Список використаних джерел:

1. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 р. №80/94-ВР URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text.
2. Задорожнюк Н. О. Сучасні технології бізнес-аналітики. Економічна аналітика: сучасні реалії та прогностичні можливості : збірник матеріалів міжнар. наук.-прак. конф. (Київ, 19 квітня 2019 р.). Київ, 2019. С. 105–107.
3. Ляпін К. Е. Виклики та можливості сучасності: комплексна система захисту інформації. Збірник матеріалів VI міжнародної науково-практичної конференції «Інформаційна безпека та комп'ютерні технології»: тези доповідей, 20-21 квітня 2023 р. Кропивницький: ЦНТУ, 2023. 96 с.
4. Яремчук Ю. Є. Комплексні системи захисту інформації: навч. посіб. та ін. 63-тє вид. Вінниця: ВНТУ, 2018. 119 с.
5. Кудінов В. А., Яровий К. В. Інформаційне забезпечення правоохоронної діяльності: навч.-практ. посіб. Київ: Нац. акад. внутр. справ, 2024. 120 с.

Кедик Єлизавета Миколаївна
курсант 203 навчальної групи ННІ № 3 НАВС, рядовий поліції

Науковий керівник:
Яровий Кирило Васильович
кандидат юридичних наук, старший викладач кафедри інформаційних технологій та кібербезпеки ННІ № 1 НАВС, капітан поліції

ПРОБЛЕМИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КОМП'ЮТЕРНИХ СИСТЕМАХ

В інформаційному суспільстві спостерігається експонентне зростання інтенсивності процесів інформаційного обміну та обробки даних, що викликає необхідність використання потужних комп'ютерних систем. До таких систем пред'являють такі вимоги, як висока швидкодія, великий обсяг пам'яті, здатність обробляти велику кількість транзакцій одночасно, підвищена надійність.

Надійність, яка є однією з головних вимог до комп'ютерних систем, адже від рівня надійності системи залежить, наскільки відповідальні інформаційні процеси їй можна довірити. Оскільки абсолютна надійність комп'ютерних систем та результатів інформаційних процесів, які у них виконуються, не може бути забезпечена, задачею досліджень є визначення критичних областей, де такі помилки та збої в роботі не допустимі.

В сучасних умовах глобалізації інформаційна безпека виступає одним з найголовніших чинників забезпечення умов реалізації національних інтересів, спроможності держави долати кризові явища при зовнішній агресії [1, с. 23]. Своєчасні ефективні заходи щодо управління інформаційною безпекою з боку держави, як основного суб'єкта забезпечення інформаційної безпеки, здатні подолати загрози соціально-економічному та політичному життю країни.

Штучний інтелект представляє собою результат людської діяльності здатний до логічного мислення, управління своїми діями, обґрунтовування своїх рішень, які не може коректувати в разі зміни умов.

ШІ (англ. Artificial Intelligence, або AI) – це набір технологій та методів, що здатні аналізувати дані, робити прогнози і виконувати завдання, які зазвичай вимагають людського розуму, такі як розпізнавання образів, прийняття рішень та взаємодія і з людьми [2, с. 94]. Зазначене тлумачення визначає ШІ, як потужний інструмент, спроможний виконувати завдання, які раніше виконувалися виключно за допомогою людських можливостей [3, с. 352].

Сьогодні, поширене використання ШІ призводить до масової автоматизації робочих місць, що призводить до великих соціальних викликів, а саме втрати цінності людської праці.

Основні труднощі при впровадженні штучного інтелекту в комп'ютерні системи полягають у неможливості передбачити всі можливі реальні ситуації та програмувати поведінку машини адекватно до них, а також у недостатній надійності та програмних помилках. Вхідні дані, на основі яких навчається штучний інтелект, можуть бути неточними.

Крім того, вказані недоліки при використанні систем штучного інтелекту призвели до безлічі інцидентів, включаючи ті, що мають летальний характер. Аналіз повідомлень про помилки штучного інтелекту дозволив визначити критичні помилки, які відносяться до таких сфер, де застосування систем штучного інтелекту пов'язане з великим ризиком [4, с. 21]. Це такі галузі, як медицина, військові дії, транспорт, виробництво, де працюють люди та роботизовані системи, небезпечні виробництва, ядерна енергетика, соціальне управління, судові процеси і таке інше.

Дослідники стверджують, що штучний інтелект - це ніщо інше, як програма, яка ґрунтується на статистиці. Точність роботи таких програм не перевищує 95% [4, с. 125].

Отже, при такому рівні недоліків необхідно бути обережними щодо довіри до систем штучного інтелекту у сферах, де на кону стоять людські життя. Розробники комп'ютерних систем з штучним інтелектом мають обов'язок забезпечити вбудовування в алгоритми процесів, які запобігають можливість шкоди людині. Хоча алгоритми стають все більш адекватними у моделюванні реальних ситуацій, вони ніколи не будуть ідеальними або бездоганними. Питання про припустимий рівень помилок, вартість помилки та переваги заміни людей на штучний інтелект

завжди буде на порядку денному. У майбутньому людина все ще буде приймати критичні рішення, незважаючи на розумність систем штучного інтелекту.

На сьогоднішній день немає жодних законодавчих норм, що регулювали б саме використання штучного інтелекту. Штучний інтелект, використовуваний у критично важливих інфраструктурах і галузях, пов'язаних із здоров'ям та безпекою людей, вважається високоризиковим. В світі структури перебувають на переломному етапі через застосування більш сучасного обладнання та програмного забезпечення для інформаційної безпеки. Зарубіжні фахівці з інформаційної безпеки підкреслюють значний потенціал інформаційного та психологічного впливу в умовах стрімкого розвитку технологій штучного інтелекту. Штучний інтелект може бути важливим інструментом моніторингу загроз та захисту персональних та державних даних у світлі впровадження нових моделей та технологій.

Список використаної літератури:

1. Гуржій Т. Інформаційне право: виклики гібридної війни. Зовнішня торгівля: економіка, фінанси, право. 2018. № 4. С. 16–26.

2. Карпенко Ю. В. Етичні принципи застосування штучного інтелекту в публічному управлінні / Ю. В. Карпенко // Вісник Національної академії державного управління при Президентові України. – 2019. – №4. – С. 93-97.

3. Яровий К. В. Актуальні проблеми управління інформаційною безпекою держави: зб. матер. всеукр. наук.-практ. конференції. Київ : Нац. акад. СБУ, 2023. 618 с.

4. Ніщименко О. А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. Наше право. 2016. № 1. С. 17–23.

5. Радутний О. Е. Кримінальна відповідальність штучного інтелекту. Інформація і право. 2017. № 2 (21). С. 124–132.