ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС
Матеріали Міжнародної науково-практичної конференції
2

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 16 травня 2025 року

Том 2

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

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 16 травня 2025 року

Том 2

Одеса
2025

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 16.05.2025 р.)

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

Є 24 **Європейські орієнтири розвитку України: нові виміри у воєнний час** : у 2 т. : матеріали Міжнар.наук.-практ. конф. (Одеса, 16 травня 2025 р.) / за заг. ред. С. В. Ківалова. – Одеса : Фенікс, 2025. – Т. 2. – 716 с.
ISBN 978-617-8430-61-0

Матеріали Міжнародної науково-практичної конференції «Європейські орієнтири України: нові виміри у воєнний час» містять результати наукових досліджень і практичних напрацювань вчених, фахівців і військовослужбовців, здійснені в умовах повномасштабної війни. У збірнику представлено як теоретичні, так і емпіричні дослідження у галузях філософії, загальної теорії держави і права, історії права, сучасних соціально-політичних процесів, соціології та психології.

Особливу увагу приділено аналізу загроз національній безпеці в конституційному, міжнародному та європейському правовому контекстах, а також питанням трудового, соціального, земельного, аграрного та екологічного права. Окремі розділи присвячено функціонуванню економіки та підприємництва в умовах євроінтеграції.

У збірнику також розглянуто проблематику цифрової трансформації, захисту інформації та кібербезпеки в умовах воєнного часу, методику викладання іноземних мов, перекладознавство, лінгвістику і журналістику. Висвітлено наукові здобутки в адміністративному, фінансовому, морському та митному праві, реформуванні судової системи, діяльності прокуратури, правоохоронних органів та адвокатури. Окремо проаналізовано питання кримінального права, кримінального процесу, кримінології, криміналістики, судової експертизи, медико-психологічного забезпечення правосуддя, а також аспекти цивільного, сімейного, господарського права, інтелектуальної власності та патентного судочинства. Розглянуто також актуальні питання діяльності бібліотек у закладах вищої освіти та фізичної підготовки здобувачів вищої освіти.

Збірник адресовано науковцям, викладачам, здобувачам вищої освіти, а також практикам у галузях права, економіки, соціології, політології, психології, філології, журналістики та кібербезпеки.

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

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

ISBN 978-617-8430-61-0

СЕКЦІЯ 22. ІНФОРМАТИЗАЦІЯ ТА ЦИФРОВІЗАЦІЯ СУСПІЛЬСТВА В ЕПОХУ СТРІМКОГО РОЗВИТКУ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

СЕКЦІЯ 23. КІБЕРБЕЗПЕКА ОСОБИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ ЯК ФУНДАМЕНТАЛЬНИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

непридатні. Структуровані логи, що включають унікальні ідентифікатори запитів, допомагають відстежувати шлях виконання через різні компоненти системи. Автоматизація процесів розгортання через інструменти на кшталт AWS CloudFormation або Terraform забезпечує узгодженість інфраструктури та мінімізує ризик людської помилки.

Безсерверна архітектура відкриває нові горизонти у створенні масштабованих, економічно ефективних застосунків. Успішна реалізація цього підходу вимагає глибокого розуміння відповідних архітектурних патернів та дотримання належних практик проектування. Подальший розвиток у цій галузі може бути досягнутий через освоєння спеціалізованих інструментів, таких як AWS SAM (Serverless Application Model), який спрощує визначення інфраструктури безсерверних застосунків, та Serverless Framework, що надає єдиний інтерфейс для роботи з різними хмарними провайдерами. Ці інструменти не лише підвищують продуктивність розробників, але й сприяють впровадженню кращих практик у процес створення безсерверних застосунків.

Список використаних джерел:

1. AWS Serverless Application Model. URL: https://www.serverless.com/
2. AWS API Gateway. URL: https://aws.amazon.com/ru/api-gateway/
3. AWS Lambda. URL: https://docs.aws.amazon.com/lambda/
4. Cloud Native Patterns Illustrated: Fan-in and Fan-out. URL: https://surl.lu/uqpzjb
5. Асинхронна взаємодія на основі повідомлень. URL: https://surl.li/miuppa
6. Serverless Framework. URL: https://aws.amazon.com/ru/serverless/sam/

Ключові слова: безсерверна архітектура, патерни, Serverless Application Model, API gateway, Serverless Framework.

Keywords: serverless architechture, patterns, Serverless Application Model, API gateway, Serverless Framework.

Трофименко Олена Григорівна
Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій,
кандидат технічних наук, доцент

ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА КОНКУРЕНТОСПРОМОЖНІСТЬ В ІТ

Ландшафт ІТ-сфери зараз стрімко змінюється, а тому вимагає постійної адаптації і навчання від її працівників. Загальні навички, набуті під час освіти, можуть допомогти на старті професійної кар'єри в ІТ, а для того, щоб бути дійсно конкурентоспроможними, варто поглиблювати спеціалізацію в конкретних

галузях, серед яких: штучний інтелект, машинне навчання, блокчейн, квантові обчислення, кібербезпека, хмарні обчислення тощо. Важливо постійно оволодівати новими технологіями, більш продуктивними інструментами та методами, тим самим розвивати професійні навички. ІТ-сфера постійно потребує інноваційних підходів. Курси, сертифікації, вебінари та участь у наукових конференціях допоможуть бути в курсі останніх трендів. Дізнаватися про тренди та обмінюватися досвідом з іншими фахівцями ІТ-галузі можна й через онлайн-спільноти, форуми, LinkedIn чи то інші платформи. Співпраця й обмін досвідом з іншими професіоналами та дослідниками може надати можливість співпраці у розробці стартапів, нових програмних продуктів та інноваційних рішень, що врешті решт підвищуватиме конкурентоспроможність.

Не менш важливими є комунікативні навички, вміння працювати в команді, лідерство, гнучкість та здатність до швидкого вирішення проблем, адже ці навички також впливають на успіх в ІТ-кар'єрі. Врахування важливості та розвитку soft skills працівників сприяє їх ефективній взаємодії та зацікавленості в досягненні гарних результатів, високій якості й продуктивності для конкурентоздатності компанії у глобальному професійному середовищі. Командна робота, тайм-менеджмент, здатність визнавати помилки, емоційний інтелект, креативність, лідерські якості, терпіння, емпатія, гнучкість у розв'язанні проблем, навички взаємодії з людьми – це основні соціальні компетентності, які потрібно розвинути розробнику програмного забезпечення для підвищення своєї продуктивності, успішного виконання професійних завдань у команді [1]. Важливо підтримувати здоровий баланс між роботою та особистим життям, адже високий рівень стресу й вигорання може впливати на продуктивність і креативність. Корисно знаходити час для відпочинку та відновлення сил.

Штучний інтелект (ШІ) є потужним інструментом для можливого покращення своїх навичок і для підтримки конкурентоспроможності в ІТ-галузі. Насамперед, ШІ допомагає автоматизувати численні рутинні, повторювані завдання, серед яких: оброблення великих даних, розробка тест-кейсів та наборів тестових даних для тестування програмного забезпечення, моніторинг систем і навіть підтримка клієнтів. Це дозволяє зекономити час, який можна витратити на більш стратегічні або творчі завдання. ШІ-інструменти допомагають писати код швидше та з меншими помилками, пропонуючи автодоповнення, перевірку синтаксису чи навіть оптимізацію коду. Це дозволяє значно зменшити час на розробку і покращити якість програмного забезпечення. Завдяки здатності ШІ швидко аналізувати великі обсяги даних, можна використовувати його для виявлення трендів, патернів та прогнозування тенденцій при ухваленні рішень [2]. Наприклад, за допомогою алгоритмів машинного навчання можна прогнозувати поведінку користувачів, виявляти аномалії в системах безпеки і навіть оптимізувати бізнес-процеси.

ІТ-спеціалісти можуть використовувати ШІ для оптимізації різноманітних процесів у компаніях: від автоматизації складних розрахунків до покращення

роботи з клієнтами через чат-боти і системи підтримки на основі ШІ [3]. Також ШІ може використовуватися ІТ-фахівцями для генерування нових ідей, наприклад, у дизайні програмних продуктів або у створенні контенту [4]. ШІ-платформи для генерування зображень або текстів допомагають ІТ-фахівцям створювати нові концепції і навіть автоматизувати частину творчих процесів.

ШІ є корисним інструментом для виявлення загроз у кібербезпеці. Системи на основі ШІ здатні виявляти аномалії в реальному часі, прогнозувати можливі атаки й автоматично реагувати на загрози, що врешті решт дозволяє швидше адаптуватися до змін у безпековому ландшафті [5].

Ба більше, ШІ-платформи можуть бути використані для персоналізованого навчання, адже системи на базі ШІ можуть адаптувати навчальний процес до індивідуальних потреб кожного, швидко аналізуючи прогрес навчання і підлаштовуючи матеріал під сильні та слабкі сторони індивіда. Це дозволяє максимально ефективно освоювати новітні технології та підвищувати кваліфікацію фахівця.

Хоча ШІ може бути потужним інструментом для покращення ефективності та конкурентоспроможності фахівців в ІТ-сфері, є ситуації, коли його використання є недоцільним або навіть шкідливим. Це стосується ухвалення стратегічних рішень для бізнесу з урахуванням етичних питань, які ШІ не може розуміти, а тому не здатен замінити людський досвід. В управлінні бізнес-процесами та ухваленні критичних рішень саме людська інтуїція та досвід здатна враховувати контекст та моральні аспекти, а тому не доречно в цих питаннях покладатись виключно на алгоритми ШІ. ШІ поки не здатен до справжнього творчого процесу, тому в задачах, що потребують креативного підходу, нестандартних ідей та інновацій (наприклад, у розробці нових концепцій) його застосування не є ефективним, позаяк людська креативність залишається незамінною. Варто зважати на те, що надмірне використання ШІ може призвести до надмірної залежності від технологій і алгоритмів, що обмежить людську здатність до критичного мислення та ухвалення рішень. У разі збоїв або помилок у системах ШІ компанія може опинитися в скрутному становищі.

Оскільки ШІ потребує великих обсягів даних для тренування, то в разі, коли даних недостатньо або коли дані нерепрезентативні для певної задачі (наприклад, дані для тренування ШІ у сфері набору персоналу можуть містити приховані упередження), це може призвести до некоректних (дискримінаційних) або несправедливих результатів. В таких випадках застосування ШІ може тільки погіршити ситуацію. Алгоритми ШІ можуть хибно інтерпретувати дані або помилятися у виявленні патернів, що призведе до некоректних висновків та рішень. Наприклад, в області прогнозування попиту чи виявлення аномалій у безпеці неправильно налаштований ШІ може призвести до серйозних бізнес-проблем чи то збоїв. З іншого боку, оскільки ШІ може працювати з великими обсягами особистих даних або чутливої інформації, то це ставить під загрозу конфіденційність та безпеку персональних даних. Зловмисники можуть використовувати вразливості в системах ШІ для атак або зловживань.

З одного боку, автоматизація за допомогою ШІ може призвести до скорочення робочих місць, особливо в сферах, де можуть бути автоматизовані рутинні, повторювані завдання. Це може створити соціальні й економічні виклики, зокрема для тих, хто не може швидко адаптуватися до нових ролей. З іншого боку, коли використання ШІ для автоматизації процесів починає заміняти важливі функції, які мають виконувати люди (наприклад, у відносинах з клієнтами чи підтримці), це може призвести до зниження якості обслуговування, оскільки клієнти дедалі частіше відчувають відчуження від автоматизованих систем, коли потребують особистого контакту або нестандартного підходу. У випадках, коли системи на основі ШІ не мають належного моніторингу або нагляду, можна зіткнутися з проблемами, пов'язаними з неконтрольованими результатами, навіть якщо вони теоретично працюють добре.

Немаловажним фактором при використанні ШІ є потреба у великих ресурсах для його налаштування та підтримки. Впровадження ШІ вимагає значних інвестицій у ресурси, як фінансові, так і людські. Якщо організація не має необхідних ресурсів для належної інтеграції та моніторингу ШІ-систем, це може привести до значних витрат без бажаних результатів.

Наразі вже не йдеться про те, чи варто використовувати ІТ-фахівцям інструменти ШІ у свої роботі. Використовувати ШІ можна і потрібно, але важливо зважати на можливі обмеження та наявні ризики, щоб його застосування було максимально ефективним і безпечним. Треба ретельно оцінювати контекст, в якому планується впроваджувати технології ШІ, і буди готовим до контролю та коригування процесів у разі потреби. Завдяки розумному і виваженому застосуванню ШІ, ІТ-спеціалісти зможуть не лише автоматизувати процеси, а й отримати перевагу на ринку, підвищити свою кваліфікацію та адаптуватися до швидких змін в ІТ-галузі.

Список використаних джерел:

1. Трофименко О. Г., Савєльєва О. С., Прокоп Ю. В., Логінова Н. І., Дика А. І. Soft skills для розробників програмного забезпечення. *Кібербезпека: освіта, наука, техніка.* 2023. № 3(19). С. 6-19. URL: https://doi.org/10.28925/2663-4023.2023.19.619.

2. Трофименко О. Г., Лобода Ю. Г., Дика А .І., Мільченко О. О., Стрілець М. І. Штучний інтелект у системному аналізі. *Таврійський науковий вісник. Серія: Технічні науки*». 2024. № 5. С. 85-97. URL: https://doi.org/10.32782/tnv-tech.2024.5.9.

3. Трофименко О. Г., Прокоп Ю. В., Задерейко О. В., Логінова Н. І. Класифікація чат-ботів. *Системні технології.* 2022. № 2 (139). С. 147-159. URL: https://doi.org/10.34185/1562-9945-2-139-2022-14.

4. Трофименко О. Г., Дика А. І., Лобода Ю. В., Толокнов А. А., Бондаренко М. Є. Штучний інтелект у розробці ігор. *Кібербезпека: освіта, наука, техніка*. 2025. № 3(27). С. 109-119. URL: https://doi.org/10.28925/2663-4023.2025.27.701

5. Трофименко О. Г., Соколов А. В., Чикунов П. О., Ахмаметьєва Г. В., Манаков С. Ю. Штучний інтелект у військовій кіберсфері. *Технології та інжиніринг.* 2024. № 4 (21). С. 85-92. URL: https://doi.org/10.30857/2786-5371.2024.4.8.

Ключові слова: штучний інтелект, ШІ, машинне навчання, ІТ-галузь, ІТ-кар'єра, конкурентоспроможність.
Keywords: artificial intelligence, AI, machine learning, IT industry, IT career, competitiveness.

Чанишев Рашид Ібрагімович
Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій,
кандидат юридичних наук, доцент

PROTECTEU – НОВА ВНУТРІШНЯ СТРАТЕГІЯ БЕЗПЕКИ ЄВРОПЕЙСЬКОГО СОЮЗУ

Європейською комісією 1 квітня 2025 року було презентовано громадськості нову безпекову стратегію для країн Євросоюзу, що отримала назву «ProtectEU». Завданням цієї стратегії є посилення можливостей Європейського Союзу щодо забезпечення захисту громадян від багатоаспектних загроз сучасності шляхом створення вдосконаленої нормативно-правової бази, орієнтованої на розширення механізмів транскордонного співробітництва та забезпечення належного рівня інформаційного обміну між державами-членами ЄС, а також посилення координаційної ролі загальноєвропейських інституцій у боротьбі зі злочинністю та кіберзагрозами [1].

Нова стратегія прийшла на зміну попередній: «Стратегії Союзу безпеки ЄС 2020-2025 рр.» (Security Union Strategy), що створила основу для координації заходів із боротьби з тероризмом, організованою злочинністю та кіберзагрозами. Водночас ProtectEU доповнює презентовану 26 березня 2025 року «Стратегію Європейського Союзу із забезпечення готовності» (Preparedness Union Strategy), орієнтовану на зміцнення спроможності ЄС запобігати, виявляти й ефективно реагувати на широкий спектр криз – від природних катастроф та пандемій до кібератак і гібридних загроз, та презентований Європейською комісією 19 березня 2025 року стратегічний документ «White Paper for European Defence – Readiness 2030», що має на меті зміцнити оборонне співробітництво та промисловий потенціал країн ЄС.

За словами комісара ЄС із внутрішніх справ Магнуса Бруннера (Magnus Brunner), основною метою стратегії ProtectEU є назріла необхідність зміни менталітету і способу мислення щодо безпеки на державному рівні для всіх країн, що входять до Євросоюзу [2].

У документі наголошується, що наразі спостерігається зростання гібридних загроз як з боку низки ворожих («hostile») держав, так і з боку організованих