adhere to the requirement of stability in its interpretation, which is set out in the Tax Code of Ukraine.

To bring the Regulation on the Ministry of Finance of Ukraine in terms of tax powers in accordance with the Tax Code of Ukraine, it is necessary to set out subparagraph 39 of paragraph 4 of the Regulation as follows: The Ministry of Finance of Ukraine fees for a period exceeding one budget year, if the amount declared for installment or deferral or the amount of deferred or deferred monetary obligations or tax debt in respect of which payment is deferred is 1 million hryvnias or more; makes a reasoned decision to grant installments or deferrals of monetary obligations or tax debt in respect of national and local taxes and fees, as well as to postpone the payment of deferred or deferred amounts, if the amount of previously granted installments or deferrals of monetary obligations or tax debt was not repaid».

Keywords: *tax sovereignty, tax legal relations, tax powers, tax competence, public authorities.*

УДК 338.1
DOI 10.31733/2078-3566-2021-1-337-342

Ольга СТАНІНА©
кандидат технічних наук
(Дніпропетровський державний університет внутрішніх справ)

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В ЗАБЕЗПЕЧЕННІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

Доведено необхідність вивчення впливу штучного інтелекту на економічну безпеку кожного окремого підприємства та країни загалом. Визначено основні причина та переваги впровадження систем штучного інтелекту в різноманітні сфери діяльності людини. Сформульовано низку загроз, що пов'язані з впровадженням штучного інтелекту, а саме: низький рівень захисту даних; особливості технології роботи системи; збільшення кількості даних, які обробляються, сортуються та зберігаються; упереджене судження штучного інтелекту через неякісне навчання; низький рівень комунікації між людиною та системою тощо. Запропоновано можливі заходи щодо протидії негативному впливу штучного інтелекту на економічну безпеку України.

Ключові слова: *безпека, економічна безпека, штучний інтелект, перспективи, ризики.*

Постановка проблеми. У сучасному світі одним з ключових критеріїв успішного розвитку держави є рівень її економіки. Економіка України пройшла довгий та тернистий шлях для досягнення стабільності та рівноваги. Але останні події у світі та країні створюють нові негативні чинники, які спричиняють загрозу не тільки економічній, але й національній безпеці держави.

Сучасний світ характеризується високим ступенем мінливості та хиткістю будь-якого фундаменту. А отже, діяльність сучасних підприємств стикається з необхідністю бути відповідними постійним змінам та різноманітним (часто неочікуваним) впливам зовнішнього середовища. Такі впливи та чинники, що їх спричиняють, не завжди є сприятливими для діяльності підприємства, а це означає, що компаніям необхідно бути весь час готовими до всіляких загроз та небезпек. У таких умовах все гостріше постає питання економічної безпеки підприємства та тих рішень, що з нею пов'язані.

Аналіз публікацій, в яких започатковано вирішення цієї проблеми. Станом на сьогодні, все більше вчених приділяють увагу дослідженню питань протидії економічним загрозам, зокрема: О. Барановський, І. Бінько, Т. Васильців, В. Геєць, М. Єрмошенко, Я. Жаліло, Ю. Лисенко, Т. Момот, В. Мунтіян, В. Предборський, Т. Пастернак–Таранушенко, А. Штангрет та багато інших. І наявність такої великої кількості науковців, що зайнята вивченням економічної безпеки, тільки підсилює важливість дослідження цієї проблеми.

З розвитком інформаційних технологій та створенням штучного інтелекту (ШІ) все більша кількість сфер впроваджує їх у свою діяльність. І сьогодні вже неможливо уявити

ORCID iD: https://orcid.org/0000-0001-6754-0317
st.olga.d@gmail.com

роботу сучасного підприємства без використання інформаційних технологій та ШІ.

Серед вчених, що займалися розробкою ШІ та дослідженням його впливу на життя людини, можна відзначити С. Хокінга, Н. Вінера, А. Тьюрінга, Ч. Беббіджа, П. Вінсона, В. Глушкова, Д. Попова, О. Швиркова та багатьох інших. Проблеми саме впровадження ШІ в життя людей досліджували такі вчені, як Є. Бабич, М. Шишкіна, В. Білик, О. Баранов та ін.

Метою статті є аналіз перспектив та ризиків використання штучного інтелекту та його роль у забезпечені економічної безпеки держави.

Виклад основного матеріалу. На сьогодні серед важливих та перспективних напрямів застосування ШІ можна виділити такі:

– машинне навчання, яке вже спроможне працювати без людини та будувати прогнози у сферах економіки, медицини, транспорту тощо;

– ШІ, пов'язаний з опрацюванням та аналізом природної мови, розшифровуванням промов, написів, створюванням нескладних нотаток тощо;

– віртуальні помічники, які допомагають створювати особистий розклад, планувати зустрічі, будувати маршрути, надавати рекомендації, допомагати під час прийняття рішень тощо;

– експертні системи в найрізноманітніших галузях економіки;

– машинний зір, який покликаний розпізнавати навколишнє середовище, малюнки, почерк, реконструювати історичних осіб та будівлі і, навіть, забезпечувати безпеку керування автомобілем.

Сучасні підприємства, які мають змогу використовувати ШІ у своїй діяльності, отримують чимало переваг:

– зниження операційних витрат за рахунок оптимізації процесів та мінімізації витрат підприємства;

– прийняття більш зважених управлінських рішень за рахунок аналізу більшого обсягу даних та прогнозування майбутнього розвитку підприємства;

– своєчасність за рахунок можливості швидкого опрацювання великих обсягів інформації;

– зниження відсотка людських та операційних помилок за рахунок автоматизації виробництва;

– захист від шахрайства.

Якщо розглядати сферу застосування ШІ у різноманітних секторах економіки, треба зазначити, що:

– в секторі маркетингу ШІ активно використовується насамперед для ефективного таргетингу (тобто реклами), аналізу, отримання якісних даних стосовно цільової аудиторії (ЦА) та як інструмент для прогнозування щодо майбутніх уподобань ЦА відповідного сегмента ринку;

– сектор торгівлі використовує ШІ для оптимізації складських запасів, ціноутворення, як інструмент для прийняття рішень щодо акцій та розпродажу, аналізу купівельної корзини;

– у банківському секторі ШІ найперше використовується для аналізу, прогнозування, прийняття управлінських рішень, організації клієнтського сервісу, безпеки (наприклад, розпізнавання обличчя) тощо;

– в телекомунікаційному секторі, як і в банківському, ШІ насамперед використовується для аналізу бази своїх клієнтів. Але він також може застосовуватися для роботи з клієнтами (наприклад, за допомогою чат–ботів), формування тарифів, безпеки (наприклад, виявлення неправомірних чи спам–дзвінків);

– сектор промисловості є чи не найбільш продуктивним для використання ШІ, адже саме в ньому застосування сучасних інформаційних технологій дозволяє не тільки утворити певний економічний ефект, але і напряму пов'язано із запобіганням помилок, що виникають через наявність людського чинника, та безпекою праці. Тому можна казати, що насамперед в цьому секторі ШІ використовується як певні автоматизовані інструменти та когнітивні помічники. Але також повсюдно зустрічається його застосування для прогнозування, прийняття управлінських рішень, оптимізації витрат;

– транспортний сектор використовує ШІ для оптимізації (наприклад, побудови найкоротшого шляху доставки сировини чи матеріалів), автоматизації (наприклад, системи автоматичного керування чи автопілот) тощо.

Сучасний ШІ завдяки самонавчанню вже не потребує такої великої частки втручання людини, яку раніше вимагали автоматизовані системи. І це призводить до того, що досить велику кількість роботи ШІ вже може виконувати самостійно (наприклад, робити певні прогнози, керувати автомобілем, писати нескладні тексти тощо). Потенціал систем штучного

інтелекту (СШІ) дуже високий, тому можна зробити припущення, що їх поширення надалі буде лише збільшуватися.

Як зазначають деякі науковці у своїх прогнозах [1], у майбутньому повсюдне використання ШІ у сфері економіки призведе до суттєвого зниження економічних ризиків та небезпек. Впровадження інформаційних технологій спричинить підвищення стабільності та стійкості фінансової системи. За деякими оцінками [2], використання ШІ може призвести до збільшення продуктивності праці на 37 % в 2035 році в розвинених країнах світу. Ще одним показником, який свідчить про зростання ролі ШІ у світі, можна вважати збільшення кількості венчурного капіталу, який припадає на частку СШІ, та збільшення економічного ефекту від ШІ [3].

Наведені наукові дослідження лише підкреслюють той факт, що у майбутньому технологічні зміни є неминучими. При цьому виникає важливе питання щодо готовності світової та національної економіки до швидких змін, адже світова глобалізація лише прискорює цей процес.

І тут треба зазначити, що, незважаючи на велику кількість переваг використання ШІ, його впровадження супроводжується також низкою труднощів і навіть небезпек. Серед наявних на цей час складнощів найперше треба виділити такі:

– нестача кваліфікованого трудового персоналу;

– занадто висока вартість введення в експлуатацію, обслуговування та модернізації індивідуального застосування ШІ;

– складнощі, пов'язані з високими вимогами щодо управління та збереження даних та інформації.

Але впровадження ШІ спричиняє не тільки труднощі, пов'язані з безпосередньою організацією процесу, але і небезпеки, які належать до питань роботи самих СШІ. Сучасні кіберзлочинці активно використовують ШІ для розробки більш ефективних методів зламування інформаційних систем підприємств чи приватних користувачів. Як показують дослідження [4], більшість сучасних комп'ютерних систем, що використовують ШІ, мають вразливість, яка виникає внаслідок обмеженості вхідних даних. Відомо, що системи ШІ, засновані на нейронних мережах (НМ) (а це велика кількість сучасних СШІ), працюють настільки добре, наскільки якісними є ті дані, на яких вони навчаються. І саме в цьому факті міститься найбільша вразливість СШІ, адже наявність навіть невеликої кількості хибних даних у навчальній виборці може призвести до суттєвих змін в отриманих результатах. Це добре було показано Яном Гудфеллоу в його статті [5], де він продемонстрував, що при додаванні шуму до початкового знімку панди ШІ розпізнавала остаточну картинку як гібона, хоча з початковим зображенням таких проблем не було. В реальності це може мати досить суттєві негативні наслідки для тих сфер, що використовують СШІ для розпізнавання зображення.

Щодо маніпуляцій інформацією стосовно приватних користувачів, досить цікавим було дослідження [6] щодо «бульбашок фільтрів». Справа в тому, що більшість користувачів Інтернету через персоналізацію мають певні обмеження в отриманні інформації. І неначе то правильна тактика, яка допомагає уникнути інформаційного перевантаження та делегувати частину роботи ШІ для концентрації насправді важливих речей. Але це призводить до підвищеної вразливості до хибної інформації, адже, як відомо, людина схильна вірити тим судженням, що підтверджуються вже наявними у неї твердженнями, навіть якщо вони хибні. Це все говорить про можливість зловмисного групування людей, їх дезінформування через подання «фейкових новин» та подальшого злочинного використання (наприклад, для створення певної політичної ситуації).

Крім того, на практиці людина схильна більше довіряти даним та рішенням, отриманим за допомогою ШІ, не зважаючи на можливі помилки та упередження. А це призводить до того, що до проблем використання СШІ часто додаються проблеми, пов'язані з хибним використанням самої системи. Тож, як зазначають американські дослідники [7], внаслідок використання системи COMPAS у сфері кримінального судочинства через машинне упередження відбувалася несправедливість у використанні поруки та покарань.

Деякі автори [8] розглядають п'ять видів ризиків, що пов'язані з впровадженням ШІ (табл. 1): 1) ризик, пов'язаний зі збереженням конфіденційних даних; 2) ризики, пов'язані з технологією роботи системи; 3) ризик, пов'язаний зі збільшенням кількості даних, які обробляються, сортуються та зберігаються; 4) ризик, пов'язаний з упередженим судженням ШІ через неякісне навчання; 5) ризики, пов'язані з налагодженням комунікації між людиною та системою.

Таблиця 1. Ризики впровадження ШІ та можливі шляхи їх уникнення

Ризик	Можливі шляхи уникнення
Низький рівень захисту даних	– Підвищена увага до міри захисту даних – Управління доступом – Дослідження різноманітних методів захисту від кібератак – Застосування прозорих протоколів – Виявлення та аналіз прогалин в системі захисту
Особливості технології роботи системи	– Моніторинг ефективності – Моніторинг аналітики – Застосування прозорих протоколів
Збільшенням кількості даних, які обробляються, сортуються та зберігаються	– Моніторинг ефективності – Якісне тестування та перевірка системи – Впровадження тестування користувачами
Упереджене судження ШІ через неякісне навчання	– Перевірка результатів на пояснюваність та прозорість – Якісне тестування та перевірка системи – Впровадження тестування користувачами – Систематичний контроль результатів – Виявлення та аналіз помилок
Низький рівень комунікації між людиною та системою	– Цілеспрямоване навчання працівників – Впровадження тестування користувачами – Зворотний зв'язок

Окремо треба зазначити ті наслідки, які спричинить повсюдне використання ШІ; і тут насамперед треба звернути увагу на два аспекти: етичні проблеми використання ШІ та питання персоналу.

До етичних питань, що у майбутньому можуть виникнути і стати гострими через впровадження ШІ, можна віднести: питання розподілу матеріальних благ, що є виробленими за допомогою автоматизованих та комп'ютеризованих систем; питання людської взаємодії з технікою та ступеня довіри до неї; питання можливості (чи неможливості) контролю за навчанням ШІ і тих наслідків, до яких може призвести його розвиток.

Але одним з перших проблемних аспектів, що вже зараз постає у зв'язку з автоматизацією та комп'ютеризацією виробництва, є питання вимог до персоналу та наявності робочих місць. Адже, як зазначається дослідниками [9], через впровадження СШІ майже 375 млн осіб до 2030 року будуть змушені перевчитися та змінити роботу, оскільки відбудеться автоматизація та комп'ютеризація їх поточного робочого місця. А отже, досить гостра проблема безробіття вже не за горами і маячить на горизонті.

Висновки. Із зростанням зацікавленості світу до глибокого навчання, популяризації біометричних систем та автономних машин, повсюдного впровадження штучного інтелекту у житті сучасної людини все гострішим стає питання інформаційної та економічної безпеки. Сьогодні вже неможливо уявити роботу сучасного підприємства без використання інформаційних технологій та ШІ, але також ще не можна уявити його діяльність без людей, які б слідкували за справністю функціонування технологічного процесу і коригували недоліки, що виникають під час застосування СШІ. Саме людям у подальшому доведеться знайти собі відповідну роль у процесі, який поєднає критичне мислення людини і високі технологічні можливості комп'ютера.

Список використаних джерел

1. Пантєлєєва Н. М. Фінансова безпека в умовах цифрової економіки: очікування і реальність. Міжнародний науково-практичний журнал «Фінансовий простір». 2020 № 2(38). С. 22–37.

2. Mark Purdy and Paul Daugherty, Why Artificial Intelligence is the Future of Growth, Accenture. 2016. P. 27. URL: https://www.accenture.com/t20170524T055435__w__/ca-en/_acnmedia/PDF-52/Accenture-Why-AI-is-the-Future-of-Growth.pdf (дата звернення: 26.02.21).

3. Nicholas Chen, Lau Christensen, Kevin Gallagher, Rosamond Mate, Greg Rafer. Global Economic Impacts Associated with Artificial Intelligence. P. 23 URL: https://www.analysisgroup.com/globalassets/content/insights/publishing/ag_full_report_economic_impact_of_ai.pdf (дата звернення: 26.02.21).

4. Osoba, Osonde A., and William Welser, An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence, Santa Monica, Calif.: RAND Corporation, RR-1744-RC, 2017. As of September 12, 2017. URL: https://www.rand.org/pubs/research_reports/RR1744.html (дата звернення: 26.02.21).

5. Goodfellow, Ian & Shlens, Jonathon & Szegedy, Christian. Explaining and Harnessing Adversarial Examples. 2014. URL: https://arxiv.org/abs/1412.6572 (дата звернення: 26.02.21).

6. Pariser, Eli, The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think, United Kingdom: Penguin Books, 2012. P. 294.

7. Angwin, Julia L., Jeff Larson, Surya Mattu, and Lauren Kirchner. Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks. ProPublica. 2016. URL: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (дата звернення: 26.02.21).

8. Benjamin Cheatham, Kia Javanmardian, and Hamid Samandari. Confronting the risks of artificial intelligence. April 2019. URL: https://www.healthindustryhub.com.au/wp-content/uploads/2019/05/Confronting-the-risks-of-AI-2019.pdf (дата звернення: 26.02.21).

9. Sam Ransbotham, Philipp Gerbert, Martin Reeves, David Kiron, Michael Spira. Artificial Intelligence in Business Gets Real URL: http://innovationinsider.com.br/wp-content/uploads/2018/09/60280 MITSMR-BCGReport-2018. Pdf (дата звернення: 26.02.21).

Надійшла до редакції 15.03.2021

References

1. Pantielieieva N. M. Financial security in the digital economy: expectations and reality [Financial security in the digital economy: expectations and reality]. The international scientific and practical journal "Financial space". 2020 № 2(38). С. 22–37. [in Ukr.].

2. Mark Purdy and Paul Daugherty, Why Artificial Intelligence is the Future of Growth, Accenture. 2016. P. 27. URL: https://www.accenture.com/t20170524T055435__w__/ca-en/_acnmedia/PDF-52/Accenture-Why-AI-is-the-Future-of-Growth.pdf.

3. Nicholas Chen, Lau Christensen, Kevin Gallagher, Rosamond Mate, Greg Rafer. Global Economic Impacts Associated with Artificial Intelligence. P. 23 URL: https://www.analysisgroup.com/globalassets/content/insights/publishing/ag_full_report_economic_impact_of_ai.pdf.

4. Osoba, Osonde A., and William Welser, An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence, Santa Monica, Calif.: RAND Corporation, RR-1744-RC, 2017. As of September 12, 2017. URL: https://www.rand.org/pubs/research_reports/RR1744.html.

5. Goodfellow, Ian & Shlens, Jonathon & Szegedy, Christian. Explaining and Harnessing Adversarial Examples. 2014. URL: https://arxiv.org/abs/1412.6572.

6. Pariser, Eli, The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think, United Kingdom: Penguin Books, 2012. P. 294.

7. Angwin, Julia L., Jeff Larson, Surya Mattu, and Lauren Kirchner. Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks. ProPublica, 2016. URL: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

8. Benjamin Cheatham, Kia Javanmardian, and Hamid Samandari. Confronting the risks of artificial intelligence. April 2019. URL: https://www.healthindustryhub.com.au/wp-content/uploads/2019/05/Confronting-the-risks-of-AI-2019.pdf.

9. Sam Ransbotham, Philipp Gerbert, Martin Reeves, David Kiron, Michael Spira. Artificial Intelligence in Business Gets Real. URL: http://innovationinsider.com.br/wp-content/uploads/2018/09/60280 MITSMR-BCGReport-2018.

SUMMARY

Olha D. Stanina. The role of artificial intelligence in ensuring the state economic security. The article provides a rationale for the need to study the impact of artificial intelligence on the economic security of each individual enterprise in particular and the country as a whole. The main reasons and advantages of the widespread introduction of systemic artificial intelligence in various spheres of human activity have been

determined. The author gives promising directions for using artificial intelligence, such as machine learning, speech analysis, virtual assistants, machine vision, expert systems, and the like. The areas of application of artificial intelligence in various areas of the economy, such as trade, marketing, industry, transport, banking and telecommunications sectors, are outlined. The author identifies a number of threats and difficulties that a person faces in the process of introducing artificial intelligence, namely: low level of data protection; features of the technology of the artificial intelligence system; an increase in the amount of data that is processed, sorted and stored; preconceived judgments about artificial intelligence due to poor-quality training; a low level of communication, which can be traced in the process of interaction between a person and a system, and the like. For each of the designated types of risk, possible measures are proposed, thanks to which the negative impact of artificial intelligence on the economic security of Ukraine is counteracted. Also, the article contains a number of difficulties that are associated with the peculiarities of the work of artificial intelligence systems. The author cites research showing that artificial intelligence is able to increase productivity growth, but it can also have an ambiguous effect on labor. The article also touches on ethical issues related to the use of artificial intelligence.

Keywords: *security, economic security, artificial intelligence, prospects, risks.*

УДК 338.22
DOI 10.31733/2078-3566-2021-1-342-347

Світлана ТЮТЧЕНКО
старший викладач
(Дніпропетровський державний університет внутрішніх справ)

Аліна ВАРЯНИЧЕНКО
асистент
(Університет Лазарського у Варшаві, Польща)

НАЦІОНАЛЬНА БЕЗПЕКА ЯК ДИНАМІЧНА СКЛАДОВА СТРАТЕГІЇ СТАЛОГО РОЗВИТКУ ДЕРЖАВИ

У статті досліджено визначення та забезпечення національної безпеки України на сучасному етапі становлення держави як одного з векторів Стратегії сталого розвитку. На підставі здійснених досліджень зроблено висновки щодо визначення національної безпеки України та шляхів її забезпечення. За авторським підходом, національна безпека визначається як динамічна складова стратегічного розвитку держави, метою якої є забезпечення безпеки держави, бізнесу та громадян, захищеності інвестицій та приватної власності, забезпечення миру і захисту кордонів.

Ключові слова: *національна безпека, стратегія розвитку, стратегія безпеки, національні інтереси, загрози, політика національної безпеки України, ризики.*

Постановка проблеми. Світові фінансові та економічні кризи є знаковими етапами в міжнародній системі політичних, економічних відносин та відносин у сфері національної безпеки. У цих умовах надзвичайно важливим є реальне бачення стану, місця і ролі кожної країни в глобальному світі, що динамічно змінюється. Тож зараз виникає потреба до переосмислення підходів щодо організації національної безпеки України та системи її забезпечення.

Головною умовою існування та розвитку України на сучасному етапі є визначення національних інтересів держави, шляхів їх досягнення та забезпечення національної безпеки.

Національна безпека, як окрема наукова галузь, охоплює методологію всіх споріднених наук і тому є комплексною за своєю суттю. Метою статті є визначення та обґрунтування

© Тютченко С. М., 2021
ORCID iD: https://orcid.org/0000-0001-8480-6519
k_inf@dduvs.in.ua

© Варяниченко А. О., 2021
k_inf@dduvs.in.ua