

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»

**ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ:
НАУКОВО-ПРАКТИЧНИЙ ВИМІР
В УМОВАХ ВОЄННИХ ВИКЛИКІВ**

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 26 квітня 2024 року

Одеса
«Фенікс»
2024

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)
Є 24

*Рекомендовано до друку вченою радою
Національного університету «Одеська юридична академія»
(протокол № 8 від 15.05.2024 р.)*

За загальною редакцією **С. В. Ківалова**

Відповідальний за випуск **М. Р. Аракелян**

Є 24 **Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів** : матеріали Міжнар.наук.-практ. конф. (Одеса, 26 квітня 2024 р.) / за заг. ред. С. В. Ківалова. – Одеса : Фенікс, 2024. – 1000 с.
ISBN 978-617-8430-05-4

У збірнику відображено наукові напрацювання вчених, практиків, військовослужбовців у теоретичній та емпіричній площині у сферах філософських основ, загальної теорії та історичних досліджень держави і права, актуальних проблем світових соціально-політичних процесів, соціології та психології в умовах повномасштабного військового вторгнення. Висвітлено питання загроз національній безпеці в їх конституційному вимірі у рамках міжнародного та європейського права, трудового права та права соціального забезпечення, земельного, аграрного та екологічного права, пов'язані з функціонуванням економіки та підприємництва в умовах європейського вибору України. Розглянуто проблеми інформатизації та цифровізації суспільства, захисту інформації та кібербезпеки в умовах військового вторгнення, питання методики викладання іноземних мов, теорії та практики перекладу, проблеми лінгвістики та журналістики. Відображено наукові напрацювання у сферах адміністративного права та процесу, фінансового, морського та митного права, організації та вдосконалення судоустрою, прокуратури, інших правоохоронних органів, адвокатури. Висвітлено питання кримінального права, кримінально-процесуальних аспектів кримінального провадження та кримінологічних особливостей протидії злочинності в умовах воєнного стану, криміналістики, судової експертизи, психології та медицини у забезпеченні судочинства, цивільного та сімейного права, інтелектуальної власності та патентної юстиції, цивільного судочинства, господарського права та процесу. Розглянуто актуальні питання діяльності сучасних бібліотек у закладах вищої освіти, фізичної підготовки здобувачів вищої освіти.

Збірник розраховано на наукових і науково-педагогічних працівників, здобувачів вищої освіти, практичних працівників у сферах юридичної, економічної, соціологічної, політологічної, психологічної, філологічної наук, журналістики та кібербезпеки тощо.

УДК 005.332.2(4):316.42(477)»364»»20»(062.552)

Матеріали видано в авторській редакції

ISBN 978-617-8430-05-4

© НУ «Одеська юридична академія, 2024
© Автори статей, 2024

<i>Лобода Юлія Геннадіївна</i> ГЕНЕРАЦІЯ НАБОРУ ДАНИХ ДЛЯ МАШИННОГО НАВЧАННЯ.....	860
<i>Манаков Сергій Юрійович</i> ВІРТУАЛЬНІ ПОТОКИ JAVA ТА КОРУТИНИ KOTLIN	862
<i>Чанишев Рашид Ібрагімович</i> ШТУЧНИЙ ІНТЕЛЕКТ ТА ПРАВО: ВИКЛИКИ ТА ПЕРСПЕКТИВИ РЕГУЛЮВАННЯ.....	864
<i>Чикунів Павло Олександрович</i> ВІДСТЕЖЕННЯ ПОШИРЕННЯ ПО ПРОГРАМІ НЕПЕРЕВІРЕНИХ ЗОВНІШНІХ ДАНИХ.....	866
<i>Щербина Юрій Володимирович</i> <i>Казакова Надія Феліксівна</i> ДОСЛІДЖЕННЯ ПОТОЧНОГО ШИФРУ, ПОБУДОВАНОГО НА ОСНОВІ XORSHIFT-ГЕНЕРАТОРА	870
<i>Грезіна Олена Миколаївна</i> ЦИФРОВА МАЙСТЕРНІСТЬ ТА ІННОВАЦІЇ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ – БЕЗПЕКОВІ ВИКЛИКИ ДЛЯ СФЕРИ ОСВІТИ	872
<i>Соловйов Артем Сергійович</i> ПРОБЛЕМАТИКА ФАЛЬСИФІКАЦІЇ СИСТЕМНИХ ЖУРНАЛІВ У ОПЕРАЦІЙНІЙ СИСТЕМІ LINUX	874
<i>Дика Анастасія Іванівна, Трофименко Олена Григорівна</i> АНАЛІЗ ПОТЕНЦІЙНИХ ЗАГРОЗ ЗАСОБАМИ SNATGPT ДЛЯ ТЕСТУВАННЯ БЕЗПЕКИ ВЕБЗАСТОСУНКІВ.....	876
<i>Проданюк Назар Богданович</i> ДЕЯКІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ДОСТУПНОСТІ ЮРИДИЧНИХ ПОСЛУГ У ЦИФРОВУ ЕПОХУ	878
<i>Світлічний Ігор Валерійович</i> <i>Світлічна Дар'я Ігорівна</i> ЧИ МАЮТЬ МИМОБІЖНІ ПРЯМІ ПРАВО НА ПЕРЕТИН? ДЕЯКІ АСПЕКТИ ЗНАХОДЖЕННЯ ВІДСТАНІ МІЖ МИМОБІЖНИМИ ПРЯМИМИ	880

СЕКЦІЯ 24. КІБЕРБЕЗПЕКА ОСОБИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ ЯК ФУНДАМЕНТАЛЬНИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

<i>Горбаченко Станіслав Анатолійович, Дикий Олег Вікторович</i> ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПРОЦЕСІ МАРКЕТИНГОВОГО ЦІНОУТВОРЕННЯ	883
<i>Казакова Надія Феліксівна, Кулешова Євгенія Романівна</i> ВИБІР ТИПУ ХМАРНИХ ПОСЛУГ ТА РИЗИК ВИТОКУ ЧУТЛИВОЇ ІНФОРМАЦІЇ.....	885
<i>Ахметмет'єва Ганна Валеріївна</i> ПРОБЛЕМИ РОЗПОВСЮДЖЕННЯ ФЕЙКОВИХ МУЛЬТИМЕДІА В МЕРЕЖІ INTERNET	887
<i>Бойко Віктор Дмитрович</i> БІБЛІОТЕКА NUMPY – ОСНОВА ІНСТРУМЕНТАЛЬНОГО СТЕКУ НАУКОВИХ РОЗРАХУНКІВ SCIPY.....	888
<i>Кухаренко Сергій Вікторович</i> ПОЛІТИКИ ТА ПРОЦЕДУРИ РЕАГУВАННЯ НА ПОРУШЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ.....	891
<i>Чепурна Олена Євгенівна</i> КІБЕРЗАГРОЗИ ДЛЯ БІЗНЕС-СЕРЕДОВИЩА ТА СУЧАСНІ ЗАХОДИ ПРОТИДІЇ	893
<i>Черевко Євген Володимирович</i> ШТУЧНИЙ ІНТЕЛЕКТ ТА ЙОГО ЗАСТОСУВАННЯ У ФУНДАМЕНТАЛЬНИХ ДОСЛІДЖЕННЯХ.....	895
<i>Овчинников Микола Юрійович</i> ОСОБЛИВОСТІ ВБУДОВУВАННЯ ПРИХОВАНОЇ ІНФОРМАЦІЇ У ФАЙЛИ ФОРМАТУ MP3	898
<i>Разінкін Нікіта Сергійович</i> КІБЕРЗАХИСТ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВІЙНИ.....	902
<i>Саврацький Олександр Олександрович</i> ОСОБЛИВОСТІ ПІДГОТОВКИ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ В УМОВАХ ВІЙНИ	905

СЕКЦІЯ 25. ПИТАННЯ МЕТОДИКИ ВИКЛАДАННЯ ІНОЗЕМНИХ МОВ, ТЕОРІЇ ТА ПРАКТИКИ ПЕРЕКЛАДУ ЯК ЗАСОБУ НАЛАГОДЖЕННЯ КОМУНІКАЦІЇ

<i>Томчаковська Юлія Олегівна</i> СТРАТЕГІЇ І ТАКТИКИ МЕДІЙНОГО ДИСКУРСУ	908
<i>Строченко Леся Василівна</i> ПЕРЕКЛАД У ВІЙСЬКОВІЙ ГАЛУЗІ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ	910
<i>Варешкіна Наталія Володимирівна</i> ДО ПРОБЛЕМИ ВИКЛАДАННЯ АНГЛІЙСЬКОЇ МОВИ ЗА ПРОФЕСІЙНИМ СПРЯМУВАННЯМ	911
<i>Дихта Наталя Миколаївна, Явдошук Анастасія Андріївна</i> НАВЧАННЯ ФОНЕТИЦІ АНГЛІЙСЬКОЇ МОВИ.....	913

ШТУЧНИЙ ІНТЕЛЕКТ ТА ПРАВО: ВИКЛИКИ ТА ПЕРСПЕКТИВИ РЕГУЛЮВАННЯ

Поняття «штучний інтелект» (далі – ШІ) (у його сучасному розумінні) з'явилося дуже давно, наприкінці 40 років ХХ століття, одночасно з появою такої науки, як кібернетика. Уже тоді вчені почали говорити про ризики, які стануть наслідком практичної реалізації цієї ідеї. На той час це було суто теоретичною проблемою, оскільки для практичної реалізації систем ШІ на той час не було технічної бази. Коли ж розвиток електроніки дав змогу створювати інтегральні схеми достатньої потужності, ШІ раптово (починаючи, приблизно, з 2018 року) увірвався в наше життя і дуже швидко став його невід'ємною частиною.

Як зазначають багато вчених, розвиток ШІ нині відбувається зі швидкістю, незрівнянно більшою, ніж розвиток інших систем інформаційних технологій. Кількість інтегральних схем, що використовуються в системах ШІ, за один рік збільшується в 2-5 разів, при цьому зростає і швидкість їхньої роботи, безперервно зростає ефективність алгоритмів навчання нейронних мереж, що дає змогу системам ШІ приблизно раз на два роки переходити на новий, вищий щабель розвитку.

Як наслідок, на відміну від багатьох інших короткочасно модних інформаційних технологій, практична реалізація систем штучного інтелекту, що реально працюють, спричинила кардинальні зміни майже в усіх сферах суспільного життя.

Такий швидкий розвиток і впровадження ШІ одразу ж повернув і страхи майже 70-річної давності. І хоча зараз майже ніхто не боїться того, що ШІ захопить владу над людством, інші негативні сторони загального використання ШІ стали проявлятися досить чітко.

Так, Даріо Амодей, голова відомої компанії Anthropic, що займається розробкою систем ШІ, виступив 2023 року в Конгресі США з попередженням про те, що новітні технології в галузі штучного інтелекту можуть найближчим часом стати інструментом у руках зловмисних осіб для здійснення масштабних біологічних атак. При цьому він послався на результати проведеного компанією Anthropic шестимісячного дослідження цієї проблеми і на заходи, вжиті цією компанією щодо запобігання використанню систем ШІ, які вона розробляє, для створення шкідливих вірусів [1]. Крім того, було висловлено побоювання, що аналогічні проблеми можуть мати місце в хімічній та ядерній сферах.

Спроби створення основ для правового регулювання систем штучного інтелекту розпочалися ще 2020 року. Так 2 грудня 2020 р. Кабінетом Міністрів України було затверджено «Концепцію розвитку штучного інтелекту в Україні» [2]. У квітні 2021 року в Європейському Союзі розпочалося розроблення The Artificial Intelligence Act, документа, завданням якого є правове регулювання штучного інтелекту на території країн Європейського Союзу [3].

У липні 2023 року було проведено і перше засідання ООН з питання ШІ. Генеральний секретар Організації підтримав пропозицію створити міжнародну організацію, метою якої буде створення світових стандартів з регулювання ШІ.

21 березня 2024 року Генасамблея ООН ухвалила резолюцію під назвою «Використання можливостей безпечних, захищених і надійних систем штучного інтелекту для сталого розвитку». Як зазначила Лінда Томас-Грінфілд, постійний представник США в ООН, «країни світу «вирішили керувати ШІ, і не допустити, щоб він керував людьми».

У цій резолюції, зокрема, висловлюється ідея про необхідність включення країн, що розвиваються, у процес цифрового перетворення, шляхом збільшення їхніх можливостей підключення до цифрової інфраструктури та доступу до технологічних нововведень.

Автори резолюції також пропонують вжити заходів для забезпечення дотримання прав на інтелектуальну власність, захисту конфіденційності та персональних даних, а також для забезпечення прозорості, передбачуваності та надійності функціонування систем штучного інтелекту впродовж усього їхнього життєвого циклу.

Згадка інтелектуальної власності пов'язана з тим, що найпершим негативним наслідком, який уже щосили проявився в усьому світі, стала проблема порушення авторських прав на інтелектуальну власність.

Так, 10 березня 2024 року було подано колективний позов до федерального суду міста Сан-Франциско проти компанії Nvidia. Три письменники: Брайан Кін, Абді Наземян і Стюарт О'Нан звинуватили цю компанію в тому, що Nvidia використовувала їхні книги, захищені авторським правом, для навчання своїх системи ШІ «NeMo», не отримавши на це їхнього дозволу.

Позивачі вимагають відшкодування збитків не тільки для себе, а й для всіх громадян Сполучених Штатів, чії роботи (196 640 книг), захищені авторським правом, використовувалися для навчання NeMo протягом останніх трьох років. Метою позову є законодавче обмеження можливості скрейпінгу (scraping, автоматичний збір даних) сервісами штучного інтелекту без виплати компенсації авторам текстів.

Крім того, став відомим випадок, коли 27 грудня 2023 року газета The New York Times подала до суду на компанії OpenAI і Microsoft, звинувативши їх у тому, що вони використовували мільйони статей газети без дозволу, щоб допомогти навчити чат-ботів надавати інформацію читачам [5].

У позові, поданому до федерального суду Мангеттена, OpenAI і Microsoft звинувачуються у спробі «нажитися на величезних інвестиціях The Times у журналістику», використовуючи їх для надання альтернативних засобів доставки інформації читачам.

У відповідь OpenAI і Microsoft заявили, що використання захищених авторським правом творів для навчання продуктів ШІ прирівнюється до «добросовісного використання». Ця правова колізія має бути вирішена в судовому порядку.

До речі, засновник і глава згаданої вище компанії Nvidia Дженсен Хуанг (Jensen Huang), виступаючи наприкінці лютого 2024 року на саміті World Government Summit у Дубаї, заявив, що, за оцінками цієї компанії, професія програміста скоро відійде в минуле, адже ШІ цілком здатний самостійно створювати програмний код за заданим технічним описом. За його словами, завдяки ШІ незабаром єдиною мовою програмування залишиться звичайна людська мова (точніше – prompt engineering) [6].

На сьогоднішній день використання ШІ все ще носить характер новизни, це скоріше розвага і навчання, ніж реальна користь. Однак, з огляду на сказане про темпи розвитку ШІ згаданим вище Даріо Амодеєм, усього лише через два-три роки ситуація може змінитися найкардинальнішим чином і серед постраждалих можуть опинитися не лише художники, письменники, журналісти й програмісти, а й звичайні громадяни всього світу.

У зв'язку з цим можна відзначити як позитивний фактор те, що багаторічне обговорення Закону ЄС «Про штучний інтелект» (The Artificial Intelligence Act) усе-таки дійшло до кінця – вже в квітні цього року його поставлять на голосування в Європарламенті, а чинності він набере орієнтовно в травні або червні. Протягом перших 6 місяців мають бути заблоковані заборонені системи ШІ, протягом року має бути забезпечено дотримання норм щодо «систем ШІ загального призначення», і протягом 3 років мають бути розроблені правові обмеження для систем ШІ «високорівневого ризику» [6].

Норми закону поділяються за рівнями ризику, які системи ШІ несуть для суспільства – «що вищий ризик, то суворіші правила».

Щодо збору даних для навчання ШІ новий Закон додаткових вимог не висуває – вони обмежуються вже чинним «Загальним регламентом щодо захисту даних» і чинними законами про авторське право.

Як висновок можна відзначити те, що прогрес удосконалення систем ШІ за швидкістю явно випереджає процес створення відповідного нормативно-правового забезпечення, що в результаті може призвести до абсолютно непередбачуваних наслідків.

Список використаних джерел

1. Dario Amodèi. For a hearing on “Oversight of A. I.: Principles for Regulation”. URL: https://www.judiciary.senate.gov/imo/media/doc/2023-07-26_-_testimony_-_amodei.pdf.
2. Чанишев Р. І. Проблеми розвитку та правового регулювання штучного інтелекту. *Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень* : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 19 трав. 2023 р.) : у 2 т. / за заг. ред. С. В. Ківалова. Одеса, 2023. С. 603–606.
3. Чанишев Р. І. Проект Ai Act: перша спроба правового регулювання використання технологій штучного інтелекту в Європейському Союзі. *Інформаційне суспільство: проблеми та перспективи* : матеріали VIII Всеукр. наук.-практ. конф. (м. Одеса, 2 черв. 2023 р.) / відп. ред. Н. І. Логінова. Одеса, 2023. С. 42–44. DOI: <https://doi.org/10.32837/11300.25263>.
4. Stempel J. Nvidia is sued by authors over AI use of copyrighted works. URL: <https://www.reuters.com/technology/nvidia-is-sued-by-authors-over-ai-use-copyrighted-works-2024-03-10>.
5. Stempel J. NY Times sues OpenAI, Microsoft for infringing copyrighted works. URL: <https://www.reuters.com/legal/transactional/ny-times-sues-openai-microsoft-infringing-copyrighted-work-2023-12-27>.
6. David E., Weatherbed J. The EU AI Act passed – here’s what comes next. URL: <https://www.theverge.com/2023/12/14/24001919/eu-ai-act-foundation-models-regulation-data>

Ключові слова: штучний інтелект, проблеми, що пов’язані із системами штучного інтелекту, правове регулювання систем штучного інтелекту, безпека людства, законодавство Європейського Союзу

Keywords: artificial intelligence, problems related to artificial intelligence systems, legal regulation of artificial intelligence systems, safety of mankind, European Union legislation

Чикунів Павло Олександрович

Національний університет «Одеська юридична академія»,

доцент кафедри інформаційних технологій,

кандидат технічних наук, доцент

ВІДСТЕЖЕННЯ ПОШИРЕННЯ ПО ПРОГРАМІ НЕПЕРЕВІРЕНИХ ЗОВНІШНІХ ДАНИХ

Taint-аналіз (taint checking) [1] – це метод аналізу текстів програм на мовах високого рівня, який дозволяє відстежувати поширення неперевіраних зовнішніх даних за програмою для виявлення потенційних безпекових загроз. Суть його полягає у відстеженні потенційно небезпечних або ненадійних даних, що вводяться у програму і можуть бути використані для атаки.

В процесі виконання програми taint-аналіз визначає, які дані можуть бути забруднені або підозрілими, і як вони можуть вплинути на безпеку програми. Основні заходи taint-аналізу включають відстеження потоку даних, визначення зв’язків між даними та їх джерелами, виявлення можливих точок витоку даних тощо. В результаті він допомагає підвищити безпеку програмного забезпечення шляхом виявлення та усунення можливих шляхів атаки.

Потрапляння неперевіраних даних у критичні секції коду може призвести до різних вразливостей, включаючи SQL-ін’єкцію (виконання зловмисником небажаних SQL-запитів), міжсайтовий скриптинг XSS (впровадження шкідливого коду у веб-сторінки, що відвідують інші