УДК 004.056.5

ШТУЧНИЙ ІНТЕЛЕКТ У СЛУЖБІ КІБЕРЗАХИСТУ: ПЕРСПЕКСТИВИ ТА РИЗИКИ

Наталія Чернящук, Юлія Гуранець

ARTIFICIAL INTELLIGENCE IN THE SERVICE OF CYBER PROTECTION: PROSPECTS AND RISKS

Nataliia Cherniashchuk, Julia Huranets

Волинський національний університет імені Лесі Українки, просп. Волі, 13, Луцьк, 43025, Україна

Abstract. *In the era of digital transformation, cyber security is of particular importance due to the growing number of threats in the virtual environment. Artificial intelligence is becoming a key tool in the fight against cyber attacks thanks to its ability to analyze large volumes of data and detect anomalies. Its use allows prompt response to threats and increases the effectiveness of protective systems. One of the main advantages of AI is the possibility of self-learning, which reduces the burden on specialists and increases the accuracy of decisions.*

У добу стрімкої цифрової трансформації кіберпростір стає не лише майданчиком для комунікації, зберігання та обробки інформації, а й ареною постійних загроз - як для окремих користувачів, так і для організацій, держав і критично важливих інфраструктур. У цьому контексті питання кіберзахисту набуває першочергового значення, адже традиційні методи забезпечення інформаційної безпеки дедалі частіше виявляються недостатніми для ефективного реагування на сучасні, складні й динамічні загрози [1].

На цьому тлі штучний інтелект постає як потужний інструмент, здатний радикально змінити підходи до забезпечення кібербезпеки. Завдяки здатності обробляти великі обсяги даних, виявляти приховані закономірності, прогнозувати поведінку систем та ідентифікувати аномалії в режимі реального часу, ШІ значно підвищує ефективність виявлення та нейтралізації кіберзагроз [4]. Проте, попри значні перспективи, використання штучного інтелекту в цій сфері супроводжується низкою ризиків: від потенційної вразливості самих алгоритмів до загроз неетичного використання технологій і зловживання ними [3].

З розвитком цифрових технологій та зростанням обсягів електронної інформації питання захисту кіберпростору стало критично важливим. Усе більше сфер діяльності переходить у віртуальне середовище, що робить їх уразливими до кібератак. Традиційні засоби захисту вже не справляються з викликами сучасності, тому виникає потреба у впровадженні нових, інтелектуальних рішень [2]. Штучний інтелект дедалі активніше використовується для забезпечення безпеки цифрових систем. Його здатність швидко обробляти великі обсяги даних і виявляти приховані загрози дає змогу оперативно реагувати на потенційні атаки. Завдяки цьому зростає не лише ефективність, а й швидкість роботи систем безпеки.

Один із головних плюсів використання ШІ полягає в тому, що системи на його основі здатні до самонавчання. Це означає, що з кожним новим інцидентом вони удосконалюють свої алгоритми й підвищують точність виявлення загроз [4]. У результаті знижується навантаження на фахівців з безпеки, а ризик помилок стає меншим. Однак технологічні переваги супроводжуються певними ризиками.

Не менш важливим є моральний і правовий аспект. Автоматизовані рішення можуть зачіпати права людини, зокрема конфіденційність і свободу дій. Якщо системи працюють непрозоро, це створює ризик дискримінації або несанкціонованого доступу до особистих даних [4]. Ще одна проблема – зловмисне використання самих технологій. Кіберзлочинці вже

зараз експериментують з алгоритмами ШІ, щоб обходити захисні механізми, створювати фішингові кампанії або шкідливе програмне забезпечення, яке важко виявити [2]. Тому важливо не лише розвивати технології, а й одночасно формувати чіткі правила їх використання. Потрібні прозорі алгоритми, контроль за навчанням моделей та аудит їх рішень. Важливу роль у цьому відіграє також співпраця між технічними, юридичними й етичними фахівцями.

ШТУЧНИЙ ІНТЕЛЕКТ У КІБЕРЗАХИСТІ	
ПЕРСПЕКТИВИ	**РИЗИКИ**
Виявлення загроз	Хибні спрацювання
Швидке реагування	Вразливість ШІ до маніпуляцій
Аналіз Big Data	Витік даних
Адаптивність	Непередбачувана поведінка алгоритмів

Отже, впровадження штучного інтелекту в галузь кібербезпеки відкриває широкі можливості для формування більш стійких і гнучких систем захисту [1]. Завдяки високій швидкості обробки інформації, здатності розпізнавати нетипову активність і навчатись на основі нових загроз, ШІ здатен не лише оперативно виявляти кібератаки, а й попереджати їх ще на ранніх етапах. Це робить його важливим елементом сучасної цифрової інфраструктури. Проте паралельно з технологічними досягненнями виникають нові етичні, правові та безпекові виклики. Недосконаліть алгоритмів, ризик помилкових рішень або їх використання зі шкідливою метою ставлять під сумнів безпечність повної автоматизації. Саме тому критично важливо дотримуватись принципів прозорості, підзвітності та контролю за рішеннями, які приймає ШІ у сфері кіберзахисту.

Ключову роль у цьому процесі повинна відігравати міжнародна взаємодія, адже інформаційні загрози мають глобальний характер. Узгоджені дії між країнами, розробка єдиних стандартів безпеки, обмін знаннями та технологіями допоможуть мінімізувати ризики й ефективніше впроваджувати штучний інтелект у захисні системи [2]. Це сприятиме створенню загальносвітової цифрової екосистеми з підвищеним рівнем довіри. Загалом, успіх використання штучного інтелекту в кібербезпеці залежить від зваженого й відповідального підходу. Поєднання інженерного досвіду, правових знань і етичних орієнтирів дозволить сформувати збалансовану стратегію впровадження ШІ. Такий підхід гарантуватиме не лише технологічну ефективність, а й захист основоположних прав людини в умовах цифрової реальності.

Бібліографія

1. Бровко О. М. Штучний інтелект як інструмент забезпечення кібербезпеки: сучасні виклики та перспективи розвитку // Інформаційна безпека України. 2023. № 1. С. 45–53.
2. Гладкий С. П. Кібербезпека в умовах цифрової трансформації: роль інтелектуальних технологій // Вісник Національного технічного університету України. 2022. Т. 18, № 2. С. 28–36.
3. Кириленко Л. А. Етичні та правові аспекти використання штучного інтелекту в системах захисту інформації // Правова держава. 2021. Вип. 32. С. 91–98.
4. Соловей І. В. Перспективи впровадження штучного інтелекту в інформаційну безпеку: міждисциплінарний підхід // Наукові праці НДІ інформатики і права. 2023. № 4. С. 60–68.