Порохняк Т. Р.

студент групи МП-11,

науковий керівник ***Будник Л.А.,***

к.е.н., доцент кафедри безпеки та правоохоронної діяльності,

Західноукраїнський національний університет

ШТУЧНИЙ ІНТЕЛЕКТ В КІБЕРБЕЗПЕЦІ: ПЕРСПЕКТИВИ ТА ВИКЛИКИ

З кожним роком штучний інтелект вдосконалюється та проникає в більшість сфер суспільного життя. Характерною особливістю штучного інтелекту є те, що це – машина, яка запрограмована виконувати певну функцію. Завдяки цьому, він може знайти та помітити те, що людина часто не здатна запідозрити, або те що залишається поза межами людського сприйняття, через неуважність, або ж просто через те, що людина не може спрогнозувати та передбачити всі можливі варіанти розвитку подій. Збиток від хакерських атак, скоєних по всьому світу за останні роки, склав від $ 300 млрд до $ 1 трлн [1].

На думку українського дослідника з питань кібербезпеки професора В.Л. Бурячка «кібератака – це сукупність узгоджених щодо мети, змісту й часу дій або заходів, так званих кіберакцій, спрямованих на певний об’єкт впливу з метою порушення конфіденційності, цілісності, доступності, спостережуваності або авторства інформації, що циркулює в ньому, з урахуванням її уразливості, а також порушення роботи ІТ-систем і мереж зазначеного об’єкта» [2]. Авторитарні держави та їх посередники використовують кібератаки для підтримки інших видів діяльності, спрямованої на вплив [3].

З цього твердження та історичного досвіду можна вивести твердження, що кібератаки можуть зазнати значного впливу не тільки на регіональному чи особистому рівні, а також і на державному та

міждержавному. Є беззаперечним той факт, що кіберзлочин має відносну поширеність, але не набув масового характеру [4]. Серед найяскравіших прикладів можна навести кібератаку на мережу “Київстар” минулого року. Хоча ця атака була лише в національних межах, тобто зачепила лише нашу країну, однак мала величезне значення, оскільки була одною із наймасовіших та найзначніших кібератак на мобільну мережу за всі часи. Збій системи по всіх регіонах України вразив всіх користувачів мережі “Київстар”, а це більша частина населення країни. Окрім шкоди самій мережі DDoS-атаки вразили сигнали повітряних тривог, банкомати та торгові термінали. Враження одної мережі спричинило хвилю хаосу в більшій частині країни

На думку компетентного вченого М. Лібікі «інформаційна війна – це засоби, які включають збір, передачу, захист, маніпулювання, спростування, заперечення та знищення інформації, завдяки яким можна встановити перевагу над противником. Маніпулювання інформацією в контексті інформаційної війни - це зміна інформації з метою викривлення сприйняття дійсності противником [5]. Саме такі дії зараз застосовує росія проти в України в цій війні за виживання. Такі дії проявляються в масовому поширені фейків, діпфейків, в які люди легко вірять, оскільки вони створені так, щоб людина сприйняла його моментально як правду і не почала перевіряти достовірність інформації, оскільки саме це люди, на жаль, так часто забувають робити.

За допомогою штучного інтелекту можна спрогнозувати найбільш вразливі точки мережі чи іншого об’єкту інфопростору проти якого може бути проведена кібератака. Видатний науковець Джон Серль визначає таку дефініцію сильного штучного інтелекту як програму, яка буде не просто моделлю розуму, вона в буквальному розумінні слова сама й буде розумом [6]. Також за допомогою штучного інтелекту людина може легко перевірити достовірність інформації та наявність реальних джерел

інформації, що будуть відповідати дійсності. Ці прості та невимогливі дії допоможуть особі не стати жертвою інформаційної війни. Однак щодо використання штучного інтелекту для національних систем кібербезпеки є певні побоювання, оскільки законодавчі системи технологічно просунутих країн прагнуть регламентувати, регулювати й обмежувати використання GenAI систем [7]. Тому слід бути вельми обережним та використовувати штучний інтелект лише для тих цілей, які будуть корисними для вас та не спричинять шкоди та поганого впливу на середовище та людей навколо вас.

ЛІТЕРАТУРА:

1. Думчиков М. О., Думчиков М. А., Dumchykov M. O. Кібератаки як новітня загроза інформаційній безпеці : thesis. 2020. URL: https://essuir.sumdu.edu.ua/handle/123456789/77915 (дата звернення: 02.04.2024).

2. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки : монографія. Київ : НАУ, 2013. 432 с.

3. Калетнік В., Калетнік Н. Кібератаки як ключові елементи «інформаційної війни» Російської Федерації. *Молодий вчений*. 2022. № 1 (101). С. 37–42. URL: https://doi.org/10.32839/2304-5809/2022-1-101-8 (дата звернення: 02.04.2024).

4. Бондаренко М. С. Некарані дії за кібератаки на сайти державних установ. *Legal science, legislation and law enforcement practice: regularities and development trends*. 2020. URL: https://doi.org/10.30525/978-9934-588-92-1-73 (дата звернення: 02.04.2024).

5. Libicki M. C. Conquest in Cyberspace: National Security and Information Warfare. Cambridge University Press, 2007. 323 с.

6. Сморжевський Н. В. Штучний інтелект: перспективи розвитку : thesis. 2019. URL: https://er.knutd.edu.ua/handle/123456789/14286 (дата звернення: 02.04.2024).

7. Бойко В., Василенко М., Слатвінська В. Програмування за допомогою систем генеративного штучного інтелекту: ризики та виклики. *Information technology and society*. 2023. № 2 (8). С. 18–26. URL: https://doi.org/10.32689/maup.it.2023.2.2 (дата звернення: 02.04.2024).

Рудов Я. В.

студент групи МП-11,

науковий керівник ***Будник Л.А.****,*

к.е.н., доцент кафедри безпеки та правоохоронної діяльності,

Західноукраїнський національний університет

ШТУЧНИЙ ІНТЕЛЕКТ ТА ПРАВОВА ОСВІТА: ЯК ЗМІНИТЬСЯ НАВЧАННЯ ТА ПІДГОТОВКА ЮРИСТІВ

Штучний інтелект (ШІ) має потенціал вплинути на багато сфер людського життя, включаючи правову сферу та освіту майбутніх юристів. Цей вплив є різностороннім, змінюючи підходи до навчання та підготовки юристів.

Перш за все, інтеграція штучного інтелекту в навчальні програми є ключовим аспектом змін. Університети та юридичні факультети можуть розробляти нові курси та модулі, що присвячені розумним технологіям та їх впливу на правову практику. Спеціалізовані курси з правової технології можуть стати нормою, охоплюючи такі аспекти, як розробка правових додатків та використання блокчейну.

Подальший крок - підготовка майбутніх юристів до роботи зі штучним інтелектом в правовій практиці. Штучний інтелект (ШІ) знайшов широке застосування в сфері юридичних послуг, зокрема у аналізі контрактів. Автоматизовані системи спрощують процес аналізу