ДЕРЖАВНА НАУКОВА УСТАНОВА
«ІНСТИТУТ ІНФОРМАЦІЇ, БЕЗПЕКИ І ПРАВА
НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПРАВОВИХ НАУК УКРАЇНИ»

АПАРАТ ВЕРХОВНОЇ РАДИ УКРАЇНИ

ІНСТИТУТ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

ПРОБЛЕМИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ТА РОЗВИТКУ ПАРЛАМЕНТСЬКОГО КОНТРОЛЮ В КОНТЕКСТІ ЄВРОПЕЙСЬКОЇ ТА ЄВРОАТЛАНТИЧНОЇ ІНТЕГРАЦІЇ УКРАЇНИ

МАТЕРІАЛИ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

КИЇВ, 25 КВІТНЯ 2024 року

Київ
2024

2. L. Redei and I. Romanyshyn, “Non-parliamentary diplomacy: The European Parliament’s diplomatic mission to Ukraine,” European Foreign Affairs Review, vol. 24, no. 1, pp. 61-79, 2019. [Online]. Available: https://doi.org/10.54648/eerr2019005

3. T. L. Saaty, «How to make a decision: The analytic hierarchy process,» European Journal of Operational Research, vol. 48, no. 1, pp. 9-26, 1990. [Online]. Available: https://doi.org/10.1016/0377-2217(90)90057-I

4. M. Loya, D. Sinha, and R. Futrell, «Exploring the Sensitivity of LLMs’ Decision-Making Capabilities: Insights from Prompt Variation and Hyperparameters,» in Proc. of the Findings of the Association for Computational Linguistics: EMNLP 2023, Singapore, Dec. 2023, pp. 3711-3716. [Online]. Available: https://aclanthology.org/2023.findings-emnlp.241

5. D. Lande, L. Strashnoy, and O. Driamov, «Analytic Hierarchy Process in the Field of Cybersecurity Using Generative AI,» SSRN, Nov. 2, 2023. [Online]. Available: https://ssrn.com/abstract=4621732 DOI: 10.2139/ssrn.4621732.

Казьмірук С. Д.
аспірант ДНУ «Інститут інформації, безпеки і права НАПрН України»

Леонов Б. Д.
доктор юридичних наук, професор, головний науковий співробітник МНДЦ при РНБО України

АКТУАЛЬНІ ПРОБЛЕМИ ПСИХОФІЗІОЛОГІЧНОГО ДОСЛІДЖЕННЯ ІЗ ЗАСТОСУВАННЯМ ІНТЕГРАЛЬНИХ СИСТЕМ ДЕТЕКЦІЇ БРЕХНІ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Сьогодні інформаційні загрози є одними з найнебезпечніших загроз національній безпеці за своїми руйнівними наслідками. В сучасних умовах цифрової трансформації, розбудови інформаційного суспільства проблема застосування інтегральних систем детекції брехні на основі штучного інтелекту ШІ (artificial intelligence AI) та кіберзахищеного програмного забезпечення є надзвичайно актуальною для підвищення ефективності проведення психофізіологічного дослідження виявлення прихованої і недостовірної інформації.

У національних стратегіях розвитку штучного інтелекту (далі ШІ) розглядається широкий спектр питань, пов'язаних із розробкою та розвитком технологій, а також широким використанням різних систем з урахуванням існуючих соціальних, економічних, політичних, технологічних та правових проблем.

Слід звернути увагу, що створення алгоритмів майже усіх сучасних систем ШІ, які демонструють високу ефективність моделювання когнітивних функцій людини, базується на використанні різних методів (machine learning) машинного навчання (штучні нейронні мережі, глибинне навчання, індуктивне логічне програмування, баєсові мережі, навчання з підкріпленням тощо) [1].

Використання таких систем має поєднуватися з довірою держави і суспільства.

У рамках європейської і євроатлантичної інтеграції України довіра до державних інститутів є одним із ключових аспектів забезпечення національної безпеки держави

Для досягнення такої довіри особливої уваги потребує проблематика впровадження ШІ при проведенні психофізіологічного дослідження із застосуванням інтегральних систем виявлення прихованої та недостовірної інформації та поліграфа із кіберзахищеним програмним забезпеченням (cyber security of polygraph software).

Не менш важливим є застосування систем детекції брехні та поліграфа, спеціальних методик (computerized polygraph system), спеціалізованого програмного забезпечення (polygraph software) на основі ШІ, які відповідають вимогам кібербезпеки.

Останні відкриття та аналіз наукових основ психофізіологічного дослідження із застосуванням поліграфа свідчать, що сьогодні технологія ШІ широко використовується в науково-аналітичних дослідженнях, промисловості, фінансовій сфері, освіті, медицині тощо. Наприклад, вебпошукова система – Google Search, відеохостинг – YouTube, платформа електронної комерції – Amazon, стримінгові сервіси – Netflix, спілкування – Google Assistant, Siri та Alexa, керування автомобілем – Waymo, генератори ідей та творчі інструменти – ChatGPT та AI art.

Актуальними є науково-практичні дослідження з практичного запровадження інтелектуальних систем детекції брехні, які поєднують швидкість і потужність апаратного забезпечення з найсучаснішим кіберзахищеним програмним забезпеченням з інноваційними й досконалими функціями. Ці функції зумовлюють нові можливості, які необхідні для якісного проведення психофізіологічного дослідження із застосуванням інтегральних систем детекції брехні.

Акцентуємо увагу, що для підвищення ефективності проведення психофізіологічного дослідження із застосуванням систем виявлення прихованої та недостовірної інформації та поліграфа доцільно зосередитися на розробці інтелектуальних систем ШІ, здатних виконувати з урахуванням належного рівня кібербезпеки завдання, які зазвичай потребують людського розуму.

Необхідно зазначити, що кожна галузь працює над інтеграцією ШІ у свою діяльність. Напрям виявлення прихованої та недостовірної інформації із застосуванням систем детекції брехні не є винятком.

Алгоритми ШІ системно вдосконалюються та оптимізуються, поглинаючи значні обсяги інформації, отримуючи конкретні результати на основі аналізу даних. ШІ еволюціонує у сфері виявлення недостовірної та прихованої інформації, надаючи більш точні, своєчасні та достовірні результати.

Зауважимо, що технології ШІ бурхливо розвиваються і з часом стануть доступними для широких верст суспільства, що, з одного боку, зумовлює появу нових ризиків та загроз в інформаційній сфері. З іншого боку, технології ШІ автоматизують трудомісткий процес перевірки інформації, мінімізації ризику людського фактору.

Отже, справжньою інновацією може стати інтегральна кіберзахищена система детекції брехні на основі ШІ. Дослідження авторами інформаційних систем моніторингу та аналізу потоків інформації в реальному часі підкреслює необхідність професійного застосування алгоритмів ШІ для детекції брехні. Зокрема, розробка стратегії дій, має бути формуватися з урахуванням сильних і слабких сторін інтегральної системи детекції брехні, мінімізуючи існуючі загрози. По суті, це аналіз обмежень, переваг та ризиків, який передує запровадженню інтегральних систем для широкого практичного застосування.

Результати наукового дослідження авторів свідчать, що ШІ може відігравати ключову роль у кожному з трьох основних інтегральних методів детекції брехні із застосуванням поліграфа:

1. Generative AI and Physiological Lie Detection (GenAI-Physio LD). Поліграф може мати вбудований генеративний штучний інтелект або може застосовуватися через інтерфейс з генеративним додатком ШІ, зовнішній інтегральний чіп (integrated circuit).

2. Generative AI and Observational Lie Detection (GenAI-Observ LD). Підвищити ефективність детекції брехні можливо за допомогою генеративної програми ШІ, яка взаємодіє із системами реєстрації (acquisition system), камерою та мікрофоном.

3. Generative AI and Cognitive Lie Detection (GenAI-Cogno LD). Підвищення ефективності детекції брехні шляхом застосування генеративного ШІ для аналізу і моделювання когнітивних аспектів [2, 3].

З огляду на наведене, можна стверджувати, що розробка й запровадження інтелектуальних систем детекції брехні та кіберзахищеного програмного забезпечення поліграфа (polygraph software) на основі ШІ за сумісними міжнародними стандартами ASTM International та ресурсами рекомендованими American Polygraph Association забезпечить підвищення ефективності застосування систем психофізіологічного виявлення прихованої і недостовірної інформації (Research in Psychophysiological Detection of Deception (Polygraph) і сприятиме системному розвитку у сфері інформаційної безпеки в контексті Європейської та Євроатлантичної інтеграції України [4, 5].

Реалізація таких систем дозволить підвищити ефективність: 1) розслідування адміністративних та кримінальних правопорушень; 2) протидії корупції шляхом реалізації програм антикорупційного спрямування, зокрема, антикорупційної перевірки осіб які мають активи, що не підтверджені законними доходами, подали недостовірні документи для призначення на посаду тощо; 3) забезпечення кібернетичного захисту програмного забезпечення систем детекції брехні; 4) військово-технічного співробітництва з міжнародними партнерами для залучення сучасних технологій в оборонну галузь та економіку держави.

В даному контексті важливо розробити єдині стандарти та методики для застосування інтегральних систем детекції брехні з урахуванням позитивного міжнародного досвіду та кращих світових практик у сфері національної безпеки держави. Це сприятиме активізації та переведення у практичну площину процесів європейської і євроатлантичної інтеграції України, а також відновленню довіри до державних інститутів.

На наше переконання, ШІ та кібербезпека систем детекції брехні – це перспективний інноваційний напрям у сфері інформаційної безпеки, що зумовлює застосування інформаційно-аналітичних систем виявлення прихованої і недостовірної інформації на основі ШІ та кіберзахисту програмного забезпечення інтегральних систем детекції брехні.

Дане дослідження, з точки зору підвищення повноти та об`єктивності інформаційної основи, може бути корисним в процесах підготовки та проведенні парламентських слухань.

Список використаних джерел

1. Пилипчук В. Г., Андрійович Б. О., Гиляка О. С. Проблема правового регулювання у сфері штучного інтелекту в контексті розви-

тку законодавства Європейського союзу. URL: http://visnyk.kh.ua/uk/article/problema-pravovogo-regulyuvannya-u-sferi-shtuchnogo-intelektu-v-konteksti-rozvitku-zakonodavstva-yevropeyskogo-soyuzu

2. Forbes. Lance Eliot Contributor. Dr. Lance B. Eliot is a world-renowned expert on Artificial Intelligence (AI) and Machine Learning On Using Generative AI As A Lie Detector Including Trying To Bust The Infamous Two Truths And A Lie Gambit Via ChatGPT. URL: https://www.forbes.com/sites/lanceeliot/2024/01/21/on-using-generative-ai-as-a-lie-detector-including-trying-to-bust-the-infamous-two-truths-and-a-lie-gambit-via-chatgpt/?sh=52ac89a25a2c

3. Raymond Nelson. Scientific Basis for Polygraph Testing. URL: https://polygraph.org/docs/nelson_2015_scientific_basis_for_polygraph.pdf

4. ASTM International. URL: https://www.astm.org/

5. American Polygraph Association. URL: https://www.polygraph.org/

Варинський В. О.
кандидат політичних наук,
доцент, доцент кафедри філософії
Національного університету «Одеська
морська академія»,
Савінова Н. А.
доктор юридичних наук, старший
науковий співробітник, директор
навчально-наукового інституту
морського права та менеджменту
Національного університету «Одеська
морська академія»

ЕФЕКТИВНІСТЬ УДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА ТА ШТУЧНИЙ ІНТЕЛЕКТ

Стан сучасного законодавства України, яке приймалося протягом років незалежності України здебільшого ситуативно, сьогодні гостро потребує на правовий аудит, а підходи до його подальшого розвитку очікує суттєва деконструкція.

Першим кроком на шляху модернізації законодавчого забезпечення в Україні має стати загальнодержавна програма Моніторингу ефективності застосування законодавства, що здатна проаналізувати вади ефективності його застосування та випрацювати напрями правової політики,