7. Office of the United Nations High Commissioner for Human Rights. Ukraine. URL: https://www.ohchr.org/en/countries/ukraine (date of access: 07.05.2026).
8. Державна служба України з надзвичайних ситуацій : офіційний вебсайт. URL: https://dsns.gov.ua/ (дата звернення: 07.05.2026).
9. NATO. Relations with Ukraine. URL: https://www.nato.int/cps/en/natohq/topics_37750.htm (date of access: 07.05.2026).

Пустова Єлизавета Олександрівна,
студентка 2 курсу бакалаврату, «Правоохоронна діяльність»
навчально-науковий інститут права та психології
Національна академія внутрішніх справ
Науковий керівник:
Хахановський Валерій Георгійович,
професор кафедри інформаційних технологій
навчально-науковий інститут права та психології
Національної академії внутрішніх справ,
доктор юридичних наук, професор

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ КІБЕРЗЛОЧИНЦІВ

Штучний інтелект (ШІ) – це галузь комп'ютерних наук, що займається створенням систем і програм, здатних виконувати завдання, які традиційно потребують людського інтелекту. До таких завдань належать аналіз інформації, навчання на основі даних, розпізнавання образів, ухвалення рішень, прогнозування та мовна обробка.

ШІ – це здатність комп'ютерних систем імітувати когнітивні функції людини для виконання складних завдань без прямого втручання людини. ШІ був вигаданий і побудований для допомоги людям, в деяких випадках штучний інтелект справляється з певними завданнями в декілька разів краще. У ШІ немає почуттів, і він точніше може проаналізувати інформацію та виконати роботу, в той час як на людину може посприяти безліч факторів: від сімейних проблем до звичайного безсоння чи відсутності настрою.

Але зі створенням ШІ виникає наступна проблема: у сучасному світі все частіше з'являється новий вид загроз – використання ШІ кіберзлочинцями. Всі технології, які раніше допомагали бізнесу, державі, кіберпростору загалом, зараз можуть використовуватись для кібератак.

На нашу думку, під час війни це особливо важливо, адже ШІ можуть застосовувати як проти кожного окремо, так і проти держави загалом. Прикладами є фішинг та соціальна інженерія. *Фішинг* – це метод шахрайства в Інтернеті, коли кіберзлочинці надсилають підроблені листи, повідомлення або сайти, щоб обманом змусити людей розкрити особисті дані (логіни, паролі, реквізити карток). *Соціальна інженерія* – це сукупність методів використання психологічних особливостей особи з метою спонукання її до певних дій, яких би вона за звичних умов не вчинила, введення особи в оману [1].

Коли ШІ створює переконливі електронні листи або повідомлення, що імітують стиль знайомих людей чи офіційних організацій, це справді лякає. Такі повідомлення часто проходять крізь фільтри безпеки і збільшують шанси на успішну атаку. Крім того, ШІ дозволяє правопорушникам автоматизувати пошук вразливостей у системах, швидко аналізувати тисячі сайтів або серверів і знаходити слабкі місця. Саме це робить кібератаки більш масштабними та ефективними, ніж традиційні методи.

Ще одна небезпечна можливість ШІ – створення фейкових даних і глибинних підробок (deepfake). З їх допомогою кіберзлочинці можуть видавати себе за керівників компаній, державних службовців або інших людей, щоб виманювати гроші, секретну інформацію чи отримувати доступ до закритих систем.

Наведемо деякі випадки, які були скоєні останнього часу в Україні:

1. *Шахрайство з кредитами через DeepFake*. Група шахраїв створювала штучні відео з DeepFake, щоб пройти верифікацію у банківських додатках і оформити кредити на імена 286 українців, завдавши збитків понад 4 млн грн [3].

2. *Голосові deepfake-дзвінки*. Шахраї почали клонувати голоси рідних людей, щоб виманювати у довірливих українців гроші (наприклад, «позичальник/рідний» нібито просить терміново перерахувати кошти) [4].

3. *Фейкові відео про події війни*. У TikTok та соцмережах поширювали AI-генеровані відео з фейковими сюжетами (наприклад, «здача в полон»), які мали на меті деморалізацію та дезінформацію українських громадян [5].

Особливо небезпечно це під час воєнного стану в Україні, коли державні та важливі системи критичної інфраструктури (енергетика, транспорт, військові та урядові портали) стають мішенню для кібератак. Зловмисники можуть використовувати ШІ, щоб швидко атакувати ці системи, поширювати фейки та створювати паніку серед людей. У таких умовах ШІ перестає бути просто технологією – він стає потужною зброєю, що загрожує безпеці країни.

Отже, штучний інтелект стає для кіберзлочинців потужним засобом, який значно ускладнює роботу як правоохоронних органів, так і звичайних людей в цілому. За нашим переконанням, для ефективної протидії таким загрозам потрібні нові методи захисту, адже нові технології – це нові можливості для кіберзлочинців. Марценюк Є. В., Партика А. І., Крет Т. Б. у своїй роботі про вразливості ШІ підкреслюють, що ефективний захист ШІ-систем має бути багаторівневим, включати технічні рішення та модель комплексної безпеки організації, яка враховує як технічні, так і організаційні аспекти управління ризиками [2]. Погоджуємося з думкою науковців, адже це підсилює думку про необхідність поєднання різних заходів для зниження загроз у кібербезпеці. Адже лише комплексне поєднання технічних і організаційних заходів дозволяє мінімізувати ризики та запобігти незаконним діям із використанням ШІ.

Список використаних джерел

1. Петрик В. Соціальна інженерія в контексті кібернетичної безпеки України (сучасні технології та шляхи захисту). Навч. посіб. Київ. 2017. 80 с.

2. Марценюк Є. В., Партика А. І., Крет Т. Б. Дослідження вразливостей штучного інтелекту та побудова комплексної моделі безпеки організації. *Сучасний захист інформації.* 2025. № 1(61).

3. Гулевичук Т. Шахраї використали штучний інтелект для оформлення кредитів на українців – викрито схему на 4 млн грн. *LIFE.KYIV.UA* : [сайт]. URL: https://life.kyiv.ua/amp/news/shahra%D1%97-vikoristali-shtuchniy-intelekt-dlya-oformlennya-kreditiv-na-ukra%D1%97nciv-vi

4. Мазуренко І. Від голосу мами не відрізниш: шахраї почали ще майстерніше виманювати мільйони в українців, як не потрапити на гачок. *TELEGRAF* : [сайт]. URL: https://news.telegraf.com.ua/ukr/obshhestvo/2025-07-10/5914388-vid-golosu-mami-ne-vidriznish-shakhrai-pochali-shche-maysternishe-vimanyuvati-milyoni-v-ukraintsiv-yak-ne-potrapiti-na-gachok

5. AI-Generated Deepfake Videos Spread Disinformation About Ukrainian Military Surrender. *OECD.AI* : [сайт]. URL: https://oecd.ai/en/incidents/2025-11-04-c0f8

Пушко Максим Ігорович,
курсант 1 курсу бакалаврату, «Право»
Національна академія внутрішніх справ
Науковий керівник:
Скриник Мирослава Віталіївна,
доцент кафедри мовної підготовки
Національної академії внутрішніх справ,
доктор філософії у галузі права

SPECIFICS OF LAW ENFORCEMENT TRAINING IN WARTIME CONDITIONS: THE CASE OF ISRAEL AND UKRAINE

The functioning of the law enforcement system in the context of armed conflict requires a fundamental change in approaches to the professional training of personnel. The experience of countries in a state of war or under a permanent terrorist threat proves that civilian police are forced to assume paramilitary functions. In this context, of particular scientific and practical interest is a comparative analysis of the experience of the State of Israel, which has been improving its security system for decades under constant threats, and Ukraine, which has been forced to urgently adapt police training to the realities of a full-scale conventional war.

Armed aggression against Ukraine has unprecedentedly expanded the functionality of the National Police. As noted by V. M. Kovbasa and co-authors, police activity under martial law has been complicated by a number of specific tasks: serving at checkpoints, countering sabotage and reconnaissance groups, participating in the evacuation of the population, and eliminating the aftermath of missile strikes Kovbasa [1].

Accordingly, the Ukrainian law enforcement training system was forced to sharply shift its focus from classic law enforcement activities to special-tactical, firearms, and medical training in combat conditions. Performing duties in extreme