Сергеєв А.В.,
курсант ННІ №4,
Харківський національний університет внутрішніх справ
(м. Кам'янець-Подільський, Україна)

ОПТИМІЗАЦІЯ ПРОЦЕСІВ ФОРМУВАННЯ ДЕРЖАВНОЇ ПОЛІТИКИ В СЕКТОРІ БЕЗПЕКИ ТА ОБОРОНИ НА ОСНОВІ АДАПТИВНИХ КІБЕРНЕТИЧНИХ МОДЕЛЕЙ У КОНТЕКСТІ ГІБРИДНИХ ЗАГРОЗ

Сучасний розвиток технологій та посилення гібридних загроз вимагають принципово нового підходу до формування державної політики в сфері безпеки та оборони. Одним з найперспективніших напрямів є впровадження адаптивних кібернетичних моделей, які поєднують передові математичні методи, штучний інтелект та сучасні системи підтримки прийняття рішень. Математичне моделювання гібридних загроз на основі теорії ігор дозволяє аналізувати складні конфліктні ситуації, зокрема кібератаки на критичну інфраструктуру. Цей підхід враховує різні рівні інформації про противника - від повних даних про вразливості систем до умов неповної інформації, характерних для APT-атак. Ключовим аспектом є оптимізація стратегій захисту з використанням критерію мінімаксних збитків, що дозволяє мінімізувати потенційну шкоду навіть за умов обмеженої інформації. Практичне застосування теорії ігор у військових та кіберстратегіях охоплює всі етапи конфлікту - від превентивного планування до аналізу ефективності після його завершення [1, с. 2-3].

Важливим інструментом прогнозування ескалації конфліктів є штучні нейромережі, які демонструють високу ефективність у аналізі складних динамічних систем. Їхня здатність обробляти нелінійні залежності та шумові дані робить їх ідеальним інструментом для передбачення розвитку гібридних загроз. Оптимізація архітектури нейромереж, зокрема використання багатошарових персептронів, дозволяє досягати високої точності прогнозів на основі аналізу часових рядів, геопросторових даних та соціальних медіа. Ці технології знаходять практичне застосування як у прогнозуванні ескалації конфліктів, так і в оптимізації розподілу ресурсів для систем безпеки. Особливе місце в оптимізації процесів прийняття рішень займають агент-орієнтовані симуляційні моделі, які базуються на концепції обмеженої раціональності Герберта Саймона. Ці моделі дозволяють імітувати поведінку політичних акторів у умовах неповної інформації, враховуючи вплив соціальних та політичних інститутів. Вони ефективно відтворюють всі стадії прийняття рішень - від ідентифікації проблеми до вибору оптимального варіанту дій, що робить їх незамінним інструментом для тестування політичних рішень у складних умовах [2, с. 3].

Реформування органів безпеки з метою підтримки адаптивного управління передбачає створення спеціалізованих кібернетичних центрів реагування. Такі центри, побудовані на принципах систем підтримки прийняття рішень, поєднують інтерактивні інструменти аналізу даних, можливості моделювання сценаріїв та механізми оперативного реагування. Інтеграція сучасних технологій, зокрема штучного інтелекту та машинного навчання, дозволяє цим системам ефективно функціонувати в умовах динамічних загроз, забезпечуючи високу ступінь гнучкості та адаптивності. Досвід країн-лідерів у сфері кібербезпеки, таких як Естонія та Ізраїль, демонструє ефективність комплексного підходу до національної безпеки. Ізраїльська стратегія, заснована на принципі "хочеш миру - готуйся до війні", передбачає постійне вдосконалення інформаційних технологій та створення єдиних інформаційних центрів, що поєднують можливості військових, спецслужб і цивільних експертів. Цей досвід є особливо цінним для України у контексті протистояння гібридним загрозам [3, с. 3-4].

Впровадження автоматизованих систем підтримки прийняття рішень у Міністерстві оборони та Раді національної безпеки і оборони дозволить значно підвищити ефективність реагування на сучасні виклики. Ці системи забезпечують аналітичну обробку великих масивів даних у реальному часі, що є критично важливим у умовах швидкої еволюції загроз. Ключовим аспектом є забезпечення безперервного циклу "виявлення - аналіз - реагування", що дозволяє ефективно протистояти як традиційним, так і асиметричним загрозам [4, с. 2-3].

Запропоновані теоретичні та практичні аспекти демонструють значний потенціал адаптивних кібернетичних моделей для реформування державної політики безпеки. Інтеграція сучасних технологій, таких як штучний інтелект та квантові обчислення, разом з необхідними інституційними змінами, може значно підвищити стійкість держави до гібридних загроз. Це вимагає комплексного підходу, що поєднує теоретичні розробки, практичні рішення та адаптацію міжнародного досвіду з урахуванням національної специфіки [5, с. 5-6].

Список використаних джерел:

1. Використання методології теорії ігор під час аналізу військових операцій, URL: https://jait.donnu.edu.ua/article/view/12238 (дата звернення 11.05.2025);

2. Застосування штучних нейронних мереж для прогнозування ризику банкрутства банків, URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis (дата звернення 11.05.2025).

3. Моделі прийняття політичних рішень за Г. Саймоном, URL: https://studies.in.ua/teorija-pryjnjattja-sus-pol-rishen-shpargalky/4113-model-priynyattya-poltichnih-rshen-za-g-saymonom.html (дата звернення 11.05.2025);

4. Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027

роки, URL: https://zakon.rada.gov.ua/laws/show/273/2023#Text (дата звернення 11.05.2025);

5. Досвід Ізраїлю щодо формування стратегії національної безпеки, URL: https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/dosvid-izrayilyu-shchodo-formuvannya-stratehiyi-natsionalnoyi?__cf_chl_tk=AO.X42YpaARji6xvzOuOg87FjzS2jhMzZU1CesvLyOE-1746956896-1.0.1.1-Q7VYYJ.4B6ZDwGgcXEyISu1QEp75hWktcMkAK1r66Bk (дата звернення 11.05.2025).