS attack detection system using big data approach. *Sustainability, 13*(19), 10743. https://doi.org/10.3390/su131910743
4. Han, S., Kim, H., & Lee, Y. S. (2020). Double random forest. *Machine Learning*, *109*, 1569–1586. https://doi.org/10.1007/s10994-020-05889-1
5. *Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms.* (2025). *Knowledge and Information Systems.* https://doi.org/10.1007/s10115-025-02429-y
6. Fidelis Security. (n.d.). *What is anomaly-based detection system?* https://fidelissecurity.com/cybersecurity-101/learn/anomaly-based-detection-system/
7. Megasis Network. (n.d.). *AI and zero-day attack detection: Anticipating unknown threats.* Medium. https://megasisnetwork.medium.com/ai-and-zero-day-attack-detection-anticipating-unknown-threats-c0a3a627a7d6
8. Exabeam. (n.d.). *What is MITRE ATT&CK®: An explainer*. https://www.exabeam.com/explainers/mitre-attck/what-is-mitre-attck-an-explainer/
9. Picus Security. (n.d.). *MITRE ATT&CK framework: Guide for beginners.* https://www.picussecurity.com/mitre-attack-framework-beginners-guide
10. PuppyGraph. (n.d.). *Big data analytics in cyber security: Enhancing threat detection.* https://www.puppygraph.com/blog/big-data-analytics-in-cybersecurity
11. Veritis. (n.d.). *Hadoop vs Spark: Key differences in big data analytics.* https://www.veritis.com/blog/hadoop-vs-spark-all-you-need-to-know-about-big-data-analytics/
12. PCWorld. (n.d.). *Apache Spot: Meet Apache Spot, a new open source project for cybersecurity.* https://www.pcworld.com/article/410492/meet-apache-spot-a-new-open-source-project-for-cybersecurity.html
13. Microsoft. (n.d.). *Advanced threat detection with user and entity behavior analytics (UEBA).* Microsoft Learn. https://learn.microsoft.com/en-us/azure/sentinel/identify-threats-with-entity-behavior-analytics
14. LogPoint. (n.d.). *Update to UEBA gives a better understanding of risks and better view of your security data.* https://www.logpoint.com/en/blog/product-releases/update-to-ueba-gives-a-better-understanding-of-risks-and-better-view-of-your-security-data

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023

Nataliia Cherniiashchuk
Doctor of Pedagogical Sciences, Professor
Lesya Ukrainka Volyn National University, Lutsk, Ukraine
ORCID: 0000-0002-3178-8377
cherniashchuk.nataliia@vnu.edu.ua

USING INDICATORS OF COMPROMISE FOR CYBERATTACK DETECTION

Abstract. This study provides a comprehensive analysis of intrusion detection and prevention systems (IDS and IPS), enabling an assessment of their effectiveness in identifying various types of cyberattacks, including those carried out through covert communication channels. Particular attention is given to examining the nature of steganographic channels, which significantly complicate attack detection, as well as the factors that influence their identification, such as network traffic dynamics and attacker behavior patterns. Indicators of compromise generated using artificial intelligence methods based on network traffic analysis are investigated, allowing for improved accuracy and speed in detecting malicious activity.

The capabilities of the Splunk Machine platform for building attack detection models and analyzing anomalous behavior in networks are evaluated. Classifiers for developing a machine-learning-based intrusion detection system have been designed. Within the research, a system architecture is proposed, an optimal dataset for model training is selected, class imbalance is mitigated, the most significant features are identified and selected, and feature space reduction is performed to enhance the efficiency and performance of the model. The model has been tuned and tested, and its effectiveness has been assessed based on the obtained results, confirming the practical applicability of the approach for detecting real cyberattacks.

The purpose of the study is to explore the potential of applying artificial intelligence to identify vulnerabilities in network infrastructure based on indicators of compromise, taking into account the specifics of covert communication channels, the dynamics of attacker behavior, and the limitations of traditional statistical methods. The results obtained can be used to improve existing cybersecurity systems and to develop effective tools for early detection of complex attacks.

Keywords: intrusion detection systems (ids), intrusion prevention systems (ips), artificial intelligence learning methods, and the splunk tool for security event analytics are key components in modern cybersecurity solutions.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Hristov, M., et al. (2021). Integration of Splunk Enterprise SIEM for DDoS attack detection in IoT. In *2021 IEEE 20th International Symposium on Network Computing and Applications (NCA)* (pp. 1–5). IEEE.
2. Gadze, J. D., et al. (2021). An investigation into the application of deep learning in the detection and mitigation of DDoS attack on SDN controllers. *Technologies, 9*(1), 14. https://doi.org/10.3390/technologies9010014
3. Awan, M. J., et al. (2021). Real-time DDoS attack detection system using big data approach. *Sustainability, 13*(19), 10743. https://doi.org/10.3390/su131910743
4. Han, S., Kim, H., & Lee, Y. S. (2020). Double random forest. *Machine Learning, 109*, 1569–1586. https://doi.org/10.1007/s10994-020-05889-1
5. *Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms.* (2025). *Knowledge and Information Systems.* https://doi.org/10.1007/s10115-025-02429-y
6. Fidelis Security. (n.d.). *What is anomaly-based detection system?* https://fidelissecurity.com/cybersecurity-101/learn/anomaly-based-detection-system/
7. Megasis Network. (n.d.). *AI and zero-day attack detection: Anticipating unknown threats.* Medium. https://megasisnetwork.medium.com/ai-and-zero-day-attack-detection-anticipating-unknown-threats-c0a3a627a7d6
8. Exabeam. (n.d.). *What is MITRE ATT&CK®: An explainer.* https://www.exabeam.com/explainers/mitre-attck/what-is-mitre-attck-an-explainer/

9. Picus Security. (n.d.). *MITRE ATT&CK framework: Guide for beginners.* https://www.picussecurity.com/mitre-attack-framework-beginners-guide
10. PuppyGraph. (n.d.). *Big data analytics in cyber security: Enhancing threat detection.* https://www.puppygraph.com/blog/big-data-analytics-in-cybersecurity
11. Veritis. (n.d.). *Hadoop vs Spark: Key differences in big data analytics.* https://www.veritis.com/blog/hadoop-vs-spark-all-you-need-to-know-about-big-data-analytics/
12. PCWorld. (n.d.). *Apache Spot: Meet Apache Spot, a new open source project for cybersecurity.* https://www.pcworld.com/article/410492/meet-apache-spot-a-new-open-source-project-for-cybersecurity.html
13. Microsoft. (n.d.). *Advanced threat detection with user and entity behavior analytics (UEBA).* Microsoft Learn. https://learn.microsoft.com/en-us/azure/sentinel/identify-threats-with-entity-behavior-analytics
14. LogPoint. (n.d.). *Update to UEBA gives a better understanding of risks and better view of your security data.* https://www.logpoint.com/en/blog/product-releases/update-to-ueba-gives-a-better-understanding-of-risks-and-better-view-of-your-security-data

Отримано редакцією журналу / Received:12.12.25
Прорецензовано / Revised: 06.01.26
Схвалено до друку / Accepted: 26.03.26

(cc) BY-NC-SA
This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.