УДК 004.056.53:004.8

ІНТЕЛЕКТУАЛЬНІ ПІДХОДИ ДО АВТОМАТИЗОВАНОГО ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА КІБЕРЗАГРОЗИ

Головко Д.І.
Paziloj444@gmail.com
Черкаський державний фаховий бізнес коледж
Бреус Р.В.
м.Черкаси, Україна

Сучасне цифрове середовище характеризується стрімким зростанням кількості та складності кіберзагроз – від класичних шкідливих програм до складних цілеспрямованих атак (APT). Організації змушені обробляти великі обсяги даних у режимі реального часу, що робить ручний аналіз неефективним. Традиційні сигнатурні системи захисту вже не забезпечують достатнього рівня безпеки, оскільки не здатні виявляти невідомі або модифіковані атаки.

У відповідь на ці виклики активно впроваджуються інтелектуальні підходи до кіберзахисту, які базуються на методах машинного та глибинного навчання, експертних системах і поведінковій аналітиці. Машинне навчання дозволяє моделювати поведінку загроз на основі історичних даних, зокрема класифікувати шкідливе програмне забезпечення та виявляти аномалії в мережевому трафіку. Глибинне навчання застосовується для аналізу складних структур даних, включаючи поведінкові патерни користувачів і взаємодії в мережі. Експертні системи забезпечують швидке реагування на відомі сценарії атак за допомогою правил і баз знань, а UEBA-технології дозволяють виявляти відхилення в поведінці користувачів і систем, що може свідчити про компрометацію облікових записів.

Підходи до виявлення загроз умовно поділяються на сигнатурні, аномалійні та гібридні. Сигнатурний аналіз ефективний лише для відомих загроз, тоді як аномалійний підхід дозволяє виявляти нові, раніше невідомі атаки. Гібридні методи поєднують обидва підходи для підвищення точності виявлення. Додатково використовуються методи аналізу мережевого трафіку та журналів

подій, що дозволяє ідентифікувати підозрілу активність, витоки даних або DDoS-атаки.

Важливим компонентом сучасних систем кіберзахисту є автоматизація реагування. SOAR-платформи координують роботу засобів безпеки та автоматизують сценарії реагування на інциденти. У разі виявлення загрози можуть автоматично блокуватися IP-адреси або облікові записи, ізолюватися заражені пристрої, генеруватися сповіщення для аналітиків, а також здійснюватися інтеграція з SIEM-системами для централізованого аналізу подій [3].

Інтелектуальні системи кібербезпеки мають низку переваг: вони забезпечують обробку великих обсягів даних у реальному часі, знижують залежність від людського фактору, здатні виявляти нові типи загроз, є адаптивними та масштабованими для великих інфраструктур. Це суттєво підвищує ефективність кіберзахисту [1].

Водночас існують і суттєві виклики. Для навчання моделей необхідні великі та якісні набори даних, спостерігається проблема хибнопозитивних спрацювань, а також складність інтеграції таких систем у вже існуючу інфраструктуру. Окремо слід виділити вразливість моделей до атак типу adversarial та етичні питання обробки даних [2].

Серед сучасних тенденцій розвитку кібербезпеки варто відзначити активне впровадження штучного інтелекту, перехід до архітектури Zero Trust, використання хмарних технологій, розвиток автономних систем реагування та інтеграцію безпеки у процеси розробки програмного забезпечення (DevSecOps) [4].

Практичне застосування інтелектуальних підходів охоплює корпоративні мережі, банківський сектор, державні інформаційні системи та IoT-середовища. Зокрема, вони використовуються для запобігання витокам даних, виявлення фінансового шахрайства та захисту критичної інфраструктури. Практика доводить, що без автоматизації процесів сучасний кіберзахист є недостатньо ефективним [3; 5].

Отже, інтелектуальні методи виявлення та реагування на кіберзагрози є ключовим напрямом розвитку сучасної кібербезпеки. Вони забезпечують швидкість, точність і масштабованість захисту, однак потребують подальшого вдосконалення, якісних даних та поєднання з експертною участю людини.

Список використаних джерел

1. Державна служба спеціального зв'язку та захисту інформації України. Офіційний вебсайт. URL: https://cip.gov.ua (дата звернення: 19.03.2026).
2. Національний координаційний центр кібербезпеки. Офіційний вебсайт. URL: https://ncscc.gov.ua (дата звернення: 19.03.2026).
3. CERT-UA. Офіційний вебсайт. URL: https://cert.gov.ua (дата звернення: 19.03.2026).
4. Закон України «Про основні засади забезпечення кібербезпеки України»: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 19.03.2026).
5. Національний банк України. Офіційний вебсайт. URL: https://bank.gov.ua (дата звернення: 19.03.2026).

УДК 004.8:004.93

ЕФЕКТИВНІСТЬ QLORA ДОНАВЧАННЯ МУЛЬТИМОДАЛЬНИХ МОДЕЛЕЙ В УМОВАХ ОБМЕЖЕНОГО ОБЧИСЛЮВАЛЬНОГО БЮДЖЕТУ

Цьома В. С.
tsyomav@gmail.com
Черкаський державний фаховий бізнес-коледж
Ночевнов Д.П.
м. Черкаси, Україна

Мультимодальні мовні моделі набувають широкого застосування в задачах розуміння зображень, однак їх використання у спеціалізованих предметних областях потребує додаткової адаптації. Запуск моделей у повному розмірі вимагає значних обчислювальних ресурсів, тоді як менші моделі можуть не досягати достатньої точності у вузьких задачах класифікації. Донавчання