КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

УДК 004.8+614.8+331.452 DOI: https://doi.org/10.32515/2664-262X.2022.5(36).1.119-124

К.М. Марченко, доц., канд. техн. наук, **О.В. Оришака**, доц., канд. техн. наук,
А.К. Марченко, А.М. Мельник
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна
e-mail: k_marchenko@i.ua, oryhsaka@gmail.com

Ризики впровадження штучного інтелекту в комп'ютерні системи

У статті розглянуті питання автоматизованої обробки інформації в комп'ютерних системах. Розглянуті вимоги, яким повинні відповідати комп'ютерні системи. Підкреслюється неможливість забезпечення абсолютної надійності алгоритмів та програмного забезпечення комп'ютерні системи, отже, повної адекватності отриманих рішень. Проаналізовані сфери використання штучного інтелекту та зроблені висновки про доцільність та безпечність його впровадження в окремих галузях з точки зору безпеки життєдіяльності людей та охорони праці.

обробка інформації, комп'ютерні системи, обчислювальні системи, алгоритм, програне забезпечення, надійність, штучний інтелект, ризики, безпека життєдіяльності, охорона праці

Постановка проблеми. В інформаційному суспільстві об'єм інформації, що виробляється людством, стрімко зростає, що зумовлює також значну інтенсифікацію інформаційних процесів, зокрема процесів інформаційного обміну та обробки даних. Інформаційні процеси такої інтенсивності на сьогодні покладаються на швидкісні комп'ютерні мережі та потужні комп'ютерні системи.

Комп'ютерна система (обчислювальна система) – будь-який пристрій чи група взаємопов'язаних чи суміжних пристроїв, один або більше з яких, діючи відповідно до програми, здійснює автоматизовану обробку даних [1]. Зокрема, потужні комп'ютерні системи використовуються в науці, в системах комерційного співробітництва, в підтримці прийняття рішень, прогнозуванні, інформаційно-управлінських системах, військовій справі, медицині, державному управлінні тощо.

До таких комп'ютерних систем пред'являють підвищені вимоги, зокрема, такі як надвисока продуктивність, великий обсяг пам'яті, здатність обробляти велику кількість транзакцій одночасно, підвищена відмовостійкість, стійкість до кібератак та надійність.

Аналіз останніх досліджень і публікацій. Надійність, яка є однією з головних вимог до комп'ютерних систем, складається з надійності пристроїв та засобів зв'язку, алгоритмів, програмного забезпечення та надійності (достовірності) результатів обробки даних [2]. У комп'ютерних науках (інформатиці) надійність – це здатність комп'ютерної системи справлятися з помилковими даними та помилками під час виконання завдань [3]. Від рівня надійності системи залежить, наскільки відповідальні інформаційні процеси їй можна довірити. Надійність комп'ютерної системи закладається на етапах проектування, виготовлення, програмування та експлуатації і забезпечується дотриманням значної множини умов. Тестування відповідальних систем викликає потребу в великому обсязі експериментів та досить тривалому спостереженні.

Підвищення надійності інформаційних систем досліджено у роботі [4] та інших. У роботі [5] та деяких інших підкреслюється неможливість досягнення абсолютної надійності комп'ютерних систем, зокрема, рекомендується досягати надійності, відповідної допустимому ризику.

Постановка завдання. 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.

Виклад основного матеріалу. Розробникам складних комп'ютерних систем та програмного забезпечення важко уникнути помилок, бо ймовірність помилки залежить від складності системи. В ідеальній ситуації програмні баги виправляють всі й одразу. У реальному житті насамперед знаходяться і виправляються очевидні та явні проблеми. Інші тихо чекають свого часу, перетворюючись на бомби уповільненої дії. Іноді помилки у програмному забезпеченні викликають справжні катастрофи [6]. Так кілька років у середині 80-х років апарати Therac-25 променевої терапії працювали бездоганно, проте згодом почали накопичуватися інциденти, що спричинили тяжкі наслідки: від ампутації кінцівок до загибелі пацієнтів. 14 серпня 2003 року невелика помилка у програмному забезпеченні системи моніторингу роботи обладнання General Electric Energy призвела до того, що 55 мільйонів людей залишилися без електрики. На Східному узбережжі США опинилися знеструмленими житлові будинки, школи, лікарні, аеропорти. У 1962 році космічний корабель "Mariner 1" був знищений із землі після старту через відхилення від курсу. Аварія виникла на ракеті через програмне забезпечення, в якому розробник пропустив лише один символ. Таких прикладів безліч.

Еволюція інформаційних та комп'ютерних систем пройшла декілька етапів у напрямку все більшої автоматизації обробки інформації. З кінця XX сторіччя інформаційні та комп'ютерні системи розвивалися в напрямку застосування підтримки прийняття рішень, експертних систем і систем штучного інтелекту.

На сьогодні не існує єдиного та однозначного визначення штучного інтелекту. Будемо вважати, що штучний інтелект – це інформаційна система або машина, яка здатна імітувати людину в процесах обробки інформації та прийнятті рішень, яка може навчатися та удосконалювати себе на основі отриманої інформації.

Сферами використання штучного інтелекту у нинішній час є пошукові системи, рекомендаційні системи, словники та перекладачі, розпізнавання та синтез мови, розпізнавання об'єктів, військова справа, медицина, системи масового обслуговування, керування виробничими процесами, керування різноманітними пристроями та обладнанням, транспорт, бізнес-аналітика, інтелектуальні системи інформаційної безпеки тощо.

Головними проблемами впровадження штучного інтелекту в комп'ютерні системи є неможливість передбачити всі реальні ситуації та запрограмувати поведінку машини адекватно до них, недостатня надійність та помилки у програмному забезпеченні. Вхідні дані, на основі яких навчається штучний інтелект можуть бути хибними. Крім того на системи штучного інтелекту впливають спосіб мислення та цінності його розробників, які не завжди обізнані з психологією, соціологією та іншими гуманітарними науками.

Ці недоліки за час використання систем штучного інтелекту привели до безлічі інцендентів, в тому числі летального характеру.

Так, весною 2018 року Uber тестувала безпілотний автомобіль на базі однієї з моделей Volvo на вулицях міста Темп у штаті Арізона, США. Машина збила жінку на смерть [7].

Медичний чат-бот на базі GPT-3, який було створено, щоб зменшити навантаження на лікарів, порадив підставному пацієнтові вбити себе. Творець чат-бота, французька компанія Nabla, зробила висновок, що «нестійкий і непередбачуваний характер відповідей програмного забезпечення робить його непридатним для взаємодії з пацієнтами в реальному світі».

У Великобританії робот-хірург фактично вбив пацієнта під час операції на серці. Кардіохірург Сукумаран Наір, який приймав участь в операції, зазначає, що насамперед люди повинні повністю розібратися у роботизованих помічниках у тих ситуаціях, коли це стосується людських життів.

На заводі Volkswagen у Німеччині людина була вбита роботом, що вийшов з-під контролю. Інцидент на заводі Volkswagen – не поодинокий випадок убивства людини роботом. Подібна пригода була вперше зафіксована у 1979 році на заводі ще одного великого автомобільному концерну – Ford.

Ще одною загрозою є здатність систем штучного інтелекту створювати та публікувати в соціальних мережах тексти, наслідуючи стиль людини. Так бот, створений програмою GPT, видавав себе за людину протягом кількох тижнів. Тексти, створені таким чином, важко розпізнати як штучні. Через такі тексти та повідомлення машина може впливати на емоції людини та створювати певний інформаційний фон, формувати думку, підштовхувати людину до певних дій та вчинків.

Значною загрозою також є застосування недостатньо навченого штучного інтелекту у життєво важливих сферах, спроби його використання для того, щоб поставити під контроль життя людини.

Ці приклади показують, що проблеми впровадження систем штучного інтелекту лежать в полі уваги багатьох наук – не лише комп'ютерних, а також безпеки життєдіяльності, охорони праці, юриспруденції, психології, соціології, етики та інших.

Чи можна довірити штучному інтелекту прийняття рішень у відповідальних ситуаціях?

За висловом Г. Грефа, голови Збербанку Росії, «Штучний інтелект, як правило, ухвалює рішення у великих системах. Маленька помилка, що закралася в алгоритм, може спричинити дуже великі наслідки. Через те, що машина робила маленьку помилку, на великих обсягах ми втрачали мільярди рублів».

26 вересня 1983 року супутник ешелону «Око» системи попередження про ракетний напад СРСР помилково повідомив про запуск п'яти балістичних ракет з території США. Тільки втручання у прийняття рішення людини - чергового офіцера запобігло початку Третьої світової війни [6].

Аналіз вибірки повідомлень про помилки штучного інтелекту дозволив визначити, до яких сфер відносяться критичні помилки, тобто де застосування систем штучного інтелекту пов'язане із значним ризиком. Зокрема, це такі галузі як медицина, військова справа, транспорт, виробництво, де співпрацюють люди та роботизовані системи, небезпечні виробництва, енергетика, соціальне управління, правові установи тощо.

Дослідник штучного інтелекту О. Хомяков стверджує, що штучний інтелект є не що інше, як програма, заснована на статистиці. Точність роботи таких програм не перевищує 95%. Отже, при такому рівні похибок не варто довіряти таким системам людські життя [8].

Ризики використання штучного інтелекту створюються самими людьми: його ідеологами – початково хибні ідеї; розробниками – помилки в алгоритмах та програмному забезпеченні; особами, на яких покладається контроль за функціонуванням, навчанням, достовірністю підключених джерел інформації; користувачами – не вірна експлуатація.

Обов’язком розробників комп’ютерних систем із штучним інтелектом є попередити закладення в алгоритми процесів, які можуть зашкодити людині [10]. В алгоритми закладаються певні показники точності, що передбачає можливість помилок. Помилки також можуть накопичуватися в процесі навчання системи. На теперішній час основний засіб контролю за адекватністю алгоритму — відсутність у нього можливості приймати критично важливі рішення самостійно. Людина обов'язково бере участь у прийнятті рішень, а алгоритм постає як помічник та радник.

Алгоритми вчаться більш адекватно моделювати реальні ситуації але вони ніколи не стануть досконалими та безпомилковими. На думку експерта Л.Жукова, питання про допустимий поріг помилок, ціни за помилку та економію від заміни людини штучним інтелектом стоятиме завжди. У найближчому майбутньому людина, як і раніше, прийматиме критичні рішення, хоч би якою розумною не була система штучного інтелекту [9].

Не вирішеним юридично залишається питання відповідальності за помилки штучного інтелекту: хто і в яких випадках має за них відповідати – розробник чи особа, яка ним користується, чи сам штучний інтелект. На сьогодні не існує жодних законодавчих норм, які б регулювали саме штучн ий інтелект [10]. Нормативне урегулювання в використанні систем штучного інтелекту знаходиться на стадії початкових спроб. Так Комісія Європейського Союзу класифікувала штучний інтелект за рівнями ризику та виявила намір чітко визначити, що може бути дозволено, а що заборонено у впроваджені штучного інтелекту в комп’ютерні системи та суспільне життя.

Висновки.

1. В теперішній час відсутні нормативна та законодавча бази з використання штучного інтелекту, тому його впровадження відбувається стихійно, що приводить до непередбачуваних результатів та аварій.

2. Штучний інтелект, що використовується в критично важливих інфраструктурах, у галузях, пов’язаних із здоров’ям та життям людей, відноситься до категорії високого ризику.

3. Засновуючись на проведеному аналізі та у зв’язку з неможливістю забезпечення абсолютної надійності комп’ютерних систем і їх програного забезпечення, автори не рекомендують використовувати штучний інтелект у сферах, пов’язаних з безпекою, здоров’ям та життям людини, особливо великих людських колективів. Пристрої, в яких використовуються системи штучного інтелекту, слід маркувати повідомленнями про його використання із зрозумілим попередженням про часткову надійність пристрою в сенсі безпеки та відповідальність споживача за використання такого пристрою.

4. Автори категорично не рекомендують використання штучного інтелекту у прийнятті відповідальних рішень у сферах, пов’язаних із безпекою великих груп людей.

Список літератури

1. Комп’ютерна система. Матеріал Вікіпедії. URL: https://uk.wikipedia.org/wiki /Категорія:Комп%27ютерні_системи (дата звернення: 06.03.2022)
2. Мальков, М.В. О надежности информационных систем . *Труды Кольского научного центра РАН*. 2012. Т. 3, №4. С. 49-58.
3. Надёжность (компьютерные науки). Материал Википедии. URL: https://ru.wikipedia.org/wiki/Надёжность_(компьютерные_науки) (дата звернення: 06.03.2022)
4. Бычков С. С. Повышение уровня надежности информационных систем . *Вестн. СибГАУ им. М. Ф. Решетнева*. 2014. № 3. С. 42-47.
5. Казарин О. В., Шубинский И. Б. Надежность и безопасность программного обеспечения : учеб. пособие для бакалавриата и магистратуры. М. : Издательство Юрайт, 2018. 342 с.

6. Катастрофические последствия программных ошибок. Стаття на сайті https://www.pvsm.ru/programmirovanie/241956 (дата звернення: 06.03.2022)
7. ИИ посоветовал пациенту умереть: самые крупные ошибки машинного обучения. URL: https://hightech.fm/2021/09/02/ai-failures (дата звернення: 06.03.2022)
8. Плохо обученный искусственный интеллект опаснее восстания машин. URL: https://www.hse.ru/news/expertise/506082229.html (дата звернення: 07.03.2022)
9. Жуков Л. Почему люди в ближайшем будущем не смогут полностью довериться ИИ. URL: https://trends.rbc.ru/trends/industry/5fb52daf9a7947234c4d28d3 (дата звернення: 07.03.2022)
10. Андраш Ю. Кто несет ответственность за преступления искусственного интеллекта? URL: https://www.lansky.at/ru/newsroom/news-media/zhurnal-lgp-news-022021/kto-neset-otvetstvennost-za-prestuplenija/# (дата звернення: 07.03.2022)

References

1. Kompiuterna systema. Material Vikipedii. *uk.wikipedia.org.* Retrieved from https://uk.wikipedia.org/wiki/Katehoriia:Komp%27iuterni_systemy [in Ukrainian]
2. Mal'kov, M.V. (2012). O nadezhnosti informacionnyh sistem [On the reliability of information systems]. *Trudy Kol'skogo nauchnogo centra RAN – Proceedings of the Kola Scientific Center of the Russian Academy of Sciences. Vol. 3, 4*, 49-58 [in Russian].
3. Nadjozhnost' (komp'juternye nauki). Material Vikipedii [Reliability (computer science). Wikipedia material]. *ru.wikipedia.org.* Retrieved from https://ru.wikipedia.org/wiki/Nadëzhnost_ (kompiuternыe_nauky) [in Russian].
4. Bychkov, S.S. (2014). Povyshenie urovnja nadezhnosti informacionnyh sistem [Increasing the level of reliability of information systems]. *Vestn. SibGAU im. M. F. Reshetneva – Vestn. Siberian State Agrarian University M. F. Reshetnev, 3,* 42-47 [in Russian].
5. Kazarin, O.V. & Shubinskij, I.B. (2018). *Nadezhnost' i bezopasnost' programmnogo obespechenija* [*Software reliability and security*]. Moskow : Izdatel'stvo Jurajt, [in Russian].
6. Katastroficheskie posledstvija programmnyh oshibok [Catastrophic consequences of software errors]. *www.pvsm.ru.* Retrieved from https://www.pvsm.ru/programmirovanie/241956 [in Russian].
7. II posovetoval pacientu umeret': samye krupnye oshibki mashinnogo obuchenija [AI advised the patient to die: the biggest machine learning mistakes]. *hightech.fm.* Retrieved from https://hightech.fm/2021/09/02/ai-failures [in Russian].
8. Ploho obuchennyj iskusstvennyj intellekt opasnee vosstanija mashin [Poorly trained artificial intelligence is more dangerous than the uprising of machines]. *www.hse.ru.* Retrieved from https://www.hse.ru/news/expertise/506082229.html [in Russian].
9. Zhukov, L. Pochemu ljudi v blizhajshem budushhem ne smogut polnost'ju doverit'sja II [Why people in the near future will not be able to fully trust A]. *trends.rbc.ru.* Retrieved from https://trends.rbc.ru/trends/industry/5fb52daf9a7947234c4d28d3 [in Russian].
10. Andrash Yu. Kto neset otvetstvennost za prestuplenyia yskusstvennoho yntellekta? [Who is responsible for the crimes of artificial intelligence?] *www.lansky.at.* Retrieved from https://www.lansky.at/ru/newsroom/news-media/zhurnal-lgp-news-022021/kto-neset-otvetstvennost-za-prestuplenija/# [in Russian].

Konstantyn Marchenko, Assoc. Prof., PhD tech. sci., **Oleh Oryshaka**, Assoc. Prof., PhD tech. sci., **Anzhelyka Marchenko**, **Anna Melnick**
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine

Risks of Implementing Artificial Intelligence in Computer Systems

Since the absolute reliability of computer systems and the results of information processes that run in them can not be guaranteed, the task of research is to identify critical areas where such errors and failures are unacceptable.

The main problems with the introduction of artificial intelligence in computer systems are the inability to predict all real situations and program the behavior of the machine adequately to them, lack of reliability and software errors. The input on which artificial intelligence is taught may be incorrect. In addition, artificial intelligence systems are influenced by the way of thinking and values of its developers, who are not always familiar with psychology, sociology and other humanities. These shortcomings during the use of artificial intelligence systems have led to many incidents, including fatal. The analysis of the sample of artificial intelligence error messages allowed us to determine which areas are critical errors, ie where the use of artificial intelligence systems is associated with significant risk. In particular, these are such areas as medicine, military

affairs, transport, manufacturing, where people and robotic systems cooperate, hazardous industries, energy, social management, legal institutions and more.

Currently, there is no regulatory and legal framework for the use of artificial intelligence, so its implementation is spontaneous, which leads to unpredictable results and accidents. Artificial intelligence used in critical infrastructures, in areas related to human health and life, belongs to the category of high risk. Based on the analysis and due to the impossibility of ensuring the absolute reliability of computer systems and their software, the authors do not recommend the use of artificial intelligence in areas related to safety, health and human life, especially large human teams. Devices using artificial intelligence systems should be marked with messages about its use with a clear warning about the partial reliability of the device in terms of safety and consumer responsibility for the use of such a device. The authors strongly discourage the use of artificial intelligence in responsible decision-making in areas related to the security of large groups of people.

information processing, computer systems, computer systems, algorithm, software, reliability, artificial intelligence, risks, safety of life, labor protection

Одержано (Received) 08.03.2022 *Прорецензовано (Reviewed) 17.03.2022*
Прийнято до друку (Approved) 31.03.2022

УДК 004.4 DOI: https://doi.org/10.32515/2664-262X.2022.5(36).1.124-134

В.В. Босько, доц., канд. техн. наук, **Л.В. Константинова,** викл., **О.К. Конопліцька-Слободенюк,** викл., **Д.В Фесечко,** магістр
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна
e-mail: victorvv2@ukr.net, liliyashel1976@gmail.com, ksuha80@gmail.com

Аналіз та дослідження фреймворку AngularJS як засобу розробки вебсайтів

Наведено аналіз фреймворку AngularJS на підтримку використання повноцінних класів, на наявність модульної архітектури, зв'язування даних, компонентів, що пришвидшують роботу та спрощують налагодження програм, а також сильних сторін в порівнянні з іншими фреймворками.

Також в роботі проаналізовано можливості розробки вебсайтів засобами фреймворку AngularJS. Для цього було проведенно дослідження та програмну реалізацію різних типів вебсайтів засобами фреймворку AngularJS. Розглянуто його недоліки й переваги. Результатом аналізу є обгрунтування вибору фреймворку при розробці вебсайтів в залежності від поставлених задач.

комп'ютерна інженерія, вебсайт, фреймворк, AngularJS

Постановка проблеми. Фронтенд розробка є дуже важливим напрямком в IT-індустрії, так як вона є «фасадом» вебдодатку. Головними критеріями оцінок при розробці вебдодатку є його економічна складова, трудоємкість інтеграції, UI, UX, а також при розробці важливим враховується наявність документації по API. Застосування фреймворку може прискорити та спростити процес розробки вебдодатків. Тому дослідження фреймворку AngularJS, як засобу розробки вебсайтів та аналіз результатів є актуальним сьогодні.

AngularJS була випущена компанією Google у 2010 році, як новаторська технологія у світі веброзробки. Вона впровадила нові стандарти у розробку вебсайтів, та випустила ряд потужних інноваційних технологій. Ця платформа стала кроком уперед у створенні прогресивних вебдодатків. Але з часом команда Google, побачила недоліки в AngularJS, які неможливо було вирішити шляхом еволюції технологій та оновлень, і використала отриманий досвід, щоб переробити фреймворк з нуля.