ПРОБЛЕМИ ТА РИЗИКИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ

Бабич М.Г.
Харківський радіотехнічний фаховий коледж, Харків, Україна
Городецький С.Л.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному цифровому середовищі кібербезпека є ключовою умовою функціонування держави, бізнесу та суспільства. Зростання кількості кіберзагроз сприяло впровадженню в цю сферу штучного інтелекту (ШІ), який дозволяє автоматизувати виявлення атак, аналізувати великі обсяги даних і ефективно ідентифікувати потенційні ризики. Водночас використання ШІ супроводжується появою нових проблем, його вразливістю, можливістю зловживання та моральними викликами, що зумовлює необхідність наукового аналізу цих аспектів.

Метою доповіді є аналіз основних проблем і ризиків, пов'язаних із використанням ШІ у сфері кібербезпеки, а також обґрунтування доцільності його застосування з урахуванням сучасних викликів і загроз цифрового середовища. Однією з головних проблем систем ШІ є те, що вони можуть помилятися. Якщо в них потрапляють неправильні або неповні дані, вони можуть зробити хибний висновок і не помітити загрозу або, навпаки, помилково вважати безпечні дії небезпечними. Ще одна важлива проблема полягає в тому, що багато систем ШІ працюють як «чорна скринька», це означає, що навіть фахівці не завжди можуть пояснити, чому система прийняла те чи інше рішення. У кібербезпеці це дуже важливо, адже потрібно розуміти, як саме було виявлено загрозу. Серйозним ризиком є те, що штучний інтелект можуть використовувати не лише для захисту, а й для атак. Хакери можуть застосовувати ШІ для створення складних вірусів, автоматичних атак або обману користувачів. Це робить кіберзагрози більш небезпечними і масштабними. Традиційні методи захисту, зокрема сигнатурний аналіз, вже не завжди є ефективними через можливість модифікації шкідливого коду, тому використання ШІ стає необхідним для більш гнучкого та інтелектуального виявлення загроз [1]. Важливим викликом у використанні ШІ в кібербезпеці є проблема надмірної довіри до автоматизованих рішень. У разі, коли фахівці повністю покладаються на результати роботи ШІ, існує ризик втрати контролю над ситуацією, оскільки помилки алгоритмів можуть призводити до серйозних наслідків для інформаційної безпеки. Особливо це проявляється в умовах, коли система генерує велику кількість автоматичних сповіщень, що здатне перевантажувати спеціалістів із кібербезпеки та ускладнювати своєчасне реагування на реальні загрози [2]. Додатковою проблемою є те, що системи штучного інтелекту працюють із великими обсягами інформації, серед якої можуть міститися конфіденційні дані. Це створює ризик їх витоку та зумовлює необхідність забезпечення належного захисту інформаційних ресурсів на всіх етапах функціонування таких систем.

Суттєві складнощі завдає також потреба у великих обсягах якісних даних для навчання моделей, значні фінансові витрати на впровадження, підтримку

та постійне оновлення інтелектуальних систем, а також складність інтерпретації результатів, отриманих за допомогою алгоритмів ШІ.

Окрему загрозу становить можливість обходу систем захисту шляхом обфускації даних, коли зловмисники змінюють структуру інформації таким чином, щоб приховати шкідливу активність від алгоритмів аналізу [3]. У зв'язку з цим доцільним є комбіноване використання різних технологій захисту, що дозволяє підвищити стійкість систем до складних і нетипових кіберзагроз. Сучасні моделі ШІ, такі як ChatGPT та GitHub Copilot, здатні автоматично генерувати значну частину програмного коду. Це підвищує продуктивність розробників, але ускладнює визначення, чи створений код людиною чи ШІ. Код, згенерований ШІ, відзначається структурною одноманітністю, типовими назвами змінних і передбачуваною синтаксичною структурою, тоді як людський код має індивідуальний стиль та непослідовні відступи. Відмінності поступово зникають із розвитком технологій, що ускладнює контроль і потребує впровадження цифрових підписів або водяних знаків для підтвердження людського авторства [3]. Попри всі ризики, використання штучного інтелекту в кібербезпеці є необхідним. Сучасні загрози настільки складні та швидкі, що без автоматизації їх важко виявити. ШІ допомагає економити час, підвищує ефективність захисту та дозволяє працювати з великими обсягами інформації. ШІ значно прискорює процес виявлення шкідливої активності порівняно з традиційними підходами та підвищує ефективність аналізу великої кількості подій інформаційної безпеки. Однак найкращий результат досягається тоді, коли ШІ використовується разом із людським контролем, а не замість нього, бо навіть найсучасніші системи штучного інтелекту не можуть повністю замінити фахівців з кібербезпеки, оскільки потребують налаштування, контролю та адаптації до конкретних умов.

Отже, штучний інтелект у кібербезпеці має як переваги, так і значні ризики. Основні проблеми пов'язані з помилками в даних, складністю роботи алгоритмів, можливістю зловживання та залежністю від автоматизації. Для зменшення ризиків важливо контролювати якість даних, перевіряти роботу систем і не відмовлятися від участі людини в процесах безпеки. У майбутньому роль штучного інтелекту буде лише зростати, тому важливо навчитися використовувати його відповідально та безпечно.

Список літератури

1. Постіл, С. Д., Любушкін, Д. (2025). Впровадження штучного інтелекту у кібербезпеці. Збірка праць XIX Міжнародної наукової конференції «Наука та освіта», 15–22 січня 2025 р., м. Хайдусобосло, Угорщина. – Хмельницький: ХНУ. С. 14-18.

2. Оніщенко Є., Мальцев В. Застосування штучного інтелекту в кібербезпеці // Theoretical and Applied Cybersecurity: Матеріали III Всеукраїнської наук.-практ. конф. (TACS-2025), [Київ], 29 травня 2025 р. - Київ, 2025. - С. 313-314.

3. Бабич М. Г. Цемма Д.О. Розпізнавання програмного коду, створеного штучним інтелектом // Проблеми інформатизації: тези доп. тринадцятої міжнар. наук.-техн. конф., 27-28 листопада 2025 р., м. Баку, м. Харків, м. Бельсько-Бяла : [у 4 т.]. Т. 3: секції 4. – Харків : НТУ "ХПІ", 2025. – С. 46.