Габорець О.А.,
доктор філософії, доцент, доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки, факультету №3,
Донецький державний університет внутрішніх справ
(м. Кропивницький, Україна)

Абзалов Д.В.,
курсант 2-го курсу факультету №3,
Донецький державний університет внутрішніх справ
(м. Кропивницький, Україна)

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ЧИННИК ТРАНСФОРМАЦІЇ КІБЕРЗАГРОЗ У КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

У контексті сучасних глобальних трансформацій стрімкий розвиток цифрових технологій, зокрема штучного інтелекту (ШІ), суттєво змінює спектр загроз у сфері національної безпеки. Використання технологій ШІ сприяє вдосконаленню механізмів виявлення кіберзагроз, оптимізації оборонних стратегій та підвищенню стійкості критичної інформаційної інфраструктури держави. Водночас ці технології дедалі активніше застосовуються як інструменти нової генерації кіберзлочинності, гібридних війн та інформаційного впливу на державні та суспільні інститути. Така дуальна природа ШІ вимагає переосмислення підходів до формування державної політики у сфері кібербезпеки та поглибленого теоретичного аналізу відповідних викликів і загроз.

Кардинальні зміни у державній політиці з питань кібербезпеки в Україні розпочалися у 2014 році з початком збройної агресії Російської Федерації. Вказані обставини актуалізували визнання кібербезпеки як одного з ключових елементів системи національної безпеки. Зокрема, Р.О. Додонов наголошує, що Україна увійшла у найскладніший період свого розвитку, коли інформаційно-психологічний вплив перетворився на основний чинник ведення сучасної гібридної війни [1].

У цих умовах формування та реалізація державної політики у сфері кібербезпеки набула стратегічного значення, що знайшло відображення у прийнятті низки нормативно-правових актів, створенні спеціалізованих органів кіберзахисту та розробці Національної стратегії кібербезпеки. Особливу актуальність у цьому процесі має інтеграція новітніх цифрових технологій, насамперед штучного інтелекту, у системи виявлення, моніторингу та нейтралізації кіберзагроз.

Відповідно до частини четвертої статті 3 Закону України «Про національну безпеку» [2], кібербезпека виокремлена як самостійний напрямок національної безпеки. Водночас її забезпечення є необхідною умовою для реалізації воєнної, зовнішньополітичної, економічної, інформаційної та екологічної безпеки. Це свідчить про універсальний характер функції кібербезпеки, яка пронизує усі сфери суспільних відносин, що мають критичне значення для стабільності держави.

Таким чином, забезпечення кібербезпеки набуває міжгалузевого характеру, стаючи невід'ємною складовою державного управління та стратегічного планування. Особливого значення це питання набуває в умовах зростаючої залежності критичної інфраструктури, державного управління, оборонного комплексу та фінансового сектору від цифрових технологій. Вразливість цих сфер обумовлює необхідність розробки комплексної, інтегрованої державної політики, орієнтованої як на превенцію загроз, так і на забезпечення здатності кіберпростору до оперативного реагування, відновлення та адаптації.

Штучний інтелект у цьому процесі виступає каталізатором трансформації традиційних підходів до безпеки. Використання алгоритмів машинного навчання, аналізу великих даних та систем автоматичного розпізнавання загроз дозволяє здійснювати моніторинг кіберпростору в режимі реального часу, виявляти аномальні патерни та прогнозувати потенційні атаки. Водночас недосконалість нормативно-правового регулювання і брак уніфікованих стандартів застосування ШІ у сфері безпеки створюють ризики зловживань, що вимагає розширення міжнародного співробітництва у розробці єдиних підходів до регулювання цієї галузі.

Серед основних кіберзагроз для національної безпеки більшості країн можна виокремити:

1. кібершпигунство та військові дії за підтримки або з відома держави, спрямовані на заволодіння державними, промисловими таємницями, персональними даними чи іншою цінною інформацією;
2. використання Інтернету у терористичних цілях, зокрема для пропаганди, збору коштів та вербування прихильників;
3. кіберзлочинність, що включає викрадення персональних даних, відмивання коштів, продаж викраденої інформації про банківські картки, паролі серверів та шкідливе програмне забезпечення [3].

Отже, сучасний спектр кіберзагроз є багатокомпонентним і динамічним, вимагаючи системного, проактивного підходу до формування державної політики кібербезпеки. Така політика має бути спрямована на превентивне виявлення загроз, підвищення рівня кіберграмотності населення, розвиток науково-технічного потенціалу, а також на розширення міждержавного співробітництва в умовах цифрової глобалізації.

Список використаної літератури:

1. Гібридна війна: in verbo et in praxi : монографія / Донецький національний університет імені Василя Стуса / під заг. ред. проф. Р.О. Додонова. Вінниця : ТОВ «Нілан-ЛТД», 2017. 412 с.
2. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2469-19 (дата звернення: 23.04.2025).
3. Законодавство та стратегії у сфері кібербезпеки країн Європейського союзу. США, Канади та інших. URL: http://euinfocenter.rada.gov.ua/uploads/documents/28982.pdf