УДК 655.1
DOI https://doi.org/10.32782/2663-5941/2024.4/18

Кримська А.О.
Чернівецький торговельно-економічний інститут
Державного торговельно-економічного університету

КЛЮЧОВА РОЛЬ ПОЛІГРАФОЛОГІЧНИХ ДОСЛІДЖЕНЬ У СТРАТЕГІЯХ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В ЕКОНОМІЧНИХ ГАЛУЗЯХ

Стаття присвячена ролі поліграфів у забезпеченні додаткового рівня безпеки та контролю доступу до конфіденційної інформації в різних галузях економіки. Це зумовлено необхідністю зменшення ризику витоку даних через недбалість або злочинну діяльність, що може серйозно зашкодити фінансовій стабільності та репутації підприємств. З'ясовано, що поліграфічні дослідження дозволяють перевірити автентичність і надійність персоналу, що має доступ до важливої інформації. Це допомагає зменшити ризик витоку даних та виявити потенційні загрози зсередини. У статті розкрито, що використання поліграфа дозволяє оцінити ступінь благонадійності співробітників та їхню готовність дотримуватися внутрішніх політик інформаційної безпеки. Виявлено, що поліграфічні перевірки дозволяють ідентифікувати потенційні загрози зсередини організації. Це включає виявлення несанкціонованого доступу до конфіденційної інформації та правопорушень, що можуть виникнути в економічних секторах, де інформаційна безпека є критичною для фінансової стабільності та репутації підприємств. У статті розкрито, що поліграфія стає інструментом попередження внутрішніх конфліктів та кіберзагроз. В умовах зростання кіберзагроз та внутрішніх конфліктів, поліграфічні перевірки стають важливою частиною управління ризиками та внутрішньої безпеки. Це допомагає підвищити рівень внутрішньої дисципліни та зменшити внутрішні загрози, які можуть походити від неправомірних дій співробітників. Розкрито, що інтеграція поліграфічних досліджень у стратегію інформаційної безпеки дозволяє підприємствам ефективно захищати свою інформацію та ресурси від внутрішніх загроз. Виявлено, що поліграфічні перевірки повинні проводитися з дотриманням етичних норм і прав працівників, щоб не порушувати їхні права та свободи. Це включає обов'язкову інформованість працівників про процедуру перевірки, отримання їхньої згоди на проведення поліграфічних досліджень та дотримання конфіденційності отриманих даних. Зазначено, що поліграфія стає потужним інструментом у загальному комплексі заходів щодо забезпечення інформаційної безпеки підприємств. Вона сприяє збереженню фінансової стабільності підприємств та зміцненню їхньої репутації.

Ключові слова: *інформаційна безпека, управлінські стратегії, економічна безпека, поліграфологія, кіберзагрози.*

Постановка проблеми. Становлення інформаційного суспільства характеризує суспільний розвиток. Створення єдиного світового інформаційного ринку є одним із напрямків, в якому бере участь Україна. Інформаційний фактор може бути використаний для захисту державних інтересів. Широкий і оперативний доступ для підвищення інформаційної ефективності є частиною процесів установ. Інформатизація сучасного суспільства включає впровадження новітніх систем обробки інформації та телекомунікацій. Для забезпечення інформаційної безпеки використовуються поліграфічні дослідження. Отримати об'єктивні дані щодо достовірності та правдивості інформації, яку надають співробітники та партнери підприємства, можна за допомогою поліграфа чи детектора брехні. За допомогою поліграфа можна визначити загрози з часом.

Вивчення проблем інформаційної безпеки є тим, що веде до розвитку інформаційних технологій. Існують заходи безпеки, які використовуються. Є перешкоди, які потрібно подолати. Існують дослідження, за допомогою яких можна знайти вразливі місця. Ви можете отримати цінну інформацію, провівши ці дослідження. Інформаційна безпека – це набір засобів, методів і процесів, які забезпечують захист інформаційних активів і гарантують збереження ефективності та практичної придатності як технічної інфраструктури інформаційних систем, так і інформації, що зберігається та обробляється при такій оцінці та аналізі. Використання поліграфа допомагає захистити територіальну цілісність і суверенітет України, що є частиною концептуальних засад суспільства.

Аналіз останніх досліджень і публікацій. Вміщено праці як вітчизняних, так і зарубіжних учених. А. Баранова, О. В. Глазова, Т. Г. Каткова та ін. Враховуючи думки авторів, необхідно приділити більшу увагу дослідженню проблем поліграфології в інформаційній безпеці, яка є пріоритетною складовою національної безпеки України. Перевірка на поліграфі використовується в системі захисту інформації.

Отримати об'єктивні дані щодо достовірності та правдивості інформації, що надається співробітниками та партнерами підприємства, можливо за допомогою поліграфа. Це може бути особливо корисним під час найму нових співробітників, проведення внутрішніх розслідувань і виявлення загроз зсередини організації. Актуальність дослідження проблем інформаційної безпеки залежить від активного розвитку інформаційних технологій. Для захисту інформаційних ресурсів використовуються різні засоби та заходи захисту.

Перешкоди для проникнення Є уразливості в системі захисту інформації. Перевірка на поліграфі допомагає виявити вразливі місця в системі захисту інформації, а також оцінити потенційні загрози, що дозволяє своєчасно розробити ефективні заходи щодо їх запобігання. Він забезпечує надійний захист інформаційних активів і підвищує загальний рівень інформаційної безпеки підприємства.

Загалом під інформаційною безпекою слід розуміти сукупність засобів, методів і процесів, які забезпечують захист інформаційних активів і, як наслідок, гарантують збереження ефективності та практичної корисності як технічної інфраструктури інформаційних систем, так і інформації зберігаються і переробляються в таких.

Постановка завдання. Мета статті полягає в дослідженні та аналізі ключової ролі поліграфологічних досліджень у стратегіях управління інформаційною безпекою в економічних галузях. У сучасних умовах глобалізації та зростання кіберзагроз, забезпечення надійного захисту конфіденційної інформації стає критично важливим завданням для підприємств різних секторів економіки. Поліграфічні перевірки надають можливість оцінити надійність та благонадійність персоналу, що має доступ до важливої інформації, з метою зменшення ризику витоку даних та виявлення потенційних загроз зсередини.

У контексті зовнішніх і внутрішніх загроз, а також його взаємозв'язку з перевірками на поліграфі постає завдання обґрунтувати використання новітніх технологій в інформаційній безпеці держави. Кількість кіберзагроз зростає. Штучний інтелект можна використовувати для аналізу великих обсягів даних і пошуку незвичайних шаблонів, які вказують на можливі атаки або витік інформації. Ви можете використовувати штучний інтелект для автоматизації процесів моніторингу та реагування на кіберінциденти. Тести на поліграфі можна використовувати з технологіями, які зосереджені на внутрішніх загрозах. Аналіз реакції людини на подразники – це те, на чому вони базуються. Інтеграція вигаданого розуму з поліграфом ускладнює можливості атак і дає комплексний підхід до захисту інформаційних ресурсів держави.

Виклад основного матеріалу дослідження. Здатність держави долати кризові явища в разі зовнішньої агресії є одним із найважливіших факторів забезпечення реалізації національних інтересів. Своєчасні та ефективні заходи щодо інфобезпеки з боку держави здатні подолати загрози соціально-економічному та політичному життю країни. Індустрія номер один у світі – це оборона та безпека, і вона зазнає серйозних змін через впровадження технологій штучного інтелекту. [2, с. 16].

У майбутньому дані технології можуть бути використані для зміни поведінки людей, соціальних стосунків і впливу на особистість людини.

Штучний інтелект в інформаційній безпеці дозволяє автоматизувати виявлення та аналіз потенційних кіберзагроз, що допомагає швидко реагувати на них і скорочувати час реакції. Системи машинного та глибокого навчання можуть аналізувати великі обсяги даних, щоб знаходити аномалії, які можуть вказувати на загрози інформаційній безпеці. перевірки на поліграфі можуть бути застосовані до внутрішньої безпеки, де аналіз відповідей може виявити загрози з боку співробітників або інших внутрішніх джерел. Інтеграція двох підходів дозволяє створити систему захисту, яка враховує як технічні, так і поведінкові аспекти. Програмне забезпечення безпеки, яке добре працювало в минулому, було обійдено кіберзлочинцями.

2 грудня 2020 року в Україні Розпорядженням Кабінету Міністрів України №1556-р було схвалено Концепцію розвитку вигаданого розуму в Україні [3], яка передбачає визначення основних напрямів та пріоритетних завдань розвитку технологій з метою забезпечення конкурентоспроможності національної економіки (рис. 1).

Рис. 1. Основні напрями забезпечення інформаційної безпеки

Джерело: [3]

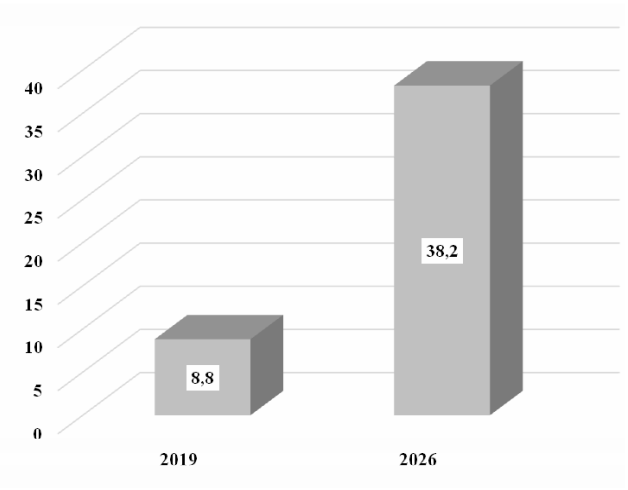

Рис. 2. Прогноз об'єму світового ринку штучного розуму в інформаційній безпеці на 2019–2026 рр., млрд дол. США

Джерело: [8]

Штучний інтелект здається дорогим і неперевіреним рішенням, на яке йдуть лише інноваційні компанії з великим бюджетом. Усі компанії потребують його використання в управлінні інформаційною безпекою, незалежно від їх розміру. Ландшафт загроз змінюється блискавично зі збільшенням кількості атак. Продукти Kaspersky запобігають понад 700 мільйонів онлайн-атак на квартал, тоді як Cisco блокує 20 мільярдів мережевих атак на день. Зловмисники використовують ці технології для їх удосконалення та трансформації, а також для обходу відомих засобів захисту з великою злочинною діяльністю. Група, що стоїть за створенням Emotet, може легко використовувати штучний інтелект для посилення атаки, оскільки основним каналом його поширення є спам-фішинг.

Більш ефективний вибір пароля є одним із способів використання в зловмисних цілях. Технології були використані для створення бота, який зміг обійти перевірку CAPTCHA. Використовуючи велику кількість різноманітних джерел даних у темній мережі з метою формування бази знань неприродних даних, де зловмисники можуть створювати атаки, тому виробники систем захисту починають активно впроваджувати технології машинного навчання [5]. Світовий ринок технологій в інформаційній безпеці оцінювався експертами в 8,8 млрд доларів США в 2019 році, і очікується, що він досягне 38,2 млрд доларів США в 2026 році (рис. 1) [7]. Основні фактори росту:

1) Зростає кількість підключених пристроїв
2) Зростає кількість користувачів Інтернету
3) Зросла кількість випадків кіберзагроз
4) Зростає вразливість мережі до загроз безпеки.

Висновки. Технологічна майстерність і прогрес останнього десятиліття привернули увагу багатьох державних адміністрацій. Перетворення технологічних можливостей у конкретну бізнес-цінність для компаній і суспільну цінність від органів державної влади, які використовують технології, було обмеженим. Відсутність можливостей в організації є однією з причин повільного прогресу у впровадженні в державне правління. Його часто розглядають як технічну експертизу в надуманому розумовому середовищі, але можливості технології розуміються ширше.

Для того, щоб державні адміністрації могли ефективно розвивати та використовувати штучний інтелект, існують різні технічні та нетехнічні компоненти. Сфери державного ладу, які є відносно зрілими з точки зору несправжнього глузду в своїх країнах, знаходяться в центрі уваги цього дослідження. У дослідженні використано декілька прикладів. Набуття можливостей, де взаємодоповнення та взаємодія між різними компонентами державних адміністрацій, які ще не використовують технології штучного інтелекту, можуть дати різні результати. Технології використовуються в державному управлінні.

З розвитком галузі деякі проблеми, можливо, уже вирішено. Якісний характер дослідження підтримує кількісні дослідження. Внесок у продуктивність організації є одним із критеріїв аналізу. Під час більш детального розгляду концепцій і компонентів було виявлено кілька питань, які не можна було вивчити так глибоко, як хотілося. Майбутні дослідження можуть досліджувати проблеми отримання такого ума різними способами.

Існує низка різних технологій, які досліджують штучний інтелект, і сектори державних послуг, які їх використовують. Країни зі складними відносинами з сусідами – Індія, Нідерланди, Пакистан, Тайвань, Україна, Велика Британія.

Розташування доменів і мережеві шляхи, через які до них йде трафік громадян, визначаємо нами. У шести країнах були різні стратегії. Деякі уряди зберігають більший суверенітет, ніж інші, але вони не можуть претендувати на незалежність, оскільки залежать від Інтернету. Територіальність не варто порівнювати з іншими речами. Існують компроміси між ризиками та залежністю. На дружніх і потужних іноземних провайдерів можна покластися, якщо існує загроза вторгнення або брак національних можливостей для захисту цифрової інфраструктури.

Досі тривають дебати щодо пошуку цифрового суверенітету. Держави мають вирішити, як вони хочуть управляти цими ризиками проти переваг, які надають цифрові технології для сприяння належному врядуванню, ефективного високотехнологічного потенціалу ефективних у часі послуг, коли вони стануть доступними для широкомасштабного розгортання. Таке рішення має право приймати державний орган. Завдяки використанню більш сучасного обладнання та програмного забезпечення, конструкції в усьому світі переживають поворотний момент.

У разі стрімкого розвитку технологій потенціал інформаційно-технічного та інформаційно-психологічного впливу буде значним. Штучний інтелект – це програмне забезпечення, яке здатне інтерпретувати стан навколишнього середовища, розпізнавати певні події та виконувати необхідні дії. Технології можна використовувати для моніторингу загроз.

Дослідження інтеграції штучного інтелекту в державному управлінні, а саме вивчення методів ефективного впровадження технологій штучного інтелекту в різних сферах державного управління включає розробку конкретних планів дій, рекомендацій щодо адаптації існуючих процесів та оцінку можливих перешкод і бар'єрів. Аналіз впливу штучного інтелекту на підвищення ефективності та продуктивності державних адміністрацій. Це може включати порівняння показників ефективності до і після впровадження технологій, а також оцінку економічного ефекту.

Технологічні та нетехнологічні компоненти дослідження взаємодії між технічними та нетехнічними компонентами в державних адміністраціях – це запорука аналізу взаємозв'язку між людськими ресурсами, організаційною культурою та процесами управління. Аналіз можливостей для підвищення ефективності за допомогою технологічних інновацій. Також включає вивчення потенціалу різних інноваційних технологій для оптимізації адміністративних процесів, зниження витрат та покращення якості послуг.

Країни з різними стратегіями розвитку технологій, де порівняльний аналіз стратегій розвитку технологій у державних адміністраціях різних країн. Такий спосіб дозволить визначити найкращі практики, а також виявити слабкі місця в підходах різних держав. Дослідження впливу геополітичних факторів на впровадження технологій штучного інтелекту в державне управління. Це включає вивчення, як міжнародні відносини, економічні санкції та інші зовнішні фактори впливають на можливості впровадження технологій.

Цифровий суверенітет та управління ризиками: дослідження підходів до досягнення цифрового суверенітету у різних країнах. Це передбачає аналіз політик і стратегій, спрямованих на забезпечення контролю над національними цифровими ресурсами та інфраструктурою. Аналіз компромісів між ризиками та перевагами використання цифрових технологій у державному управлінні. Це включає вивчення потенційних загроз кібербезпеки та розробку стратегій для мінімізації ризиків.

Інформаційно-технічний та інформаційно-психологічний вплив: дослідження потенціалу інформаційно-технічного та інформаційно-психологічного впливу сучасних технологій. Це включає аналіз можливостей для використання технологій у моніторингу суспільних настроїв, боротьбі з дезінформацією та підтримці громадського порядку. Аналіз використання технологій для моніторингу та реагування на загрози. Це передбачає вивчення способів використання штучного інтелекту та інших технологій для виявлення та попередження потенційних загроз, таких як кіберзлочинність, тероризм та інші небезпеки.

Подальші дослідження в цих напрямках допоможуть краще зрозуміти потенціал і виклики використання технологій у державному управлінні, а також сприятимуть розробці ефективних стратегій їх впровадження.

Список літератури:

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

2. Концепція розвитку штучного інтелекту в Україні [Електронний ресурс]: Розпорядження Кабінету міністрів України № 1556-р від 02.12.2020. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення: 07.12.2021).

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

4. Укроборонпром хоче використовувати штучний інтелект в «оборонці». URL: https://www.epravda.com.ua/news/2021/08/26/677230 (дата звернення: 07.12.2021).

5. Artificial Intelligence (AI) In Cyber Security Market Will Reach to USD 30.9 Billion By 2025: Zion Market Research. URL: https://www.globenewswire.com/news-release/2019/08/28/1907655/0/en/Artificial-Intelligence-AI-In-Cyber-Security-Market-Will-Reach-to-USD-30-9-Billion-By-2025-Zion-Market-Research.html (accessed 22 January 2024).

6. Artificial Intelligence in Cybersecurity Market by Offering. URL: https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-ai-cyber-security-market-220634996.html (accessed 22 January 2024).

7. Jeschke S., Brecher C., Song H., Rawat D.B. *Industrial Internet of things and cyber manufacturing systems*. Cham: Springer International Publishing Switzerland. 2017. Vol. 3, pp. 3–19.

8. Leveraging artificial intelligence to maximize critical infrastructure cybersecurity. URL: https://www.thalesgroup.com/en/worldwide/security/magazine/leveraging-artificial-intelligence-maximize-critical-infrastructure (accessed 22 January 2024).

9. Pretorius B., van Niekerk B. Cyber-security for ICS/SCADA. *International Journal of Cyber Warfare and Terrorism*. 2016. Vol. 6. P. 1–16.

10. Nesterov V. Integration of artificial intelligence technologies in data engineering: Challenges and prospects in the modern information environment. *Bulletin of Cherkasy State Technological University*. 2023. Vol. 28, No. 4. P. 82–92. URL: https://doi.org/10.62660/2306-4412.4.2023.82-90

11. Ahn M. J., Chen Y.-C. (2022). Digital transformation toward AI- augmented public administration: The perception of government employees and the willingness to use AI in government. *Government Information Quarterly*. 2022. Vol. 39. No. 2. Article 101664. URL: https://doi.org/10.1016/j.giq.2021.101664 (accessed 22 January 2024).

12. Sanina A., Balashov A., Rubtcova M. The socio-economic efficiency of digital government transformation. *International Journal of Public Administration*. 2021. Vol. 46. No. 1. P. 85–96. URL: https://doi.org/10.1080/01900692.2021.1988637 (accessed 22 January 2024).

13. Mergel I., Dickinson H., Stenvall J., Gasco M. Implementing AI in the public sector. *Public Management Review*. 2023. P. 1–14. URL: https://doi.org/10.1080/14719037.2023.2231950 (accessed 22 January 2024).

14. Medaglia R., Tangi L. The adoption of artificial intelligence in the public sector in Europe: Drivers, features, and impacts. *ICEGOV '22: Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance*. New York: Association for Computing Machinery, 2022. https://doi.org/10.1145/3560107.3560110 (accessed 22 January 2024).

Krymska A.O. THE KEY ROLE OF POLYGRAPH EXAMINATIONS IN INFORMATION SECURITY MANAGEMENT STRATEGIES IN ECONOMIC SECTORS

Polygraphs play an important role in providing an additional level of security and control of access to confidential information in various sectors of the economy. This is due to the need to reduce the risk of data leakage due to negligence or criminal activity, which can seriously damage the financial stability and reputation of enterprises. Polygraphic tests allow you to check the authenticity and reliability of personnel who have access to important information. This helps reduce the risk of data leakage and identify potential insider threats. The use of a polygraph allows you to assess the degree of trustworthiness of employees and their willingness to comply with internal information security policies. Polygraphic checks allow you to identify potential threats from within the organization. This includes detecting unauthorized access to confidential information and offenses that may occur in economic sectors where information security is critical to the financial stability and reputation of businesses. Polygraphy becomes a tool for preventing internal conflicts and cyber threats. In the face of growing cyber threats and domestic conflicts, polygraph checks are becoming an important part of risk management and homeland security. This helps to increase the level of internal discipline and reduce internal threats that may come from employee misconduct. The integration of polygraphic studies into the information security strategy allows enterprises to effectively protect their information and resources from internal threats. Polygraphic checks must be carried out in compliance with ethical standards and the rights of employees, so as not to violate their rights and freedoms. This includes the mandatory informing of employees about the verification procedure, obtaining their consent to conducting polygraphic examinations and maintaining the confidentiality of the data obtained. Polygraphy becomes a powerful tool in the general complex of measures to ensure information security of enterprises. It contributes to maintaining the financial stability of enterprises and strengthening their reputation.

Key words: *information security, management strategies, economic security, polygraphology, cyber threats.*