нового покоління, здатних функціонувати в умовах високої невизначеності та постійної еволюції кіберпростору.

1. ENISA Threat Landscape 2024. European Union Agency for Cybersecurity, 2024.
2. ENISA Threat Landscape 2023. European Union Agency for Cybersecurity, 2023.
3. NIST. Cybersecurity Framework 2.0. National Institute of Standards and Technology, 2024.
4. Artificial Intelligence and Cybersecurity Research. ENISA, 2023.
5. Котенко Д. та ін. Штучний інтелект у системах виявлення і запобігання кібератакам. Управління розвитком складних систем. 2024.
6. Mohamed N. Artificial Intelligence and Machine Learning in Cybersecurity: State-of-the-Art Techniques and Future Paradigms. Knowledge and Information Systems. 2025.
7. Integrating AI/ML in Cybersecurity: Analysis of Open XDR Technology and its Application in Intrusion Detection. 2023.
8. ENISA. Artificial Intelligence Cybersecurity Challenges. 2023.
9. Lavrenchuk A. Майбутнє кібербезпеки: виклики штучного інтелекту та машинного навчання. Молодий вчений. 2024.

Дослідження використання штучного інтелекту для ідентифікації джерел радіоелектронної боротьби

УДК 004.89:621.396

Роман Бибик[1], Іван Опірський[2]

Національний університет "Львівська політехніка",
[1]roman.t.bybyk@lpnu.ua [2]ivan.r.opirskyi@lpnu.ua

Метою роботи є дослідження можливостей використання методів штучного інтелекту для підвищення ефективності ідентифікації джерел радіоелектронної боротьби на основі просторово-частотного аналізу сигналів. Актуальність дослідження обумовлена зростанням кількості електромагнітних загроз та необхідністю створення адаптивних систем протидії РЕБ, здатних функціонувати в умовах динамічної електромагнітної обстановки. Наукова новизна роботи полягає у поєднанні методів просторово-частотного орієнтування з алгоритмами машинного навчання для автоматизованої класифікації сигналів джерел РЕБ та підвищення точності їх локалізації.

Сучасні умови ведення бойових дій характеризуються активним застосуванням засобів радіоелектронної боротьби, які здійснюють вплив на системи зв'язку, навігації, управління та засоби ураження. Зростання кількості електромагнітних загроз зумовлює необхідність удосконалення методів виявлення та ідентифікації джерел радіоелектронного випромінювання. Особливої актуальності набуває використання технологій штучного інтелекту, здатних забезпечити автоматизований аналіз електромагнітного середовища та адаптацію до змін параметрів сигналів у реальному масштабі часу.Одним із

перспективних напрямів є застосування методів просторово-частотного орієнтування, які дозволяють визначати параметри джерел РЕБ на основі аналізу часових, спектральних та просторових характеристик сигналів. Просторово-частотний аналіз базується на оцінюванні параметрів електромагнітного сигналу

$$S(t)=A(t)cos(2\pi ft+\varphi(t)) \quad (1)$$

де A(t) — амплітуда сигналу, f — частота сигналу, φ(t) — фазова складова сигналу. Для визначення напрямку на джерело випромінювання використовується оцінка кута приходу сигналу

$$\theta=arcsin(c\Delta t/d) \quad (2)$$

де c — швидкість поширення електромагнітної хвилі, Δt — різниця часу надходження сигналу, d — відстань між елементами антенної системи.

Інтеграція алгоритмів машинного навчання у системи просторово-частотного аналізу дозволяє автоматизувати процес класифікації сигналів та підвищити точність локалізації джерел РЕБ. Для задач ідентифікації можуть застосовуватись штучні нейронні мережі, методи глибокого навчання, дерева рішень та алгоритми кластеризації. Основною перевагою використання штучного інтелекту є можливість виявлення прихованих закономірностей у сигналах та адаптація до нових типів електромагнітних загроз. До таких характеристик можуть належати частотний діапазон, ширина спектра, тип модуляції, рівень потужності та часові параметри випромінювання. Аналіз зазначених параметрів дозволяє формувати адаптивні системи підтримки прийняття рішень щодо протидії засобам РЕБ.

Таблиця 1

Результати класифікації сигналів джерел РЕБ

Метод	Точність, %	Час аналізу, мс	Стійкість до шумів
Класичний аналіз	74	210	Низька
Нейронна мережа	91	85	Висока
Кластеризація	86	110	Середня

Порівняльний аналіз результатів показує, що використання нейронних мереж забезпечує суттєве підвищення точності класифікації сигналів та скорочення часу аналізу електромагнітного середовища. Використання інтелектуальних алгоритмів дозволяє ефективно працювати в умовах шумів та активних перешкод, що є важливим фактором у сучасних системах радіоелектронної боротьби. Таким чином, використання методів штучного інтелекту у поєднанні з просторово-частотним аналізом є перспективним

напрямом розвитку систем протидії РЕБ. Подальші дослідження доцільно спрямувати на розробку адаптивних моделей машинного навчання та вдосконалення методів аналізу сигналів у реальному масштабі часу. Отримані результати показують, що використання алгоритмів штучного інтелекту дозволяє підвищити точність класифікації сигналів джерел РЕБ та скоротити час аналізу електромагнітного середовища. Запропонований підхід забезпечує адаптивність системи до зміни параметрів сигналів і може бути використаний у перспективних системах підтримки прийняття рішень для протидії засобам радіоелектронної боротьби.

1. Haykin S. Neural Networks and Learning Machines. New York: Pearson, 2009. 936 p.
2. Goodfellow I., Bengio Y., Courville A. Deep Learning. Cambridge : MIT Press, 2016. 775 p.
3. Richards M. Fundamentals of Radar Signal Processing. New York: McGraw-Hill, 2014. 689 p.
4. Конахович Г.Ф., Пузиренко О.Ю. Основи радіоелектронної боротьби. Київ : НТУУ «КПІ», 2018. 320 с.

ШІ як інструмент практичної підготовки фахівців з кібербезпеки

УДК 004.85

Лілія Білокриницька

Відокремлений структурний підрозділ "Тернопільський фаховий коледж" Тернопільського національного технічного університету імені Івана Пулюя, bilokrynytskali@gmail.com

Розвиток інформаційних технологій супроводжується стрімким зростанням кіберзагроз, що висуває принципово нові вимоги до підготовки фахівців у сфері захисту інформації. За даними IBM, понад 90% кібернападів виникають через людські помилки [1], що підкреслює критичну роль якісної освіти у формуванні культури кібербезпеки. Академічна освіта не завжди встигає за темпом змін у галузі, залишаючи відчутний розрив між теоретичними знаннями та практичними вимогами ринку праці. У цьому контексті штучний інтелект все частіше розглядається як інструмент, здатний суттєво підвищити якість та ефективність підготовки майбутніх фахівців з кібербезпеки.

Класична система підготовки будується переважно на теоретичній базі, що об'єктивно не завжди встигає за темпом розвитку реальних кіберзагроз. Сучасні ШІ-інструменти натомість здатні створювати динамічне навчальне середовище, що адаптується до рівня знань кожного студента індивідуально. Платформи на основі машинного навчання аналізують прогрес учня, виявляють слабкі місця та автоматично підбирають відповідні завдання і сценарії, що дозволяє перейти від стандартизованого навчання до персоналізованого підходу. Крім того, ШІ здатний симулювати реальні кібератаки у безпечному середовищі, надаючи студентам практичний досвід без ризику для реальних систем.

Сучасний ринок освітніх технологій пропонує широкий спектр інструментів для практичної підготовки. Як зазначають фахівці, "вакансії провідних