***Левченко Дарина Олександрівна***
Студентка н.гр. 103_СПД ННІ права та психології НАВС

*Науковий керівник:*
***Хахановський Валерій Георгійович***
доктор юридичних наук, професор, професор кафедри інформаційних технологій ННІ права та психології НАВС

## ШТУЧНИЙ ІНТЕЛЕКТ В РУКАХ ХАКЕРІВ: НОВА ЕРА КІБЕРЗАГРОЗ ТА ВИКЛИКИ ДЛЯ УКРАЇНИ

Поширення інструментів ШІ кардинально змінює ландшафт кіберзагроз: автоматизація збору даних, генерація персоналізованих фішингових атак, створення deepfake-контенту та автоматизоване сканування вразливостей підвищують ефективність і масштабність атак при значному зниженні порога входу для зловмисників. Це створює нову ітерацію загроз для національної безпеки, особливо в умовах гібридної агресії проти України, де кібероперації вже використовуються як складова гібридного тиску.

Як саме хакери використовують ШІ (тактики й приклади):

– Автоматизація фішингу та соціальної інженерії.

– Deepfake та клонування голосу.

– Автоматогенерація шкідливого коду.

– Аналіз великих масивів даних для вибору мішеней.

*Наслідки для України.*

Українська критична інфраструктура залишається в зоні підвищеного ризику. Поєднання традиційних тактик і нових можливостей ШІ здатне підвищити як частоту, так і складність атак на промислові системи управління. CERT-UA та Держспецзв'язку фіксують збільшення інцидентів соціальної інженерії, де елементи ШІ пришвидшують виробництво контенту.

*Проблеми адаптації:*

– технічні бар'єри: відсутність сучасних систем виявлення аномалій;

– кадрові проблеми: дефіцит фахівців зі знанням ШІ;

– правове регулювання: недостатня нормативна база щодо ШІ.

*Рекомендації:*

– розробка національної стратегії «ШІ-безпека»;

– інтеграція ШІ у засоби захисту;

– захист від deepfake і верифікація каналів;

– розширення освітніх програм;

– публічно-приватна платформа обміну даними;

– законодавче оновлення стандартів.

***Висновки***. ШІ змінює правила гри у кіберпросторі: атаки стають більш масштабними, персоналізованими й дешевими. Україна має створити комплексну політику, яка поєднує технічні рішення, кадрову підготовку, нормативну базу та етичні стандарти. Круглий стіл може стати платформою для вироблення дорожньої карти впровадження таких змін.

**Список використаних джерел:**

1. CERT-UA – Офіційний сайт Національної команди реагування на кіберінциденти. https://cert.gov.ua/

2. РНБО України. Річний аналітичний огляд кіберзагроз, 2024–2025.

3. Vavryk Y., Opirskyy I. Штучний інтелект: кібербезпека нового покоління. Ukrainian Scientific Journal of Information Security, 2024.

4. Сироватченко М. Правові аспекти забезпечення кібербезпеки в Україні, 2024.

5. Аналітичні матеріали Київстар Hub – «Тренди кібербезпеки на 2025 рік».

***Гусол Олексій Дмитрович***
Студент н.гр. 104_СПД ННІ права та психології НАВС

*Науковий керівник:*
***Хахановський Валерій Георгійович***
доктор юридичних наук, професор, професор кафедри інформаційних технологій ННІ права та психології НАВС

## СУЧАСНІ ВИКЛИКИ В СФЕРІ КІБЕРБЕЗПЕКИ

У сучасному світі інформаційні технології стали невід’ємною частиною економіки, політики, освіти та безпеки. Водночас активна цифровізація створює передумови для виникнення нових загроз у сфері кібербезпеки. Під кібербезпекою розуміють стан захищеності кіберпростору, при якому забезпечується цілісність, конфіденційність і доступність інформації. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», держава зобов’язана створювати систему захисту критичної інфраструктури та інформаційних ресурсів від кібератак. Одним із головних викликів сьогодення є зростання кількості цілеспрямованих атак на державні установи та правоохоронні органи.