МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ

МАУП

ISSN 3083-6557 print

НАУКОВІ ПРАЦІ МАУП

Проблеми модернізації України

Випуск 1 (48), 2025

Київ
2025

УДК 330-339; 321.7; 159.9
М58

Схвалено Вченою радою Міжрегіональної Академії управління персоналом (протокол № 4 від 28.05.2025)

Редакційна колегія:
С. В. Храпатий (голова), д-р фіз.-мат. наук, проф.
І. А. Семенець-Орлова, д-р наук з держ. упр., проф.
Я. М. Раєвська, д-р психол. наук, проф.
С. О. Лисенко, д-р юрид. наук, проф.
А. І. Федосов, д-р мед. наук, проф.
М. І. Зубрицький, д-р. юрид. наук
О. М. Гордієнко, канд. техн. наук
В. І. Меджебель (*Чуєнко*), канд. юрид. наук
Л. М. Крива, канд. істор. наук
І. М. Капеліста (виконавчий редактор), канд. наук з держ. упр.
Є. Я. Черняк

Матеріали подано в авторській редакції.
Відповідальність за зміст та орфографію матеріалів несуть автори.

Міжрегіональна Академія управління персоналом.
М58 Наукові праці МАУП. Проблеми модернізації України / редкол.: С. В. Храпатий (голова) [та ін.]. Вип. 1 (48). Київ: Міжрегіональна Академія управління персоналом, 2025. 686 с. Бібліогр. в кінці ст.

У збірнику висвітлено матеріали X Міжнародної науково-практичної конференції "Розбудова інноваційних економіки, менеджменту та освіти в умовах нової соціальної реальності" (Київ, Міжрегіональна Академія управління персоналом, 20–22 травня 2025 р.).

Наведено тези доповідей учасників науково-практичної конференції МАУП з проблематики широкого кола аспектів процесу системної модернізації України.

Для науковців, громадсько-політичних діячів, студентів, а також усіх, хто цікавиться розвитком Української держави і світовим досвідом проведення модернізаційних процесів.

Видається з 2001 року.
Періодичність: 1 раз на квартал.
Засновник: *ПрАТ "ВНЗ "Міжрегіональна Академія управління персоналом".*
УДК 330-339; 321.7; 159.9

© Міжрегіональна Академія управління персоналом (МАУП), 2025

В. Г. Деменко
Актуальні системи штучного інтелекту різного функціоналу як інструмент інноваційного розвитку *657*

А. О. Абрамов, Р. Р. Гавеля, Р. Д. Овчаренко, Л. С. Осадча, О. С. Снєжков
Автоматичне генерування розкладу для наукових підрозділів: сучасні підходи та інноваційні рішення *659*

М. С. Коваленко
Штучний інтелект як інструмент забезпечення кібербезпеки *660*

МОДЕРНІЗАЦІЯ МЕДИЧНОЇ ТА ФАРМАЦЕВТИЧНОЇ ОСВІТИ

Д. О. Герасименко
Формування довіри пацієнтів як ключовий фактор успішного реінжинірингу в приватній медицині *662*

O. G. Aliyeva, O. O. Popazova, L. V. Makeyeva, O. I. Pototska, T. S. Gromokovska, M. L. Tavrog
Innovative strategies for teaching of morphological disciplines in modern medical education *664*

Я. Ю. Биц, В. М. Рудіченко
Роль динамічного візуалізуючого спостереження за порожнистими утворами печінки у своєчасному менеджменті пацієнтів на різних етапах надання медичної допомоги (з використанням власних клінічних спостережень) *667*

В. М. Рудіченко, Я. Ю. Биц
Опрацювання нормативно-правової бази інноваційного оцінювання повсякденного функціонування особи на прикладі власних клінічних спостережень важкого хворого при підготовці лікарів первинної ланки *670*

Г. О. Кузьменко, Р. М. Якуба
Особливості функціонування системи охорони здоров'я в умовах децентралізації *672*

Р. М. Якуба
Модернізація медичної та фармацевтичної освіти: виклики, тенденції, перспективи *674*

Г. О. Кузьменко, В. Шекман
Механізми управління наданням медичної допомоги на місцевому рівні *675*

Г. О. Кузьменко, В. М. Бузовір
Інноваційно-цифрові та нормативно-ресурсні підходи до модернізації управління ЕМД *677*

- Враховують людський фактор, включаючи побажання науковців, потреби у гнучкому графіку, уникнення емоційного вигорання, що є критичним для дослідницької діяльності.

Таким чином, новизна теми виявляється у комплексному, інтелектуальному та гнучкому підході до автоматизації процесів.

1. Розробка ефективного, адаптивного та уніфікованого алгоритму автоматичного формування розкладів для забезпечення потреб викладачів та здобувачів освіти.
2. Проектування інтуїтивно зрозумілого, адаптивного інтерфейсу користувача для взаємодії з формами введення та табличними структурами даних у системі.
3. Розробка механізму ідентифікації користувачів з подальшим розпізнаванням ролей в процесі автентифікації та авторизації для забезпечення безпечного і рольового доступу до функціоналу системи.
4. Створення централізованої структури бази даних, яка підтримує взаємодію з кількома пов'язаними таблицями, зокрема тими, що містять інформацію про викладачів, студентів та їхні ролі в системі.
5. Розробка алгоритму генерації розкладів у форматі PDF з урахуванням параметрів, визначених користувачем, з метою забезпечення зручного експорту та подальшого використання.
6. Створення системи стилізації інтерфейсу, яка відповідає загальній візуальній концепції веб-ресурсів МАУП, з дотриманням принципів єдиного брендингу та користувацької ідентичності.

Доля особистої участі:
Абрамов А. О. — back-end developer
Гавеля Р. Р. — back-end, front-end and MySQL developer
Овчаренко Р. Д. — back-end, front-end and MySQL developer
Осадча Л. С. — front-end developer
Снєжков О. С. — back-end and MySQL developer

Науковий керівник: **А. О. Коваль**,
старший викладач кафедри ІКІТД

М. С. КОВАЛЕНКО
аспірант, МАУП, м. Київ

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Розвиток цифрових технологій супроводжується зростанням обсягів кіберзагроз, які щороку ускладнюються та модифікуються. В умовах гібридної війни, масових кібератак на критичну інфраструктуру, системи управління, фінансові та державні ресурси України, питання забезпечення кібербезпеки набуває надзвичайної актуальності. Одним із найбільш перспективних інструментів протидії є впровадження систем

штучного інтелекту (ШІ), здатних до самонавчання, прогнозування атак, виявлення аномалій та автоматизованого реагування [1].

Розвиток систем штучного інтелекту в контексті кібербезпеки відкриває нові горизонти у боротьбі з постійно еволюціонуючими кіберзагрозами. В умовах стрімкої цифровізації та високої динаміки інформаційного простору, традиційні засоби захисту втрачають свою ефективність. ШІ, навпаки, забезпечує можливість гнучкого, адаптивного й проактивного реагування, що стає критично важливим у запобіганні складним атакам, які часто здійснюються з використанням штучного інтелекту самими зловмисниками.

Однією з найважливіших переваг ШІ в цій сфері є здатність до виявлення невідомих раніше загроз — так званих zero-day атак. Використовуючи алгоритми глибокого навчання, системи можуть аналізувати великі обсяги даних у режимі реального часу, розпізнавати відхилення у поведінці користувачів або пристроїв, а також визначати потенційно шкідливі дії ще до того, як вони призведуть до реальних наслідків. Це дозволяє реалізовувати концепцію превентивного кіберзахисту, що значно підвищує стійкість інформаційних систем. Крім того, інтеграція ШІ в системи кібербезпеки сприяє автоматизації процесів реагування на інциденти. Завдяки цьому вдається мінімізувати часові витрати на аналіз і ухвалення рішень, що є ключовим фактором у ситуаціях, коли кожна секунда може мати критичне значення. Наприклад, виявлення та блокування фішингової атаки або вторгнення в мережу в межах кількох секунд може зупинити розповсюдження шкідливого програмного забезпечення і врятувати чутливі дані.

Попри численні переваги, широке впровадження ШІ у сферу кіберзахисту стикається з низкою викликів. Перш за все, йдеться про етичні, правові та організаційні обмеження. Питання прозорості алгоритмів, забезпечення недискримінаційного прийняття рішень, збереження конфіденційності та запобігання зловживанням залишаються актуальними і потребують комплексного регулювання. Національне законодавство має йти в ногу з технологічним розвитком, створюючи чіткі рамки для безпечного та відповідального використання інтелектуальних систем. Важливо також враховувати геополітичний контекст. Для України, яка вже кілька років перебуває в умовах гібридної війни, впровадження ШІ у сферу кібербезпеки є не лише питанням технологічного розвитку, а й елементом стратегічної оборони. Це вимагає координації між державними органами, науковими установами, бізнесом і громадянським суспільством для створення національної екосистеми кіберзахисту, в якій ШІ відіграє центральну роль. Таким чином, ШІ постає не лише як інструмент підвищення технічної ефективності, а як системоутворюючий фактор нової архітектури цифрової безпеки. Його потенціал полягає у здатності забезпечити стійкий кіберпростір, захистити державні інституції, критичну інфраструктуру та кожного громадянина у світі, де інформаційні загрози дедалі більше стають елементом глобальної нестабільності.

Джерела

1. Концепція розвитку штучного інтелекту в Україні. 2020. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#n8
2. OECD. Artificial Intelligence in Society. Paris: OECD Publishing, 2019. 140 p. DOI: https://doi.org/10.1787/eedfee77-en