ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей V Міжнародної науково-практичної конференції ІБІТ 2024

27 листопада 2024 року

Міністерство освіти і науки України
Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Національний університет “Львівська політехніка”

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ІБІТ 2024

Збірник доповідей
V Міжнародної науково-практичної конференції

27 листопада 2024 року

Львів – 2024

ББК 32.81+78.362

*Інформаційна безпека та інформаційні технології: з*бірник доповідей V Міжнародної науково-практичної конференції, ІБІТ 2024, м. Львів, 27 листопада 2024 року. Львів, ЛДУ БЖД, 2024, 661 с.

Ольга МЕНЬШИКОВА – к.ф.-м.н., доцент, заступник начальника факультету цивільного захисту Львівського державного університету безпеки життєдіяльності з навчально-наукової роботи;

Андрій ІВАНУСА – к.т.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Валентина ЯЩУК – к.е.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Орест ПОЛОТАЙ – к.т.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Валерія БАЛАЦЬКА – викладач кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Ігор МАЛЕЦЬ – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Назарій БУРАК – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Ольга СМОТР – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Юрій БОРЗОВ – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Роман ГОЛОВАТИЙ – к.т.н., старший викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Олександр ХЛЕВНОЙ – к.т.н., старший викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності.

УДК 004.8

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПРИ ЗАХИСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УСТАНОВ ОСВІТНЬОЇ ГАЛУЗІ

***Ярослав ДОРОГИЙ*[1]**
***Василь ЦУРКАН*[2]**
***Олена ДОРОГА-ІВАНЮК*[3]**

[1]Донецький національний технічний Університет, Дрогобич, Україна

[2]Інститут спеціального зв'язку та захисту інформації КПІ ім. Ігоря Сікорського, Київ, Україна

[3]Пологівський ліцей Ковалівської територіального громади с. Пологи, Білоцерківський район, Київська обл., Україна

Abstract. *The article examines the possibilities of using artificial intelligence (AI) technologies to protect critical infrastructure in the educational sector. Particular attention is paid to cyber threats caused by the military aggression of the Russian Federation and methods of countering them. Modern AI technologies are presented that can provide monitoring, threat identification and protection of sensitive data of educational institutions.*

Keywords: *educational sector, artificial intelligence, critical infrastructure, protection of critical infrastructure, cybersecurity.*

Анотація. *У статті розглянуто можливості застосування технологій штучного інтелекту (ШІ) для захисту критичної інфраструктури в освітній галузі. Особливу увагу приділено кіберзагрозам, зумовленим військовою агресією російської федерації, і методам протидії їм. Представлено сучасні технології ШІ, здатні забезпечити моніторинг, ідентифікацію загроз і захист чутливих даних освітніх установ.*

Ключові слова: *освітня галузь, штучний інтелект, критична інфраструктура, захист критичної інфраструктури, кібербезпека.*

*Вступ***.** Критична інфраструктура освітньої галузі є ключовою для забезпечення стабільного функціонування освітніх установ і збереження даних студентів та працівників. З розвитком цифрових технологій зростає важливість захисту інформаційних ресурсів у зв'язку з посиленням кіберзагроз, особливо з боку країн, що використовують кіберпростір як засіб агресії. Однією з країн, що активно впроваджує кібернапади на освітні та інші установи України, є російська федерація. У цих умовах штучний інтелект може стати важливим інструментом для моніторингу і забезпечення безпеки освітньої інфраструктури.

*Виклики для кібербезпеки освітньої галузі***.** З початком військової агресії рф проти України кількість кібератак на освітні установи країни значно зро-

сла. Ці атаки часто спрямовані на порушення функціонування платформ для дистанційного навчання, що є важливою складовою освітнього процесу, особливо в умовах війни. У той же час такі дії мають на меті викрадення конфіденційної інформації про учнів, студентів та працівників навчальних закладів.

Російські хакерські угруповання, зокрема ті, що пов'язані з державними структурами або діють з мовчазної згоди влади рф, цілеспрямовано атакують сервери українських освітніх установ. Основна мета цих атак – дестабілізація навчального процесу, знищення або спотворення критично важливих даних, що може порушити роботу установ і завдати шкоди особистій безпеці громадян. Такі кіберзлочини становлять загрозу для освітніх установ, оскільки вони підривають довіру до безпеки навчальних платформ, ускладнюють доступ до навчальних матеріалів, а також створюють ризики для особистих даних та інформації про академічні досягнення.

Ці кібератаки можуть також слугувати для впливу на інформаційний простір, підриваючи моральний стан студентства і викладачів та створюючи додатковий психологічний тиск на тлі військової агресії. З огляду на це, забезпечення захисту інформаційних систем освітньої галузі України стає стратегічно важливим завданням, для вирішення якого застосовуються передові технології, зокрема штучний інтелект, здатний забезпечити проактивний моніторинг, виявлення та відсіч подібним загрозам. [1].

*Застосування ШІ для моніторингу та виявлення загроз***.** ШІ здатний забезпечити постійний моніторинг мережевої інфраструктури навчальних закладів, що допомагає своєчасно виявляти й блокувати загрози. Системи на основі машинного навчання та обробки великих даних можуть розпізнавати патерни атак і аномальну активність, що можуть свідчити про спроби несанкціонованого доступу до систем [2]. Така технологія може бути особливо корисною для шкіл і університетів, які мають обмежені можливості в сфері кібербезпеки.

*Захист чутливих даних за допомогою ШІ***.** Захист чутливих даних, зокрема інформації про студентів, їхню успішність та медичні дані, є однією з головних задач в освітній галузі. Використання ШІ значно покращує ефективність захисту таких даних. Алгоритми машинного навчання допомагають виявляти підозрілу активність, аналізуючи поведінку користувачів і їхні дії в реальному часі. Це дозволяє оперативно реагувати на спроби несанкціонованого доступу до чутливих даних або їх витоку, знижуючи ризики для студентів та викладачів. Важливим аспектом є те, що системи на основі ШІ можуть працювати в автоматичному режимі, що підвищує їхню ефективність порівняно з традиційними методами безпеки, де часто є потреба в людському втручанні.

Машинне навчання, зокрема методи класифікації документів та виявлення аномальних дій, можуть бути використані для захисту від витоків чу-

тливої інформації в освітніх установах. Наприклад, системи, що використовують випадкові ліси (Random Forest), допомагають виявляти документи, які можуть містити конфіденційну інформацію, навіть якщо сама інформація не є очевидною на перший погляд [3].

*Впровадження ШІ для підвищення кіберстійкості освітньої інфраструктури***.** Впровадження ШІ в освітній інфраструктурі може значно покращити її кіберстійкість, оскільки дозволяє виявляти вразливості та загрози на ранніх етапах. Зокрема, ШІ здатний автоматично здійснювати аналіз поведінки користувачів і виявляти аномалії, що є важливим для забезпечення безпеки систем дистанційного навчання. Інтеграція ШІ також дозволяє оперативно реагувати на атаки, автоматизувати процеси відновлення даних та адаптувати стратегії безпеки відповідно до нових загроз [4].

Висновки. Застосування штучного інтелекту в освітній галузі значно посилює захист критичної інфраструктури, особливо на тлі зростання загроз з боку рф. Використання інтелектуальних систем для моніторингу, виявлення аномалій, захисту чутливих даних та управління доступом дозволяє ефективніше боротися з кіберзагрозами та забезпечує стабільність навчального процесу.

Інформаційні джерела

1. Державна служба якості освіти України. Безпечне освітнє середовище – нові вимоги. SQE, 2023. URL: https://sqe.gov.ua/bezpechne-osvitnie-seredovishhe-novi-vim/.

2. Pawlick, J., Colbert, E., & Zhu, Q. "A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy." Computers & Security, vol. 89, 2020, pp. 101–115. DOI: https://doi.org/10.1016/j.cose.2019.101654.

3. Nightfall AI. "How AI and Machine Learning Powers Next-Gen Data Leak Prevention (DLP)." Nightfall AI, https://www.nightfall.ai/blog/how-ai-and-machine-learning-powers-next-gen-data-leak-prevention-dlp.

4. Cyber Resilience for Critical Infrastructure Using AI. CPOMagazine. [Online]. Available: https://www.cpomagazine.com/cyber-security/using-ai-to-build-cyber-resilience-for-critical-infrastructure/. [Accessed: 12-Nov-2024].