ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ТА ЕЛЕКТРОННА ІНЖЕНЕРІЯ
INFORMATION AND COMMUNICATION TECHNOLOGIES, ELECTRONIC ENGINEERING

№ 5 (1), 2025

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

ГІБРИДНА МОДЕЛЬ ВИЯВЛЕННЯ МЕРЕЖЕВИХ АНОМАЛІЙ З ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ

М.Климаш [ORCID: 0000-0002-1166-4182], **Н. Бальковський** [ORCID: 0009-0007-0126-0356], **О. Шпур** [ORCID: 0000-0001-8156-8017]

Національний університет «Львівська політехніка», вул. С. Бандери, 12, 79013, Львів, Україна

Відповідальний за рукопис: Назарій Бальковський (e-mail: nazarii.y.balkovskyi@lpnu.ua)

(Подано 25 березня 2025)

Зростаюча складність кіберзагроз вимагає розробки ефективних методів виявлення та класифікації атак у мережевому трафіку. У даному дослідженні проаналізовано ефективність трьох популярних алгоритмів машинного навчання: Random Forest, який використовується для виявлення аномалій, Support Vector Machines (SVM), що виконує класифікацію кіберзагроз, та автоенкодерів, які застосовуються для попередньої обробки даних та глибокого аналізу трафіку. Враховуючи переваги кожного з методів, запропоновано комбіновану модель, яка поєднує можливості цих алгоритмів, підвищуючи ефективність виявлення загроз та оптимізуючи процес класифікації атак. Проведені експерименти демонструють, що запропонований підхід забезпечує збільшення точності виявлення атак на 3–7% та зменшення часу реагування порівняно з використанням окремих алгоритмів машинного навчання. Окрім того, комбінована модель сприяє оптимізації ресурсів, що є критично важливим фактором для розгортання масштабованих рішень у реальних умовах. Особливу увагу приділено гібридній моделі, яка поєднує автоенкодери та алгоритм Random Forest. Її ефективність підтверджена у тестових середовищах, де продемонстровано кращі результати виявлення мережевих аномалій порівняно із застосуванням лише одного алгоритму. Запропонований підхід дозволяє не лише підвищити рівень захисту інформаційних систем, а й забезпечити гнучкість у налаштуванні, що робить модель придатною для використання у широкому спектрі кібербезпекових завдань. Отримані результати можуть бути використані для вдосконалення існуючих методів кіберзахисту, зокрема у сфері захисту критичної інфраструктури, де своєчасне виявлення загроз є ключовим фактором безпеки. Висока ефективність комбінованого підходу підтверджує його доцільність для впровадження у системах моніторингу мережевого трафіку та кібербезпеки в цілому.

Ключові слова: *кібербезпека, машинне навчання, розподілені системи, алгоритми безпеки, оптимізація, захист інформації, інформаційна безпека, інформаційні системи, цифрові технології, інформація, загрози.*
УДК: 621.391

Вступ

Сучасний цифровий світ динамічно розвивається завдяки впровадженню технологій хмарних обчислень, Інтернету речей (IoT) та великих даних, однак зростання цієї цифрової інфраструктури

© 2025 Національний університет “Львівська політехніка”

супроводжується дедалі складнішими кібератаками. Особливо вразливими виявляються розподілені інформаційні системи, які широко застосовують у сферах критичної інфраструктури (енергетика, транспорт, зв'язок), бізнесі та державному управлінні. У таких системах необхідно гарантувати високий рівень конфіденційності, цілісності й доступності даних та сервісів [1].

Останнє десятиліття ознаменувалося справжнім проривом у методах машинного та глибинного навчання, що дає змогу обробляти величезні обсяги даних і виявляти складні закономірності. Такі підходи знайшли застосування й у кібербезпеці: від виявлення аномалій у мережевому трафіку до аналізу загроз соціальної інженерії, використовуючи, зокрема, методи обробки природної мови (NLP) [2]. Завдяки цьому вдалося підвищити точність і швидкість виявлення кіберзагроз, що постійно змінюються.

Попри успіхи, масове впровадження машинного навчання у сфері кібербезпеки зіштовхується з низкою викликів:

- Значний обсяг і різноманітність мережевих даних, що потрібно аналізувати в реальному часі.
- Постійна еволюція атак, включаючи складні багаторівневі кібератаки та методи соціальної інженерії.
- Необхідність оптимізувати витрати ресурсів (процесорних, мережевих) і забезпечувати масштабованість у розподілених системах [3].

Поєднання алгоритмів штучного інтелекту з великими даними дало змогу створювати проактивні рішення, здатні не лише реагувати на атаки, а й передбачати їх на основі виявлення закономірностей у мережевому трафіку. Таке поєднання великих даних, систем штучного інтелекту та машинного навчання забезпечує кібербезпеку, надавши зацікавленим організаціям можливість ефективніше аналізувати інциденти безпеки і реагувати на них, знижувати ризики і адаптуватися до розвитку кіберзагроз.

У цьому контексті машинне навчання стає одним із перспективних підходів, що дає змогу аналізувати нетривіально великі обсяги трафіку, виявляти аномалії та прогнозувати можливі атаки з високою точністю. Водночас, впровадження таких рішень у розподілених системах [4] залишається складним завданням через брак обчислювальних ресурсів, проблеми інтеграції та жорсткі вимоги до часу реагування.

Метою даного дослідження є розробка гібридної моделі алгоритмів машинного навчання (зокрема Random Forest, SVM та автоенкодери), яка сприятиме ефективному розгортанню кіберзахищених розподілених систем. У роботі детально проаналізовано популярні методи виявлення мережевих загроз, обґрунтовано їхню інтеграцію та модифікацію для підвищення продуктивності і рівня безпеки. Практична значущість результатів полягає в можливості впровадження описаного підходу у великих корпоративних мережах та середовищах критичної інфраструктури, де надійний кіберзахист є одним із визначальних факторів стабільності [5].

2. Порівняльний аналіз алгоритмів машинного навчання для виявлення аномалій мережевого трафіку

Одним із найпоширеніших методів для виявлення аномалій мережевого трафіку є Random Forest (далі — RF). У дослідженні [1] продемонстровано його ефективність у сценаріях виявлення DDoS-атак завдяки здатності RF обробляти великі обсяги даних із високим рівнем точності. Водночас автори наголошують, що RF потребує значних обчислювальних ресурсів, що потенційно ускладнює роботу в режимі реального часу.

Support Vector Machines (SVM) також широко застосовують у кібербезпеці, зокрема для класифікації атак. У [2] показано, що SVM може успішно розрізняти різні типи загроз, як-от SQL-ін'єкції та фішингові атаки із високою точністю. Водночас ефективність SVM значною мірою залежить від вибору ядра та параметрів.

Серед методів глибинного навчання особливе місце займають автоенкодери, що здатні аналізувати приховані патерни даних і виявляти нові типи загроз. У роботі [6] продемонстровано, що автоенкодери показують низький рівень хибних спрацювань і можуть працювати із великими обсягами мережевого трафіку. Однак їхнє впровадження потребує високих обчислювальних ресурсів, що може стати проблемою для розподілених систем.

Дедалі більшої популярності набуває комбіноване (гібридне) використання кількох алгоритмів. Зокрема, у [7] описано підхід, де RF виконує попередню фільтрацію даних, а автоенкодери здійснюють поглиблений аналіз. Цей підхід дав змогу зменшити кількість хибних позитивних спрацювань на 15% порівняно з окремим застосуванням цих методів.

Утім, досі відкритими залишаються питання оптимізації використання ресурсів, масштабованості моделей і адаптивності до нових типів атак. У дослідженні [8] наголошується на важливості розробки гібридних моделей, які б поєднували переваги різних підходів і забезпечували реальну ефективність у складних мережевих середовищах.

Random Forest – це ансамблевий метод, який створює декілька дерев рішень і агрегує їхні передбачення. Кожне дерево робить прогноз $h_m(X)$, а остаточний прогноз є середнім значенням (для регресії) або більшістю голосів (для класифікації).

$$H_m(X) = \arg\max y \sum_{m=1}^{M} I\left(h_m(X) = y\right), \tag{1}$$

де M - кількість дерев у лісі; $h_m(X)$ - прогноз з дерева m; $I()$ - функція-індикатор (підраховує голоси за кожен клас).

RF проводить голосування за найбільш імовірний клас, що дає змогу досягати високої точності навіть за складних патернів трафіку (рис.1). Це забезпечує високу точність класифікації навіть у випадку складних і нелінійних залежностей даних [1].

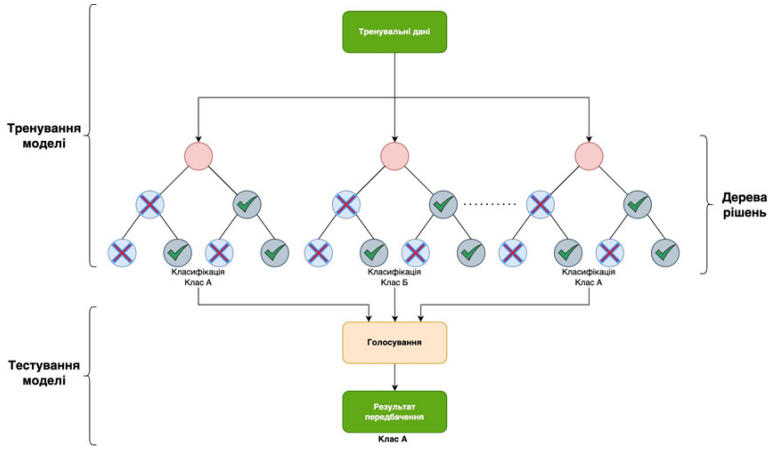

Рис. 1. Блок-схема роботи алгоритму Random Forest

Support Vector Machines (SVM) застосовується для класифікації загроз завдяки здатності створювати оптимальні гіперплощини для розмежування класів. SVM добре працює з невеликими наборами даних і демонструє високу точність у задачах із багатьма характеристиками [2]. На рисунку 2 схематично показано формування гіперплощини та принцип поділу вибірки на різні класи (атака/не-атака).

Формула класифікації має наступний вигляд:

$$y' = sign\left(\sum_{i=1}^{n} a_i y_i K(x_i, x) + b \right), \quad (2)$$

де y' - передбачений клас; y_i - клас мітки (1 або -1); x_i - дані навчальної вибірки; $K(x_i,x)$ - обраний метод ядра; b - зміщення (bias)

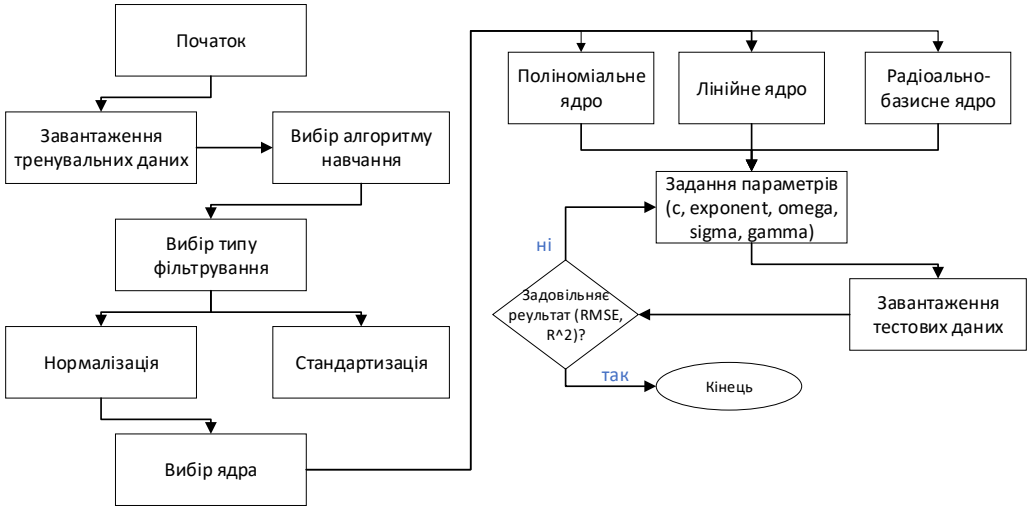

Рис. 2. Блок-схема роботи алгоритму SVM

Автоенкодери, метод глибинного навчання, використовуються для аналізу мережевого трафіку. Вони дозволяють автоматично виявляти приховані патерни в даних, що може бути корисним для виявлення нових типів загроз, які не мають чітких сигнатур [6].

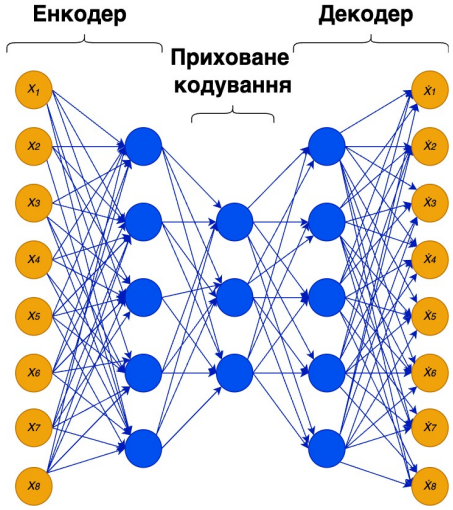

Рис. 3. Блок-схема роботи Автоенкодерів

Спираючись на переваги та недоліки кожного алгоритму, зосередимось на комбінованому застосуванні Random Forest (RF), Support Vector Machines (SVM) та автоенкодерів. Метою є перевірити, чи дає такий підхід змогу суттєво підвищити точність і швидкість виявлення загроз у розподілених системах.

3. Розроблення гібридної моделі виявлення мережевих аномалій

За результатами дослідження наведених алгоритмів запропоновано гібридну модель машинного навчання із використанням автоенкодера для кодування великого обсягу мережевих даних та Random Forest для класифікації мережевого трафіку (рис.4). Оскільки для гібридної моделі

потрібна тільки попередня обробка результатів (енкодер), то використання декодера не використовується. Головним завданням автоенкодера (енкодера) є попередня обробка мережевих пакетів з метою виявлення головних особливостей кожного пакету та зменшення об'ємності даних. Оптимізовані дані мережевих пакетів дальше передаються на вхід Random Forest, який вже здійснює безпосередню класифікацію пакетів на основі попередньо виділених ключових деталей пакетів. Таким чином збільшується швидкодія алгоритму Random Forest оскільки об'ємність даних стає суттєво меншою за рахунок використання автоенкодера. Точність виявлення аномалій теж покращується за рахунок відкидання незначущих частин мережевого трафіку.

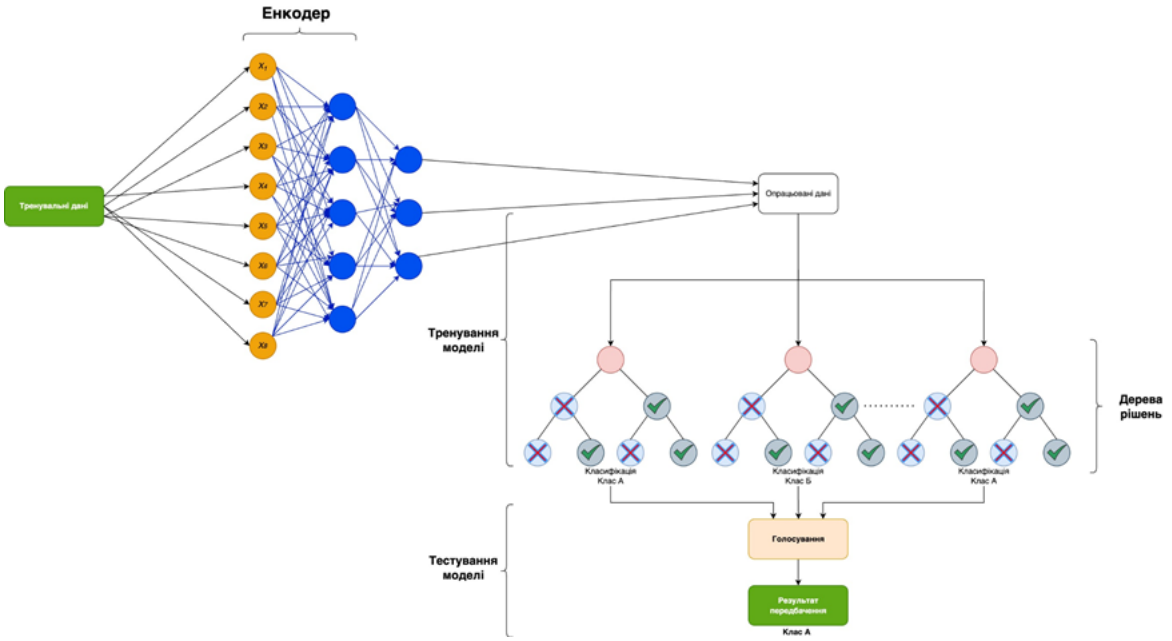

Рис. 4. Запропонована гібридна модель виявлення мережевих аномалій

4. Дослідження ефективності роботи гібридної моделі виявлення мережевих аномалій

Дослідження ефективності запропонованої моделі виявлення загроз будемо проводити на основі загальновідомих критеріїв оцінки показників ефективності виявлення мережевих аномалій:

Точність (Accuracy) - загальна частка правильно класифікованих зразків серед усіх зразків у наборі даних.

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

де TP (true positive) - правильне передбачення "атаки"; TN (true negative) - правильне передбачення "нормального" трафіку; FP (false positive) - хибне передбачення "атаки"; FN (false negative) - хибне передбачення "нормального трафіку".

Прецизійність (Precision) - наскільки часто прогноз атаки є достовірними.

$$\Pr ecision = \frac{TP}{TP + FP}.$$

Повнота (Recall) - з усіх реальних атак скільки обрана модель змогла виявити

$$\mathrm{Re}call = \frac{TP}{TP + FN}.$$

F1-оцінка (F1-Score) - балансна оцінка між точністю та прецизійністю

$$F1 = 2\frac{\Pr ecision * \Re call}{\Pr ecision + \Re call}.$$

Дослідження проводилось на операційній системі MacOS із використанням мови програмування Python. Основні характеристики робочої станції:

- ОЗП - 32GB
- Відеопам’ять - спільна пам’ять із ОЗП
- Процесор - Apple Silicon M1 Ultra
- Версія ОС - macOS Sequoia 15.1.1

Для аналізу алгоритмів SVM, Autoencoders та Random Forest у дослідженні використано мову Python та спеціалізовані бібліотеки:

- tensorflow - бібліотека для глибокого навчання та побудови нейронних мереж. Використовується для створення та тренування моделі на основі автоенкодерів (Autoencoders).
- scikit-learn (sklearn) - модуль машинного навчання, котрий містить алгоритми регресії, кластеризації та класифікації. Використовується для реалізації методу опорних векторів (SVM) та випадкового лісу (Random Forest).

Обрані бібліотеки дозволяють ефективно проводити навчання моделей, що використовуються в дослідженні, працювати з великими обсягами даних та виконувати аналіз результатів тренування моделей. Схема навчання і тестування запропонованої моделі наведено на рисунку 5.

Рис. 5. Схема навчання та тестування моделей

У ході дослідження було проведено навчання декількох моделей на основі алгоритмів машинного навчання для класифікації мережевого трафіку з використанням набору даних CICIDS 2017 [10]. Набір містить попередньо оброблені CSV-файли. Кожен запис містить характеристики мережевого з’єднання та відповідну мітку класу (BENIGN або ATTACK).

На першому етапі навчання кожного алгоритму проводилось окремо:

- *SVM* – розмежування звичайного (нормального) та шкідливого трафіку.
- *Random Forest* – покращення класифікації за рахунок багатьох дерев рішень.
- *Autoencoder* – нейронна мережа, яка навчалася реконструювати вхідні дані, виявляючи відхилення у шкідливому трафіку.

Після навчання кожного алгоритму було проведено тестування на основі тестового набору даних. Наступним кроком є детальний аналіз отриманих результатів, який допоможе зрозуміти ефективність розробленої гібридної моделі в умовах реального використання.

4.1 Результати тестування моделі на основі Random Forest

Random Forest було обрано як базовий алгоритм для першого етапу тестування завдяки його високій ефективності в задачах класифікації мережевого трафіку. Отримані результати наведено у табл. 1.

Таблиця 1.

Розраховані метрики оцінки моделі на основі Random Forest

Точність (Accuracy)	**Прецизійність (Precision)**	**Повнота (Recall)**	**F1-оцінка (F1-Score)**
92.13%	91.08%	99.99%	95.33%

З таблиці 1 бачимо, що модель на основі Random Forest показує непогані результати передбачення виду мережевого трафіку. Середній час опрацювання одного мережевого пакету 760.40 нс.

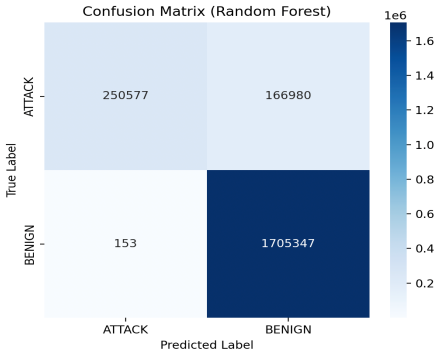

Рис. 6. Матриця помилок для моделі на основі Random Forest

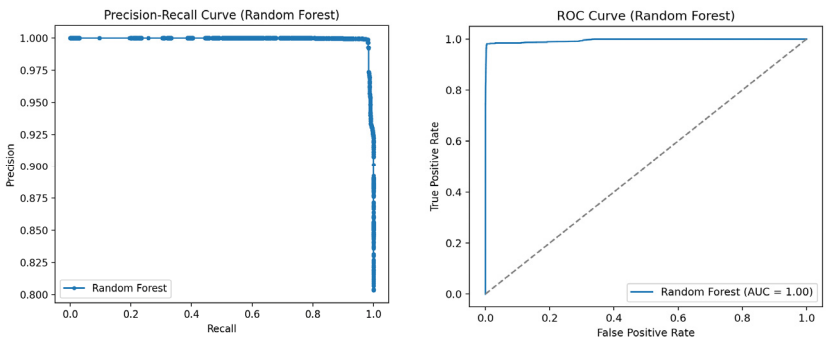

Рис. 7. Криві точності оцінювання вхідного трафіку Random Forest

Матриця помилок показує, що модель на основі Random Forest показує хороші результати із невеликою кількістю хибних прогнозів.

Рис. 7 демонструє криві точності (ROC-криві), отримані в результаті тестування моделі на основі алгоритму Random Forest для оцінювання вхідного мережевого трафіку. Як видно з графіка, модель забезпечує високу ефективність класифікації, що підтверджується площею під ROC-кривою (AUC), близькою до одиниці. Це свідчить про те, що алгоритм Random Forest успішно розрізняє нормальний і шкідливий трафік з високим ступенем точності. Варто зазначити, що крива швидко наближається до верхнього лівого кута графіка, що є ознакою високої чутливості та специфічності моделі, а отже, і її ефективності у виявленні аномалій та кіберзагроз у мережевому трафіку.

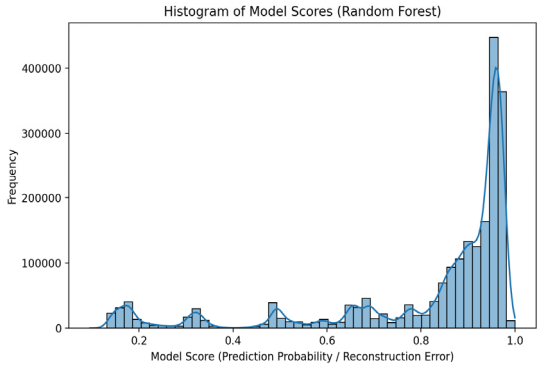

Рис. 8. Гістограма оцінок моделі на основі Random Forest

На рис. 8 зображена гістограма розподілу оцінок класифікації, отриманих у результаті тестування моделі Random Forest. Як видно із графіка, більшість оцінок моделі концентруються біля високих значень (близько 0.9–1.0), що свідчить про впевненість алгоритму у своїх прогнозах та високий рівень точності класифікації мережевого трафіку. Водночас, присутність невеликої кількості оцінок у нижчому діапазоні (0.4–0.6) вказує на існування окремих випадків, коли модель стикається з труднощами у чіткому визначенні класу трафіку. Це відкриває потенційні напрямки для подальшої оптимізації алгоритму з метою зменшення таких неоднозначних класифікацій.

4.2 Результати тестування моделі на основі SVM

Наступним етапом експерименту було оцінювання ефективності алгоритму Support Vector Machines (SVM), який застосовується для класифікації мережевого трафіку на нормальний та шкідливий. Вибір цього алгоритму обумовлений його високою точністю у класифікації наборів даних із великою кількістю характеристик. Основні метрики, отримані за результатами тестування SVM-моделі на наборі даних CICIDS 2017, наведено у табл. 2.

Таблиця 2.

Розраховані метрики оцінки моделі на основі SVM

Точність (Accuracy)	Прецизійність (Precision)	Повнота (Recall)	F1-оцінка (F1-Score)
84.61%	85.91%	96.71%	90.99%

Як видно з таблиці, модель демонструє досить високі результати, однак у порівнянні з моделлю Random Forest точність є нижчою. Це свідчить про наявність деяких обмежень алгоритму SVM при роботі з великим обсягом різноманітного мережевого трафіку. Середній час опрацювання одного мережевого пакету складає **255.50 µs**

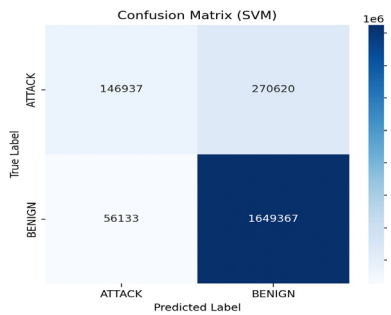

Рис. 9. Матриця помилок для моделі на основі SVM

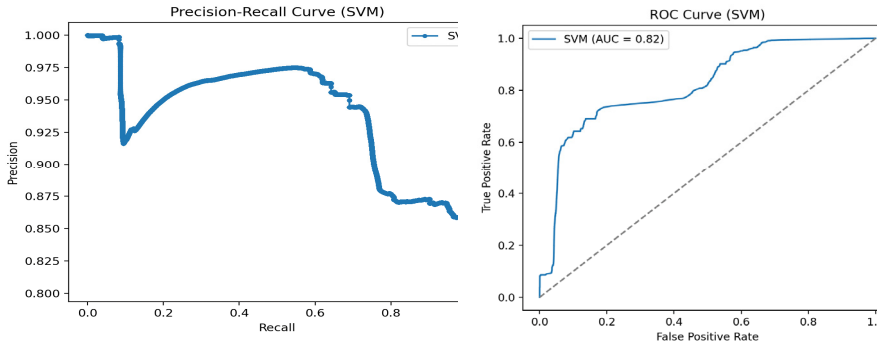

Рис. 10. Криві точності оцінювання вхідного трафіку

На рис. 9 наведено матрицю помилок (confusion matrix) для моделі на основі алгоритму SVM, що демонструє кількість правильних та хибних класифікацій мережевого трафіку. Як видно з матриці, модель загалом добре справляється з виявленням шкідливого трафіку, однак порівняно з Random Forest, кількість хибних класифікацій є помітно більшою. Зокрема, модель частіше класифікує нормальний трафік як шкідливий (хибно-позитивні прогнози), що може призводити до додаткових витрат ресурсів на перевірку таких помилкових спрацювань. Цей результат вказує на необхідність подальшої оптимізації параметрів моделі або додаткової передобробки даних для зменшення кількості помилок такого типу.

На рис. 10 представлено ROC-криві, які ілюструють ефективність моделі на основі алгоритму SVM у класифікації мережевого трафіку. Криві свідчать про достатньо високу здатність моделі розрізняти нормальний і шкідливий трафік, що підтверджується високим значенням площі під кривою (AUC). Водночас помітно, що порівняно з результатами алгоритму Random Forest, ROC-криві для SVM знаходяться трохи нижче, що свідчить про більшу кількість хибних передбачень та нижчу загальну ефективність моделі. Це також узгоджується з отриманими раніше метриками точності та прецизійності. Вказане підтверджує необхідність додаткового налаштування параметрів моделі SVM для подальшого підвищення її ефективності.

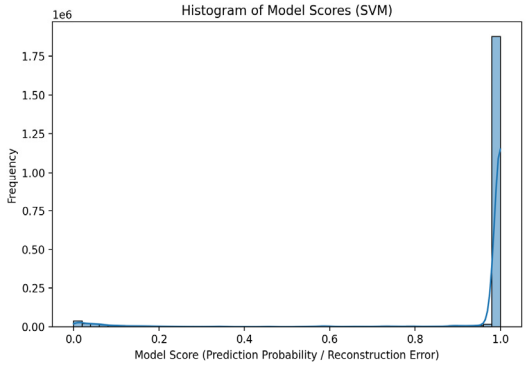

Рис. 11. Гістограма оцінок моделі на основі SVM

Гістограма показує, що модель на основі SVM робить чіткі прогнози щодо шкідливості трафіку.

4.3 Результати тестування моделі на основі Autoencoders

Третій етап експериментального дослідження був присвячений тестуванню моделі на основі автоенкодерів (Autoencoders). Вибір цієї моделі зумовлений її здатністю ефективно виявляти приховані закономірності у великих масивах даних, що теоретично дозволяє виявляти нові, раніше невідомі типи кіберзагроз. Проте, як продемонстрували результати тестування, наведені нижче, ефективність автоенкодерів для загальної класифікації різних типів атак у наборі даних CICIDS 2017 виявилася суттєво нижчою порівняно з попередніми моделями.

Таблиця 3.

Розраховані метрики оцінки моделі на основі Автоенкодера

Точність (Accuracy)	Прецизійність (Precision)	Повнота (Recall)	F1-оцінка (F1-Score)
38.33%	66.97%	45.85%	54.43%

Як видно з наведених значень, модель має значно нижчі показники ефективності порівняно з алгоритмами Random Forest і SVM. Особливо низьким є показник точності (Accuracy), що свідчить про низьку загальну здатність автоенкодерів правильно класифікувати різноманітні типи мережевого трафіку у даному наборі даних. Середній час обробки одного мережевого пакету становить 20.17 μs, що є достатньо швидким, однак не компенсує низьку точність класифікації.

Отримані результати вказують на те, що автоенкодер найбільш ефективно застосовувати у вузькоспеціалізованих сценаріях з обмеженим переліком загроз, а не для загального виявлення широкого спектру атак.

Проаналізувавши матрицю помилок, можна чітко побачити, щоб автоенкодер погано підходить для загального аналізу мережевого трафіку для виявлення різних типів атак. Автоенкодер повинен бути натренованим для виявлення конкретного типу атак, а оскільки тестовий набір даних містить інформацію про різні види атак, то модель на основі автоенкодера не може справитись із задачею.

Крива точності оцінювання вкотре показує, що автоенкодер не підходить для класифікації загальних типів атак та повинен бути натренований окремо для виявлення кожного виду атак окремо. З графіка чітко видно, що модель має низьку здатність чітко розмежовувати ці класи, про що свідчить значне перекриття між нормальним та шкідливим трафіком.

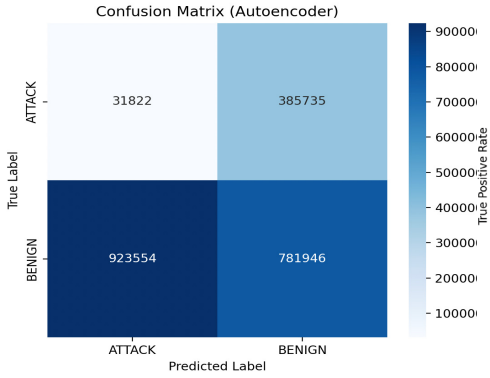

Рис. 12. Матриця помилок для моделі на основі Автоенкодера

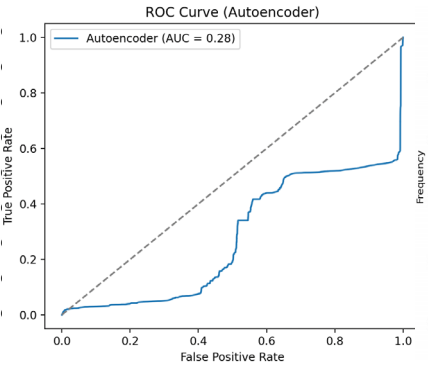

Рис. 13. Крива точності оцінювання трафіку моделі на основі Автоенкодера

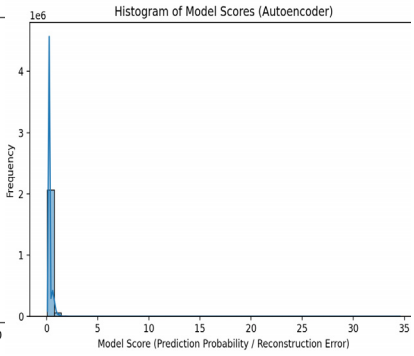

Рис. 14. Гістограма корекції помилок моделі на основі Автоенкодера

Велика кількість випадків потрапляє в зону невизначеності (середні значення прогнозу), що призводить до частих хибних класифікацій. Отримані дані підтверджують, що автоенкодер потребує додаткового тренування або спеціалізованої адаптації під конкретні типи загроз, оскільки в загальному випадку він демонструє недостатньо високий рівень розпізнавання мережевих аномалій.

4.4 Результат тестування гібридної моделі (Autoencoders + RF)

Заключним етапом експериментального дослідження стало тестування гібридної моделі, яка поєднує переваги автоенкодерів та алгоритму Random Forest. Враховуючи результати попередніх тестувань, саме таке комбінування алгоритмів було обране з метою оптимізації процесу класифікації мережевого трафіку: автоенкодер виконує попередню обробку та стиснення вхідних даних, а Random Forest — безпосередню класифікацію аномалій. Нижче наведено результати тестування цієї гібридної моделі, що демонструють суттєве покращення показників порівняно з окремими алгоритмами та підтверджують ефективність запропонованого підходу.

Таблиця 4.

Розраховані метрики оцінки гібридної моделі

Точність (Accuracy)	Прецизійність (Precision)	Повнота (Recall)	F1-оцінка (F1-Score)
97.33%	97.73%	98.98%	98.35%

Результати тестування гібридної моделі (автоенкодер + Random Forest), наведені в табл. 4, демонструють помітне покращення ключових показників ефективності порівняно з використанням лише алгоритму Random Forest. Зокрема, точність (Accuracy) зросла до 97.33%, а прецизійність

(Precision) досягла 97.73%, що свідчить про суттєве зменшення кількості хибних спрацьовувань у процесі класифікації шкідливого трафіку. Показник F1-оцінки (F1-Score), що враховує баланс між точністю і повнотою, також значно покращився та склав 98.35%, підтверджуючи загальну ефективність гібридного підходу. Хоча повнота (Recall) дещо знизилась до 98.98% через збільшення кількості помилкових класифікацій нормального трафіку як шкідливого, цей компроміс є виправданим завдяки значному покращенню загальної точності та прецизійності. Окрім цього, гібридна модель продемонструвала високу швидкодію із середнім часом обробки одного мережевого пакету 12.24 μs, що підкреслює її придатність для застосування в реальних умовах із високою інтенсивністю трафіку.

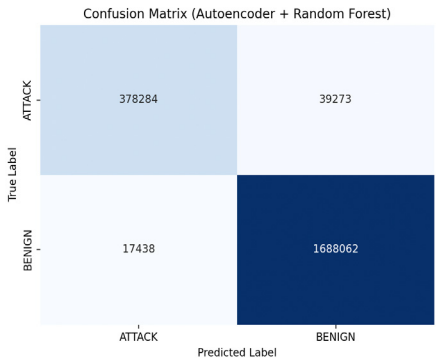

Рис. 15. Матриця помилок для комбінованої моделі

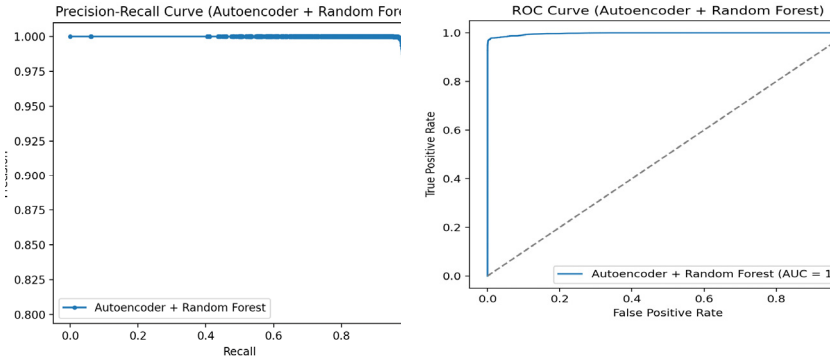

Рис. 16. Криві точності оцінювання вхідного трафіку гібридної моделі

Матриця помилок (confusion matrix) для комбінованої моделі, що поєднує автоенкодер і Random Forest, наведена на рис. 15, демонструє суттєве покращення в порівнянні з результатами, отриманими при використанні лише алгоритму Random Forest. Як видно з графіка, гібридна модель точніше класифікує шкідливий трафік: кількість правильно виявлених атак зросла з 250 577 (для Random Forest) до 378 284. Також значно зменшилась кількість хибних виявлень шкідливого трафіку (false positive)—з 166 980 до 39 273 випадків, що свідчить про підвищену прецизійність моделі.

Однак, важливо звернути увагу й на збільшення кількості нормального трафіку, помилково класифікованого як шкідливий (false negative)—з 153 до 17 438. Це підкреслює необхідність додаткових налаштувань порогу класифікації або оптимізації моделі, щоб зменшити кількість таких помилок у реальних умовах. Загалом, матриця помилок підтверджує значний потенціал гібридної моделі у підвищенні точності та надійності виявлення кіберзагроз.

На рис. 16 представлено ROC-криві, що ілюструють точність класифікації мережевого трафіку гібридною моделлю (автоенкодер + Random Forest). Графік свідчить про дуже високий рівень ефективності запропонованого підходу, що підтверджується близькістю ROC-кривої до верхнього лівого кута (і, відповідно, високим значенням площі під кривою—AUC). Це вказує на здатність моделі чітко й надійно розмежовувати нормальний та аномальний мережевий трафік. Водночас, хоча загальна точність моделі висока, певна кількість помилок залишається, зокрема помилкове виявлення нормального трафіку як шкідливого. Це потребує подальшого налаштування моделі для зменшення рівня таких хибних спрацювань, що дозволить зробити її ще більш ефективною та придатною до використання у реальних мережевих середовищах.

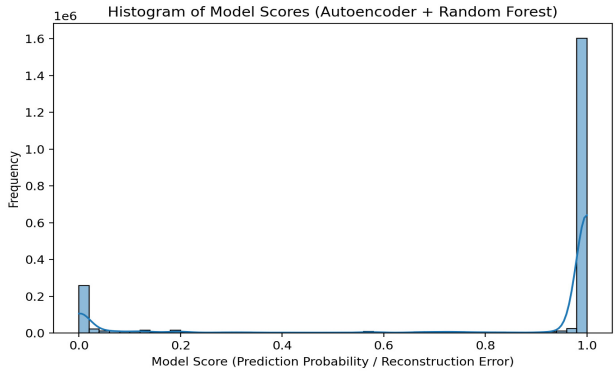

Рис. 17. Гістограма оцінок гібридної моделі

На рис. 17 наведено гістограму розподілу оцінок гібридної моделі (автоенкодер + Random Forest) при класифікації мережевого трафіку. Графік чітко демонструє покращення якості прогнозування: більшість оцінок моделі концентруються в крайніх областях (близько 0 або 1), що свідчить про високу впевненість моделі у своїх рішеннях щодо класифікації трафіку. Кількість проміжних або невизначених прогнозів суттєво зменшилась у порівнянні з попередніми результатами окремих алгоритмів, підтверджуючи ефективність гібридного підходу у чіткому виявленні мережевих аномалій.

Узагальнюючі результати проведених досліджень наведено в табл. 5, де порівнюються ключові показники роботи окремих алгоритмів (Random Forest, SVM, автоенкодери) та запропонованої комбінованої моделі.

Таблиця 5.

Порівняльна таблиця ефективності алгоритмів та моделі

Модель/Метрика	**Точність (Accuracy)**	**Прецизійність (Precision)**	**Повнота (Recall)**	**F1-оцінка (F1-Score)**	**Час опрацювання пакету**
Random Forest	84.61%	85.91%	96.71%	90.99%	760.40 ns
SVM	94.15%	98.80%	98.6%	97.75%	255.50 µs
Автоенкодер	38.33%	66.97%	45.85%	54.43%	20.17 µs
Гібридна	**97.33%**	**97.73%**	**98.98%**	**98.35%**	**12.24 µs**

Аналіз отриманих результатів показує, що запропонована комбінована модель значно перевершує окремі алгоритми за точністю виявлення аномалій і класифікації загроз. Точність виявлення аномалій в рамках комбінованої моделі досягла 97.33%, що на 3-9% більше, ніж у випадку використання тільки одного з алгоритмів, таких як Random Forest або SVM. Це підтверджує, що поєднання різних методів дозволяє компенсувати обмеження кожного з них і забезпечити більш надійний захист від кіберзагроз. Важливою перевагою є також зниження рівня хибних спрацювань, оскільки кожен алгоритм вносить свій внесок у фільтрацію помилкових сигналів, підвищуючи загальну точність моделі [12].

Запропонований комбінований підхід демонструє високу ефективність у порівнянні з окремими алгоритмами. Підвищена точність виявлення аномалій та загроз є основною перевагою, яка робить модель більш надійною для використання в реальних умовах. Однак варто зазначити, що для реального застосування в умовах великих розподілених систем необхідно враховувати можливі обмеження, пов'язані з обчислювальними витратами. Водночас, завдяки інтеграції методів попередньої обробки даних, таких як автоенкодери, можна знизити ці витрати, одночасно зберігаючи високу точність і ефективність роботи

Висновки

Штучний інтелект і машинне навчання розширюють межі кібербезпеки, відкриваючи шлях до суттєвих досягнень та можливостей стаючи більш стійкими з кожною атакою та здатними виявляти, захищати й усувати збитки від кібератак без втручання людини. На додаток, штучний інтелект і машинне навчання гратимуть ключову роль у пошуку загроз, допомагаючи фахівцям із кібербезпеки у превентивному виявленні загроз. Замість того, щоб реагувати на порушення, системи безпеки передбачатимуть і нейтралізуватимуть загрози, формуючи проактивне середовище кібербезпеки.

В результаті проведеного дослідження розроблена та протестована комбінована модель для виявлення аномалій і класифікації загроз у розподілених інформаційно-комунікаційних системах. Модель поєднує алгоритми машинного навчання, зокрема Random Forest, Support Vector Machines (SVM) та автоенкодери, що дозволило досягти значного підвищення точності виявлення загроз порівняно з використанням кожного з алгоритмів окремо.

Запропонована модель може бути ефективно застосована для захисту розподілених інформаційно-комунікаційних мереж, включаючи системи Інтернету речей (IoT), хмарні інфраструктури, а також для виявлення складних кібератак, таких як DDoS або SQL-ін'єкції. Подальша оптимізація алгоритмів і адаптація до конкретних типів загроз дозволить значно знизити витрати ресурсів і забезпечити більшу гнучкість.

Список використаних літературних джерел

[1] U. Islam, A. Muhammad, R. Mansoor, M. S. Hossain, I. Ahmad, E. T. Eldin, J. A. Khan, A. U. Rehman, and M. Shafiq, "Detection of Distributed Denial of Service (DDoS) Attacks in IoT Based Monitoring System of Banking Sector Using Machine Learning Models," Sustainability, vol. 14, no. 14, p. 8374, Jul. 2022, doi: 10.3390/su14148374

[2] C. Liu, J. Yang, and J. Wu, "Web intrusion detection system combined with feature analysis and SVM optimization," EURASIP Journal on Wireless Communications and Networking, vol. 2020, no. 1, pp. 1–14, doi: 10.1186/s13638-019-1591-1

[3] W. Song, M. Beshley, K. Przystupa, H. Beshley, O. Kochan, A. Pryslupskyi, D. Pieniak, and J. Su, "A Software Deep Packet Inspection System for Network Traffic Analysis and Anomaly Detection," Sensors, vol. 20, no. 6, p. 1637, Mar. 2020, doi: 10.3390/s20061637

[4] M. M. Klymash and M. M. Panchenko, "Packet Delay Monitoring System in Software-Configured Telecommunication Networks," in Proc. of the International Scientific and Technical Conference "Telecommunications Perspectives," 2016. (In Ukrainian)

[5] E. Pantelidis, G. Bendiab, S. Shiaeles, and N. Kolokotronis, "Insider Detection Using Deep Autoencoder and Variational Autoencoder Neural Networks," in Proc. 2021 IEEE Int. Conf. on Cyber Security and Resilience (CSR), Rhodes, Greece, Jul. 2021, pp. 155–160, doi: 10.1109/CSR51186.2021.9527954

[6] Z. S. Mahdi, R. M. Zaki, and L. Alzubaidi, "Advanced hybrid techniques for cyberattack detection and prevention," Security and Privacy, vol. 7, no. 2, pp. e471, 2024, doi: 10.1002/spy2.471

[7] M. Injadat, A. Moubayed, A. B. Nassif, and A. Shami, "Multi-Stage Optimized Machine Learning Framework for Network Intrusion Detection," IEEE Transactions on Network and Service Management, Jun. 2021, vol. 18, no. 2, pp. 1803–1816, , doi: 10.1109/TNSM.2020.3014929

[8] CICIDS 2017 Dataset, Canadian Institute for Cybersecurity, University of New Brunswick. [Online]. Available: https://www.unb.ca/cic/datasets/ids-2017.html (accessed: 10.03.2025).

[9] P. Prakriti, "Cyber threat detection using machine learning," Int. J. Sci. Res. Eng. Manag. (IJSREM), Apr. 2024, vol. 4, no. 4, pp. 1–6, doi: 10.55041/IJSREM36799

[10] I. Khlevna and B. Koval, "Parallel and distributed machine learning techniques for anomaly detection systems," in Proc. of the Int. Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2023), CEUR Workshop Proc., vol. 3624, pp. 131–138. [https://ceur-ws.org/Vol-3624/Paper_16.pdf]

[11] H. Kamal and M. Mashaly, "Enhanced hybrid deep learning models-based anomaly detection method for two-stage binary and multi-class classification of attacks in intrusion detection systems," Algorithms, vol. 18, no. 2, p. 69, Feb. 2025, doi: 10.3390/a18020069

[12] H. Torabi, "Practical autoencoder-based anomaly detection by using vector reconstruction error in cloud computing networks," Cybersecurity, vol. 5, no. 1, p. 9, 2022, doi: 10.1186/s42400-022-00134-9

[13] E. E. Abdallah, W. Eleisah, and A. F. Otoom, "Intrusion detection systems using supervised machine learning techniques: A survey," Procedia Computer Science, vol. 201, pp. 125–132, 2022, doi: 10.1016/j.procs.2022.03.029

HYBRID MODEL OF NETWORK ANOMALIES DETECTION USING MACHINE LEARNING

Mykhailo Klymash, Nazar Balkovskyi, Olha Shpur

Lviv Polytechnic National University, S. Bandery Str., 12, 79013, Lviv, Ukraine

The increasing complexity of cyber threats requires the development of effective methods for detecting and classifying attacks in network traffic. This study analyzes the effectiveness of three popular machine learning algorithms: Random Forest, which is used for anomaly detection, Support Vector Machines (SVM), which performs cyber threat classification, and autoencoders, which are used for data preprocessing and deep traffic analysis. Considering each method's advantages, a combined model is proposed that combines the capabilities of these algorithms, increasing the efficiency of threat detection and optimizing the attack classification process. The experiments demonstrate that the proposed approach increases attack detection accuracy by 3–7% and reduces response time compared to using individual machine learning algorithms. In addition, the combined model contributes to resource optimization, which is a critical factor for deploying scalable solutions in real-world conditions. Special attention is paid to the hybrid model that combines autoencoders and the Random Forest algorithm. Its effectiveness has been confirmed in test environments, where better results in detecting network anomalies were demonstrated compared to the use of only one algorithm. The proposed approach allows not only to increase the level of protection of information systems, but also to provide flexibility in configuration, which makes the model suitable for use in a wide range of cybersecurity tasks. The results obtained can be used to improve existing cyber protection methods, in particular in the field of critical infrastructure protection, where timely detection of threats is a key security factor. The high efficiency of the combined approach confirms its feasibility for implementation in network traffic monitoring systems and cybersecurity in general.

Keywords: *cybersecurity, machine learning, distributed systems, security algorithms, optimization, information protection, information security, information systems, digital technologies, information, threats.*