УДК 378:351.86:004.056 DOI: 10.31673/2786-8362.2026.017902

Конотопець М.М., к.т.н.; **Щиголь Ю.Ф.,** к.юр.н.;
Кубрак В.О, PhD; **Крамський А.Є.;**
Туровський О.Л., д.т.н.

РОЗВИТОК НАЦІОНАЛЬНОЇ СИСТЕМИ ПРОФЕСІЙНОЇ КВАЛІФІКАЦІЇ ТА ТРАНСФОРМАЦІЇ ВИЩОЇ ОСВІТИ В СЕКТОРІ БЕЗПЕКИ ТА ОБОРОНИ ВІДПОВІДНО ДО СТАНУ НОВІТНІХ ЦИФРОВИХ ТЕХНОЛОГІЙ ТА ГІБРИДНОГО ХАРАКТЕРУ ЗАГРОЗ ОБ'ЄКТАМ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Konotopets M.M., Shchygol Yu.F., Kubrak V.O., Kramsky A.Ye., Turovskyi O.L. Development of the national system of professional qualifications and transformation of higher education in the security and defense sector in accordance with the state of the latest digital technologies and the hybrid nature of threats to critical information infrastructure facilities. The article considers the impact of the development of information technologies on the processes of standardization of professions in the context of the hybrid nature of threats to critical information infrastructure facilities.

Special attention is paid to the transformation of professional competencies in the field of information technologies and cybersecurity under the influence of digitalization, automation, the introduction of artificial intelligence and the spread of new technologies, such as: GNSS, RTLS, Bluetooth, Wi-Fi and Wi MAX, adaptive signal processing. It was determined that one of the important competencies of a future specialist in the field of cybersecurity and information protection is strategic academic communication, which allows graduates of higher education institutions to quickly adapt to life and work in a multicultural environment.

The need for constant updating of professional standards is substantiated, taking into account the rapid nature of the evolution of cyber threats, the latest technologies that connect the physical, digital and biological worlds, the emergence of new business models, the restructuring of production, consumption, transport and supply systems.

Mechanisms for implementing adaptive professional standards are proposed, which will ensure the flexibility of the educational system's response to the needs of the industry.

Based on the research conducted, the main directions of state policy regarding the development of human resources in the information technology industry and cybersecurity as a fundamental element of the state's digital resilience are formulated.

Keywords: artificial intelligence, digital technologies, hybrid nature of threats, critical information infrastructure objects, internationalization of higher education, professional standards

Конотопець М.М., Щиголь Ю.Ф., Кубрак В.О., Крамський А.Є., Туровський О.Л. Розвиток національної системи професійної кваліфікації та трансформації вищої освіти в секторі безпеки та оборони відповідно до стану новітніх цифрових технологій та гібридного характеру загроз об'єктам критичної інформаційної інфраструктури. У статті розглянуто вплив розвитку інформаційних технологій на процеси стандартизації професій у контексті гібридного характеру загроз об'єктам критичної інформаційної інфраструктури.

Особливу увагу приділено трансформації професійних компетентностей у галузі інформаційних технологій та кібербезпеки під впливом цифровізації, автоматизації, впровадження штучного інтелекту та поширення нових технологій, таких як: GNSS, RTLS, Bluetooth, Wi-Fi і Wi MAX, адаптивної обробки сигналів. Визначено що однією з важливих компетентностей майбутнього фахівця сфери кібербезпеки та захисту інформації є стратегічна академічна комунікація, що дозволяє щвидко адаптуватись випускникам закладів вищої освіти до життя та роботи в мультикультурному середовищі.

Обґрунтовано необхідність постійного оновлення професійних стандартів з урахуванням швидкоплинного характеру еволюції кіберзагроз, новітніх технології, що зв'язують фізичний, цифровий та біологічний світи, появою нових бізнес-моделей, перебудовою систем виробництва, споживання, транспорту та постачання.

Запропоновано механізми впровадження адаптивних професійних стандартів, що забезпечать гнучкість реагування освітньої системи на потреби галузі.

На основі проведеного дослідження сформульовано основні напрями державної політики щодо розвитку кадрового забезпечення галузі інформаційних технологій та кібербезпеки як фундаментального елементу цифрової стійкості держави.

Ключові слова: штучний інтелект, цифрові технології, гібридний характер загроз, об'єкти критичної інформаційної інфраструктури, інтернаціоналізація вищої освіти, професійні стандарти

Вступ

Неодмінно кібербезпека в сучасному світі відіграє важливу роль і є однією з вагомих складових національної безпеки, економічної стабільності країни та суспільної довіри. З розвитком цифрових технологій зростають і загрози, спрямовані на уряди, бізнес та окремих осіб, що в свою чергу робить сильний кіберзахист критично важливим інструментом для захисту критичної інформаційної інфраструктури та даних.

Таким чином, однією з складових забезпечення належного рівня національної безпеки України, є високий рівень навченості особового складу, його якісна підготовка на всіх рівнях вищої освіти (бакалаврському, магістерському, PhD) періодичне підвищення кваліфікації та оволодіння новими знаннями в професії [1]. При цьому компетентності, що визначають здатність здобувачів вищої освіти виконувати трудові функції та трудові дії, які тісно пов'язані з захистом об'єктів критичної інформаційної інфраструктури повинні відповідати викликам ведення гібридної війни та сталому тренду інтернаціоналізації вищої освіти.

Аналіз останніх досліджень. На сьогоднішній день в Україні створена, функціонує та отримує подальшого розвитку система захисту інформації, яка складається із взаємопов'язаної сукупності трьох базових складових: організаційної інфраструктури, нормативно-правової та матеріально-технічної бази, які поєднані між собою за метою, місцем, часом та завданнями з захисту інформації.

Так, відповідно з розпорядженням Кабінету Міністрів України від 3 грудня 2025 р. за № 1383-р, Про затвердження операційного плану заходів з реалізації у 2025-2028 роках, Стратегії розвитку вищої освіти в Україні на 2022-2032 роки та внесення змін до Стратегії розвитку вищої освіти в Україні на 2022-2032 роки визначено відповідні стратегічні цілі в рамках яких сформовані операційні цілі та кроки їх досягнення. Так, в Стратегічній цілі 1. Ефективність управління в системі вищої освіти, що є соціально відповідальною зазначено, що формування пріоритетів підготовки фахівців з вищою освітою, зокрема ІТ-спеціальностей, необхідно проводити на основі моніторингу ринку праці з забезпеченням переходу до формування державного замовлення на підготовку здобувачів вищої освіти на новій інформаційній базі. Там же, було запропоновано запровадження системи контрактування першого робочого місця для майбутніх випускників-бюджетників, які здобули вищу освіту за рахунок бюджетних коштів.

В Стратегічній цілі 3. Забезпечення якісної освітньо-наукової діяльності, конкурентоспроможної вищої освіти, яка є доступною для різних верств населення передбачено гармонізацію освітніх та професійних стандартів, залучення бізнесу та професійних спільнот до їх розроблення, оснащення сучасних базових навчальних лабораторій та передових науково-дослідних лабораторій закладів вищої освіти обладнанням для інформаційних технологій (цифровою інфраструктурою).

Вагомим фактром в формуванні компетентностей майбутнього фахівця сфери кібербезпеки та захисту інформації є стратегічна академічна комунікація, яка представляє собою цілеспрямоване, системне і довгострокове управління інформаційними потоками в закладах вищої освіти (ЗВО) та спрямована на досягнення академічних, дослідницьких і соціальних цілей.

Вона охоплює як внутрішню комунікацію між науково-педагогічними працівниками, здобувачами вищої освіти та керівництвом закладу вищої освіти, так і зовнішню взаємодія з академічною спільнотою на державному та міжнародному рівнях, співпрацю з бізнесом, громадськістю, стейкхолдерами.

На це спрямована Операційні ціль 1 та 4. Забезпечення порівнюванності та визнання українських освітніх кваліфікацій в Європі та світі. Стратегічної цілі 4. Інтернаціоналізація вищої освіти України. *Вони передбачає розвиток національної системи кваліфікацій, спрощення процедур визнання іноземних освітніх кваліфікацій, гармонізацію системи освітньої статистики в межах євроінтеграційних зобов'язань України та адаптація випускників закладів вищої освіти до життя та роботи в мультикультурному середовищі*.

Цю думку яскраво підтверджує і нещодавній форум Європейського фонду управління якістю (EFQM 2025), – що уявляє собою інноваційну некомерційну організацію, яка поєднує

аналітичні звіти, ретельно підібрані програми навчання та розвитку, а також можливості для налагодження контактів на користь організацій та окремих осіб у всьому світі. Ключові моменти діяльності фонду полягають в сприянні забезпеченню технологічного лідерства, що є критично важливим рушієм продуктивної праці, процвітання, креативності, інновацій та сталого розвитку.

Реалізація інноваційних моделей управління в майбутньому буде пов'язана з підвищенням організаційної досконалості компаній та робочого персоналу шляхом запровадження спрощених процедур визнання професійних кваліфікацій та комплексних навчальних програм, які підкріплені відповідними сертифікатами.

Центральне місце в таких моделях управління посідають процеси адаптації до нових робочих практик, що характеризується зростанням популярності віддаленої та гібридної видів роботи, що вимагає нових практик та середовищ. При реалізації такого підходу важливим є забезпечення стійкості ланцюгів поставок, безперервності ведення бізнесу та прогнозування розвитку.

Немало важливим елементом в формуванні компетентностей майбутнього фахівця сфери кібербезпеки та захисту інформації є стратегічна академічна комунікація, яка представляє собою цілеспрямоване, системне і довгострокове управління інформаційними потоками в закладах вищої освіти та спрямована на досягнення академічних, дослідницьких і соціальних цілей. Вона охоплює як внутрішню комунікацію між науково-педагогічними працівниками, здобувачами вищої освіти та керівництвом закладу вищої освіти, так і зовнішню взаємодія з академічною спільнотою на державному та міжнародному рівнях, співпрацю з бізнесом, громадськістю, стейкхолдерами.

В Стратегічній цілі 5. Привабливість закладів вищої освіти для навчання та академічної кар'єри на найближчу перспективу зазначено, що важливим фактором особистого та професійного зростання є створення умов для безперервного навчання (освіти дорослих) в результаті чого буде визнання результатів навчання неформальної та інформальної освіти в системі формальної освіти, підтвердження професійних кваліфікацій розроблення концепції модульної архітектури здобуття другої вищої освіти з врахуванням результатів навчання неформальної та інформальної освіти.

В звіті Європейського центру розвитку професійної освіти (Cedefop) [2], зазначається що системна діяльність щодо розширення міжнародного розуміння кваліфікацій і кваліфікаційних рівнів у країнах за посередництвом європейських інструментів, таких, як: Болонський процес, Європейська рамка кваліфікацій (EQF), Європейська кредитна система професійної освіти і навчання (ECVET) та Europass у поєднанні із зростаючою міжнародною рекрутинговою мобільністю персоналу в компаніях, збільшила розуміння і потенціал цінності національних кваліфікацій на міжнародному ринку праці.

Зміни, що відбуваються у функціях кваліфікацій, пов'язані з: а) дією кваліфікацій як показника для попиту і пропозиції на ринку праці; б) дією кваліфікацій як показника для міжнародних порівняльних досліджень; в) досягненням колективних угод; г) розвитком трудових ресурсів; г) цінністю кваліфікацій для фізичних осіб та їх мотиваційним ефектом щодо навчання [2] .

В свою чергу основною метою Europass стало надання громадянам доступ до зручних та уніфікованих інструментів, що є зрозумілими у європейському просторі освіти й праці, з метою представлення своїх знань, навичок, освітніх досягнень і професійного досвіду. Першого липня 2024 року відбувся офіційний запуск Національного центру Europass в Україні, що стало важливим крок до спрощення прозорості кваліфікацій та доступу до нових перспектив у сфері освіти й працевлаштування.

Наступним інструментом з розвиток компетентностей профорієнтаційної спільноти впродовж життя через призму європейського досвіду є відома в Європі європейська мережа національних ресурсно-інформаційних центрів з професійної орієнтації Euroguidance. Вона об'єднує фахівці з профорієнтації, експерти з розробки політик в секторі освіти та сфери зайнятості в країнах-членах ЄС, а також у країнах-кандидатах та співфінансується програмою Erasmus+ у 38 європейських країнах включаючи Україну.

Директива (ЄС) 2022/2557 Європейського Парламенту та Ради від 14 грудня 2022 року про стійкість критично важливих об'єктів та про скасування Директиви Ради 2008/114/ЄС. Вона розкриває поняття CER (Critical Entities Resilience) — «фізичної» стійкісті критичної інфраструктури, встановлює європейську правову базу для забезпечення безперервного надання послуг, необхідних для підтримки життєво важливих суспільних або економічних функцій, на всьому єдиному ринку та замінює Директиву 2008/114/ЄС, яка вважалася застарілою через зростання кількості загроз (кібернетичних, фізичних, кліматичних, гібридних) і зростаючу взаємозалежність інфраструктур по всій Європі.

Директива вимагає від держав-членів визначати, контролювати та підтримувати державні або приватні установи, що вважаються критично важливими в 11 ключових секторах, таких як енергетика, транспорт, охорона здоров'я та водопостачання. Ці установи повинні впроваджувати організаційні та технічні заходи для запобігання, протидії, пом'якшення та відновлення після інцидентів, які можуть вплинути на надання основних послуг.

Директива також вимагає від кожної держави-члена прийняти до 17 січня 2026 року національну стратегію стійкості, що базується на оцінці ризиків та супроводжується заходами підтримки. Документ також визначає посилену координацію між національними та європейськими органами влади, тісно пов'язану з вимогами щодо кібербезпеки директиви NIS2 [3].

Крім міжнародних стандартів в Україні сформовано та продовжує вдосконалюватись національне законодавство з цих питань. Прикладом може слугувати Закон №1882-IX “Про критичну інфраструктуру”, який визначає правові та організаційні засади національної системи захисту критичної інфраструктури, розкриває режими функціонування (штатний/криза/відновлення), визначає розмежування повноважень між суб’єктами та їх координацію, і є складовою законодавства у сфері національної безпеки [4].

Ще один документ, який запроваджує єдиний державний підхід до моніторингу захищеності систем, у яких обробляються державні інформаційні ресурси, службова інформація або дані, що становлять державну таємницю є постанова Кабінет Міністрів України, ухвалена від 31 грудня 2025 р. № 1799 «Про затвердження Порядку оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об’єктів критичної інфраструктури, об’єктів критичної інформаційної інфраструктури».

Нові правила дають можливість імплементувати кращі міжнародні практики, зокрема вимоги Директиви ЄС 2022/2555 (NIS2) та стандарти серії ISO/IEC 27001 та NIST CSF [5,6].

Наступним документом є “Порядок оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об’єктів критичної інфраструктури, об’єктів критичної інформаційної інфраструктури”. Він визначає чіткий механізм проведення оцінювання для органів державної влади, місцевого самоврядування та операторів критичної інфраструктури. Документ запроваджує чотири ключові види оцінювання: перевірку дотримання цільових профілів безпеки для авторизації систем, аналіз поточного стану кіберзахисту, оцінювання на відповідність національним стандартам та оцінку стану захищеності державних інформаційних ресурсів [7].

Спільний наказ Служби безпеки України та Адміністрації Держспецзв’язку від 19 грудня 2024 року № 627/772. “Деякі питання розробки, затвердження та погодження планів захисту об’єктів критичної інфраструктури за проектною загрозою національного рівня “кібератака кіберінцидент” спрямований на удосконалення кіберзахисту критичної інфраструктури. В ньому затверджено нові рекомендації та форма плану захисту від кіберзагроз для об’єктів критичної інфраструктури (ОКІ – далі) та виділено три глобальних напрямки. В напрямку “Вдосконалення взаємодії” надано оновлені шаблони планів, обов’язковим є проведення оцінки ризиків, врахування взаємозалежностей між об’єктами інфраструктури та адаптацію до ландшафту нових загроз. Змінено і порядок затвердження планів: тепер вони мають погоджуватися послідовно з Держспецзв’язку та СБУ.

В напрямку “Кіберстійкість” акцент робиться на процес безупинної цифрової трансформації, що пов’язана з остаточним переходом на європейскі стандарти кібербезпеки

відповідно до вимог Закону України № 4336-IX. “Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об’єктів критичної інформаційної інфраструктури”.

В напрямку “Стримування” основним завданням залишається моніторинг та аналіз діяльності , що пов'язаний з підготовкою щорічних аналітичних звітів про виконання Плану реалізації Стратегії кібербезпеки [8].

Активно сприяє розвитку національної системи професійної кваліфікації Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України №865 від 29.12.2025. Про затвердження професійних стандартів у сфері захисту критичної інфраструктури. А саме ним введено в дія такі професійні стандарти, як : *“Аналітик з оцінки ризиків, загроз та стану захищеності об’єктів критичної інфраструктури (за видами діяльності)”; “Експерт із захисту об’єктів критичної інфраструктури (за видами діяльності)”;“Фахівець із захисту та стійкості критичної інфраструктури*”[9].

Постановка завдання. Стаття присвячена аналізу впливу розвитку інформаційних технологій на стандартизацію професій, розгляду основних міжнародних та українських нормативно-правових документів, та їх адаптації в Україні. Окрему увагу приділено гібридному характеру викликів критичній інформаційній інфраструктурі, які потребують комплексного підходу до професійної підготовки фахівців у цій галузі. Основні проблеми, що досліджуються в статті:

1. Аналіз міжнародних та українських нормативно-правових документів, що в сучасних реаліях враховують необхідні професійні навички та уміння фахівця майбутнього.

2. Вплив процесів впровадження цифрових технологій, автоматизації та використання штучного інтелекту, процесів аналізу великих даних, використання хмарних технологій та мобільних пристроїв, розвитку Інтернету речей (IoT) на зміну вимог до сучасних професійних компетентностей у галузі інформаційних технологій.

3. Трансформація необхідних фахових компетентностей сучасного фахівця кібербезпеки та захисту інформації під впливом гібридного характеру загроз об’єктам критичної інформаційної інфраструктури.

4. Шляхи досягнення затребуваних компетентностей у фахівців кібербезпеки майбутнього з урахуванням викликів сучасності.

Метою статті є дослідження ключових проблем створення ефективної системи підготовки кадрового потенціалу зі спеціальності Кібербезпека та захисту інформації, який буде здатний в майбутньому протидіяти швидкоплинному ландшафту загроз та забезпечувати побудову конкурентоспроможної економіки.

Виклад основного матеріалу дослідження

Одними з вагомих факторів впливу на бурхливий розвиток затребуваних на ринку праці результатів навчання є швидкоплинні процеси впровадження цифрових технологій, автоматизація та використання штучного інтелекту, процесів аналізу великих даних, використання хмарних технологій та мобільних пристроїв, розвиток Інтернету речей (IoT), та багато інших призводить до трансформації традиційних трудових функцій та трудових дій в професіях та появи нових, які вимагають сучасних компетенцій та інноваційних підходів до вирішення проблемних питань.

Так, з появою цифрової обробки РЧ-сигналів (Digital RF) стали поширеними бездротові мережі та поява інтернету речей (IP). Так Digital RF представляє собою злиття цифрових комп'ютерних технологій, цифрової обробки сигналів та програмованих логічних інтегральних схем (ПЛІС) з традиційними радіочастотними додатками. Це призвело, як до блискавичного поширення нових технологій, таких як GNSS, RTLS, Bluetooth, Wi-Fi і Wi MAX, та появи нових продуктів для кінцевих користувачів. В свою чергу ПЛІС дозволяють будувати складні проекти на одному кристалі, проводити багаторівневу перевірку на всіх етапах розробки, а при необхідності дозволяють здійснювати швидку реконфігурацію внутрішньої архітектури в процесі їх функціонування.

Прикладом можуть слугувати глобальні супутникові навігаційні системи, GPS включно транслюють сигнали які приймаються наземними пристроями такими як смартфони та трекери. В результаті попереднього аналізу цих сигналів системи визначають точне місцезнаходження об'єкту на земній поверхні, що широко застосовується в військовій справі, судноводінні, міжнародних перевезеннях, метеорології і таке інше.

Крім глобальних радіотехнологій отримали поштовх в розвитку і локальні технології місцезнаходження – так званні RTLS-системи. Вони забезпечують актуальною інформацією в реальному масштабі часу і дозволяють легко визначати своє місцезнаходження всередині протяжних за розмірами об'єктів та систем, застосовувати в якості ідентифікації людей та техніки, різного роду обладнання, а також забезпечення контролю доступу до об'єктів захисту.

З цієї ж метою можливо використання технологію Wi-Fi позиціонування. Пристрої сканують Wi-Fi-мережі та використовують значення потужності сигналів для розрахунку свого місцезнаходження.

Іншим прикладом для визначення свого місцезнаходження на малих відстанях служать опорні сигнали Bluetooth-маячків, які постійно випромінюються в повітряний простір. Мобільні пристрої або трекери визначають своє місцеположення відносно цих сигналів.

Ще одним варіантом реалізації є ультразвукова система RTLS. Вона використовує ультразвукові хвилі для позиціонування та слідкування всередині приміщення. Система розраховує місцезнаходження об'єктів або людей, аналізуючи час проходження ультразвукових сигналів від передавача до приймача. В порівнянні з такими технологіями, як Wi-Fi RTLS, ультразвукова система RTLS забезпечує високу точність та стійкість до електромагнітних завад. Вона широко поширена в робототехніці, системах безпеки та системах позиціонування всередині приміщень, де точність визначення місцезнаходження об'єктів є вельми важливою характеристикою. Разом з тим ультразвукова система RTLS може затребувати більш складної інфраструктури в порівнянні з іншими технологіями.

Вагомим фактором розвитку радіотехнологій останніх десятиліть також стало втілення в радіотехнічних системах адаптивної цифрової обробки сигналів. Це дало можливість реалізації потенційно можливих характеристик радіоелектронних систем в умовах швидкоплинної радіоелектронної обстановки та постійного її ускладнення, збільшення пропускної здатність таких засобів та комплексів, автоматизації процесів та підвищення якості їх функціонування.

Так в системах рухомого зв'язку четвертого та п'ятого поколінь експлуатуються адаптивні антенні решітки з алгоритмами адаптації, які засновані на рівняннях Вінера-Хопфа. А використання технології MIMO (Multiple Input Multiple Output – множинний вхід, множинний вихід), для бездротового зв'язку та мобільного інтернету, яка базується на розподілені потоку даних між декількома антенами для їх передачі та наступного прийому. Це дозволяє паралельно передавати данні по декількох потоках, що значно підвищує швидкість передачі сигналів та якість сигналів що передаються.

Адаптивна обробка сигналів суттєво покращила боротьбу з мінімізацією впливу завад в умовах невизначеності про їх параметри. А саме, актуальними є напрямки поєднання методів MIMO та адаптивної обробки сигналів, розподілених обчислень вагових коефіцієнтів в системі зв'язку на базі даних геоінформаційних систем.

Швидкий розвиток Інтернету речей (далі – IoT) також завдав сприятливого впливу на подальші корінні зміни в комунікаційних технологіях і на сьогоднішній день пропонує різноманітні сервіси для клієнтів. Відомі методи штучного інтелекту (далі – AI) активно впроваджуються для спрощення процедур IoT та підвищення їх потенціалу в сучасних умовах [10].

Слід зауважити, що вдале поєднання IoT та AI призвело до нової мережевої парадигми під назвою Інтелектуальний інтернет речей (IIoT), яка сприяла суттєвій трансформації бізнесу та промисловим процесам, змінам в підходах до управління державним сектором та охороною здоров'я, підвищенню якості управління дорожнім рухом та протидії *мережевим атакам з подальшим застосуванням потенційних контрзаходів в кіберпросторі,* покращення якості

надання послуг місцевого самоврядування та адаптивному енергоменеджменту в розумних мережах, впровадженню розумних механізмів управління водними ресурсами для їх ефективного розподілу, збереження та підтримки якості питної води [10].

Термін «інтелектуальна індустрія» означає інтеграцію розумних технологій у виробничі процеси, і IIoT є необхідним для аналізу великих обсягів даних, створених промисловими машинами та IoT-пристроями. На різних етапах виробництва ці методології дозволяють моделювати процеси, моніторити, прогнозувати та контролювати [10].

Штучний інтелект (далі – AI) продовжує активно розвиватися, впливаючи на бізнес-процеси, технології та повсякденне життя людства. У найближчому майбутньому ми очікуємо на появу нових трендів, які визначатимуть напрямки розвитку AI. На сьогоднішній день відомі як мінімум п'ять головних трендів активного застосування AI в сферу життєдіяльності людства.

По-перше це активне просування AI в сферу повсякденних бізнес-процесів для уникнення виконання рутинних дій. Один із прикладів, що можна навести це застосування прогностичних моделей для організації продажу товарів та послуг, управління персоналом та процесами. Так уряди, які інвестують у цифрову грамотність та грамотність у сфері штучного інтелекту на державній службі, краще оснащені для відповідального управління технологіями. Це включає не лише технічні навички, але й здатність визначати проблеми, оцінювати результати та розмірковувати над непередбачуваними наслідками. Практика громади, спільні стандарти та внутрішні структури навчання мають більше значення, ніж індивідуальні історії успіху [11].

Розуміння ризику також еволюціонує. Відповідальне використання штучного інтелекту полягає не в уникненні невизначеності чи сліпому прийнятті технологій, а в цілеспрямованому управлінні ризиками протягом усього життєвого циклу системи: раннє встановлення очікувань, постійний моніторинг впливу та готовність адаптуватися або зупинитися, коли суспільна цінність не досягається.

Іншим напрямком втілення в людське життя є *використання генеративних моделей AI для створення текстів, відео-продукції та музикальних творів (обробка людської мови – NLP).* Так обробка природньої мови дозволяє полегшити її використання. Розуміння обчислювальними машинами текстів та мови в загалі дозволяє підвищувати продуктивність людської роботи за рахунок використання локальних чат-ботів, автоматизація процесів зменшує вплив людського фактору та зосередитись на ключових моментах бізнесу.

Третім визначним напрямком є *використання AI для виявлення кіберзагроз у реальному масштабі часу.* Так Attack Signal Intelligence (ASI) від Vectra AI – це технологія, яка використовує AI і машинне навчання для автоматизованого виявлення, аналізу та пріоритизації підозрілої активності в мережі. На відміну від традиційних систем безпеки, що генерують безліч попереджень, ASI фокусується на виявленні реальних ознак активних кібератак. ASI аналізує дані з різних джерел, включаючи мережевий трафік, логи, дані кінцевих точок і хмарні сервіси, для побудови повної картини того, що відбувається, і виявлення прихованих загроз. Унікальність ASI полягає в її здатності розуміти контекст атак, виявляти ланцюжки подій і оцінювати серйозність загрози з точки зору потенційного збитку для бізнесу [12].

Четвертим вагомим напрямком є використання *хмарних технологій* (Cloud Technology), що надає можливість людству отримувати обчислювальні ресурси для обробки та зберігання даних за принципом сервісу. Тобто, Вам не потрібно купувати дороге комп'ютерне обладнання – готовий продукт адаптований для використання на звичайному гаджеті або ПК у вигляді додатку. Доступ до нього надається за допомогою мережі інтернет. Як і інші технології вигадані людством, хмарним технологіям притаманні переваги та недоліки. Що стосується переваг, то до них можна віднести: гнучкість, економічність, швидкість взаємодії з даними, можливості захисту інформації, автоматизація процесів, доступність.

До недоліків даної технології можна віднести: обов'язкову наявність інтернету, неможливість повного контролю за фізичними серверами, неможливість дізнатись про фізичне знаходження даних, необхідність слідкувати за регулярною сплатою [13].

Ще одним важливим напрямком є аналітика великих даних, яка включає методи, інструменти та застосунки, які використовуються для збору та обробки великих масивів різнорідних та швидко створюваних даних, та видобування з них цінної інформації. Джерелом цих даних можуть слугувати браузери, мобільні застосунки, електронна пошта, соціальні мережі та інтелектуальні мережеві пристрої. Отримана початкова інформація можлива бути представлена як в структурованому так і в неструктурованому вигляді та в різних форматах. Користь використання аналітика великих даних полягає в можливості швидкого корегування виробничих процесів, підвищувати якість кінцевого продукту, індивідуально надавати послуги, оптимізувати та прогнозувати розвиток бізнесу [14].

Вплив гібридного характеру загроз об'єктам критичної інформаційної інфраструктури. З урахуванням сучасного етапу розвитку суспільства, сфери інформаційних технологій та наукових досягнень свідчить, що вирішення конфліктів між державами суто військовими методами не є ефективним. На перше місце виходить одночасне використання традиційних і не традиційних методів та засобів ведення війни. Використання цих методів та засобів у комплексі і є суттю «гібридної війни».

Гібридні війни стають особливо актуальними в контексті геополітичних конфліктів, де держави використовують широкий спектр засобів для досягнення своїх цілей. Російська гібридна агресія проти України є прикладом такого використання різних елементів військового та невійськового впливу для досягнення політичних та стратегічних цілей.

Визначальними складовими гібридних війн є інформаційна, ідеологічна, психологічна, економічна, політична, дипломатична, військова, технологічна, ресурсна, енергетична. Наразі зі зростанням інформаційних технологій, технологічних можливостей і різноманітних економічних зв'язків у сучасному світі з'являються нові форми ресурсного протиборства у вигляді транспортного, енергетичного, банківського, протиборства за інфраструктуру фінансових ринків та суттєві вплив на сферу охорони здоров'я та державного управління і навіть забезпечення питною водою та їжі, каналізації.

Типові приклади таких дій застосовувались і раніше. Так, спроба відвести води річки Йордан від Ізраїлю, яка стала однією з причин «шестиденної війни» 1967 р. [15]. Ці події увійшли в історію як «Водна криза».

На початку березня 2019 року влада Венесуели обвинуватила США в "електричній війні" з метою руйнування електроенергетики країни. Тоді міністр зв'язку та інформації Венесуели Хорхе Родригес в уряді Ніколаса Мадуро заявив, що до відключення електрики привела кібератака на гідроелектростанцію «Эль-Гурі». Тривале відключення електроенергії країні призвело до перебоїв в системі водопостачання низки міст [16].

Ще одним прикладом таких дій стало застосування російськими хакерами за кілька годин до початку російського вторгнення 24 лютого 2022 кіберзброї під назвою «AcidRain» проти американської компанії супутникового зв'язку Viasat з метою порушення командування та управління українськими військовими частинами та підрозділами, посіяти хаос на полі бою, коли російські війська перетнуть кордон [17].

На відміну від наведених вище прикладів, гібридні атаки можуть переслідувати кілька цілей одночасно. Користуючись прогалинами в національному або міжнародному законодавстві, Росія ставить собі за мету підірвати міжнародний порядок, заснований на верховенстві права, зображаючи західні країни лицемірами щодо їх власних цінностей та норм.

Мета також може бути більш конкретною й практичною: віднайти найефективніший шлях підриву засад цивільного життя й загального функціонування суспільства – чи то шляхом саботажу критичної інфраструктури, спричинивши політичні чвари за допомогою інформаційних операцій, чи то різними шляхами посіявши страх у суспільстві. У деяких випадках кібератаки достатньо для того, щоб зупинити роботу лікарні, як наприклад, це часто відбувалося останніми роками на території Франції [18].

Проте якщо ефект такої атаки може послабити адекватний кіберзахист, нападник може вдатися до фізичної атаки, перерізавши кабелі чи скоївши інші акти саботажу.

Наслідки різних типів атак надають супротивнику таку цінну інформацію, як наприклад, зручний час здійснення атаки. Так, навряд чи можна вважати простим проте в більшості випадків мета гібридної війни проходить нижче *порогу збройного конфлікту*. Тож це фактично явище, характерне для мирного часу. Росія тестує стійкість європейських країн, не порушуючи меж конвенційної війни, і таким чином веде свої дії поза межами можливостей ефективного реагування НАТО. До 2022 року Росія могла практично безкарно займатися агресивними діями в «сірій зоні» через брак політичної волі європейських столиць заявляти про її причетність і реагувати на такі відверто ворожі дії [19].

Від моменту введення в дію воєнного стану в 2022 році Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ) взяла на себе додаткові зобов'язання. Це включає в себе той факт, що служба наразі очолює процес формування національної політики кібероборони та нагляду за імплементацією рамок захисту критичної інформаційної інфраструктури (КІІ) [19].

Із квітня 2023 року ДССЗЗІ обслуговує Державний реєстр об'єктів критичної інформаційної інфраструктури України, разом із централізованою базою даних кіберзагроз та вразливостей. Ця система дозволяє ДССЗЗІ та профільним відомствам актуалізувати й слідкувати за виконанням вимог кібербезпеки щодо критичної інфраструктури, гармонізувати власне законодавство з вимогами ЄС, зважаючи на різний досвід європейських країн з імплементації Директиви NIS2, Директиви щодо стійкості критичної інфраструктури (CER) та європейських правил захисту даних. Навіть для країн-членів ЄС впровадження цих директив стало викликом – лише двом країнам вдалося вкластися в строки імплементації Директиви NIS2, і лише двом вдалося повноцінно реалізувати Директиву CER [19].

Із кінця 2023 року чотири комерційні судна, які прямували з російських портів у Балтійському морі, підозрюються в пошкодженні цифрових і електричних кабелів та підводного газопроводу [20, 21].

Окрім того, групи, пов'язані з російською зовнішньою розвідкою, часто вчиняли акти підпалу, фізичні напади, шкідливі кібервторгнення, радіоелектронні втручання в роботу комунікаційних систем, та інші акти саботажу проти критичної інфраструктури по всій Центральній, Східній та Північній Європі. Ці атаки часто зумисно плануються таким чином, щоб ускладнити їх виявлення, уникнути відповідальності й відкласти ефективне реагування на них [19].

Ще один яскравим прикладом гібридних дій у бойових діях у Перській затоці 2026 року стали удари по опріснювальних установках морської води в Ірані та Бахрейні – основних джерел питної води. Таким чином в лічені секунди перетворивши системи водопостачання з технологічного дива на вразливі місця інфраструктури країн і фактично ставлячи під загрозу базові умови життя цивільного населення.

Прецеденти таких дій вже були, коли у 1991 році іракські війська під командуванням Саддама Хусейна навмисно вилили нафту з кувейтського нафтопроводу в Перську затоку з метою перешкодити морській десантній операції сил США та їхніх союзників для визволення Кувейту, а також вивести з ладу сусідні саудівські опріснювальні установки.

Іншим випадком є обстріли Росією Запорізької АЕС та знищення греблі Каховської гідроелектростанції російськими окупаційними силами в загарбницькій війні проти України. Руйнування цієї гідроспоруди, наразило на небезпеку велику кількість цивільного населення та створило загрозу для системи охолодження реакторів Запорізької АЕС [22].

Шляхи досягнення затребуваних компетентностей у фахівців кібербезпеки майбутнього з урахуванням викликів сучасності. Для подолання вище зазначеної ситуації в технічній сфері необхідно намагатися зменшити технологічну залежність України від продукції іноземних виробників в сфері інформаційно-комунікаційних технологій та знижувати ступінь уразливості інформаційної інфраструктури від незадекларованих функцій шляхом запровадження дієздатної системи оцінки відповідності такої продукції вимогам з безпеки.

В організаційно-правовому полі спрямувати основні зусилля на вдосконалення законодавчих актів та нормативно-правових документів у сфері кібербезпеки та оновлення їх

у сфері захисту інформації. Пришвидшити процеси зв'язані з гармонізацією положень європейського законодавства з національним.

В площині підготовки кадрового потенціалу необхідно постійно моніторити ринок праці та дотримуватись відповідності рівня компетентностей що надаються під час навчання та підвищення кваліфікації фахівців з питань кібербезпеки та захисту інформації сучасним змінам бизнес-моделей на ринку праці. Спрямувати головний акцент на розвитку навичок аналізу отриманої інформації, умінню конструктивної аргументації та прийняттю виважених рішень, творчому підходу в подоланні критичних ситуаціях. А також більш ширшому впровадженню індивідуальних траєкторій навчання, вихованню відповідальності за свою освіту та вдосконалення професійних компетентностей.

Запорукою успішного оволодіння професією також є набуття здобувачами вищої освіти навичок роботи в багатонаціональних колективах. Відповідно до цього необхідно розвивати та удосконалювати систему тренінгів для здобувачів вищої освіти щодо роботи в багатонаціональному середовищі та глобальних бізнесах, посилити систему міжнародної мобільності в закладах вищої освіти.

З урахуванням розвитку Інтелектуального інтернету речей затребуваними будуть такі здібності, як креативність, ініціативність, лідерство та обґрунтований скептицизм. Для цього необхідно реалізовувати підхід доступного навчання суспільства країни протягом усього життя, щоб громадяни були не лише готові до майбутнього, що базується на штучному інтелекті, а й були активними, поінформованими та критично важливими учасниками його формування. У глобальній гонці за можливості штучного інтелекту найстійкішими суспільствами будуть ті, які ставляться до своїх громадян не лише як до користувачів технологій, а й як до їхніх здібних та впевнених розпорядників [23].

Для подолання низького рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту, побудови системи підвищення цифрової грамотності та культури безпекового поводження в кіберпросторі люди повинні володіти культурою обґрунтованого скептицизму. По-перша, вона базується на тому що за людиною залишається останнє слово, а AI лише підвищує її продуктивність і пришвидшує рух до поставленої мети. По-друге це кібергігієна. Вся конфіденційна інформація повинна залишатися виключно оф-лайн. По-третє, виховувати у громадян звичку перевіряти інформацію спираючись на довірені першоджерела.

Недостатня захищеність від кібератак державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури вимагає формування в державних органах відповідних структурних підрозділів, які виконували функції належного контролю за кіберзахистом.

Висновки

Стаття присвячена розгляду актуального наукового завдання, присвяченого аналізу вплив розвитку інформаційних технологій на процеси стандартизації професій у галузі інформаційних технологій та кібербезпеки на фоні гібридного характеру кіберзагроз об'єктам критичної інформаційної інфраструктури.

1. Проведено огляд основних нормативно правових документів національного та міжнародного законодавства у галузі інформаційних технологій та кібербезпеки, та їх імплементація в Україні.

Особливу увагу приділено трансформації професійних компетентностей у галузі інформаційних технологій та кібербезпеки під впливом цифровізації, автоматизації, впровадження штучного інтелекту та поширення нових технологій, таких як: GNSS, RTLS, Bluetooth, Wi-Fi і Wi MAX, адаптивної обробки сигналів.

Визначено що однією з важливих компетентностей майбутнього фахівця сфери кібербезпеки та захисту інформації є стратегічна академічна комунікація, що дозволяє швидко адаптуватись випускникам закладів вищої освіти до життя та роботи в мультикультурному середовищі.

2. Обґрунтовано необхідність постійного оновлення професійних стандартів з урахуванням швидкоплинного характеру еволюції кіберзагроз, новітніх технології, що

зв'язують фізичний, цифровий та біологічний світи, появою нових бізнес-моделей, перебудовою систем виробництва, споживання, транспорту та постачання.

3. Запропоновано механізми впровадження адаптивних професійних стандартів, що забезпечать гнучкість реагування освітньої системи на потреби галузі.

4. На основі проведеного дослідження сформульовано основні напрями державної політики щодо розвитку кадрового забезпечення галузі інформаційних технологій та кібербезпеки як фундаментального елементу цифрової стійкості держави.

Список використаної літератури:

1. Указ Президента України від 14 вересня 2020 року №392/2020. Про рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України». URL: https://www.president.gov.ua/documents/3922020-35037.

2. Changing qualifications. A review of qualifications policies and practices. – CEDEFOP Reference series.– Luxembourg, 2010. – 201-202 c. [Електронний ресурс]. – URL: http://www.CEDEFOP.europa.eu/EN/Files/3059_en.pdf.

3. Сайт: Wavestone (2026). CER Directive: where does Europe stand on critical infrastructure resilience? | Wavestone Insights/ (Директиви ЄС 2022/2555 (NIS2)). URL: https://www.wavestone.com/en/insight/critical-infrastructure-cybersecurity-cer-directive.

4. Про критичну інфраструктуру: Закон України від 21.09.2024 р. №1882-IX: станом на 21 вересня. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text.

5. Стандарти серії. ISO/IEC 27001:2022 – Система управління інформаційною безпекою (СУІБ).

6. The NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology. 29 February 26, 2024. URL: https://doi.org/10.6028/NIST.CSWP.

7. Постанова Кабінету Міністрів України від 31 грудня 2025 року № 1799 "Про затвердження Порядку оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури". URL: https://zakon.rada.gov.ua/laws/show/1799-2025-%D0%BF#Text.

8. Спільний наказ Служби безпеки України та Адміністрації Держспецзв'язку від 19 грудня 2024 року № 627/772. "Деякі питання розробки, затвердження та погодження планів захисту об'єктів критичної інфраструктури за проектною загрозою національного рівня "кібератака кіберінцидент". URL: https://cip.gov.ua/ua/news/spilnii-nakaz-sluzhbi-bezpeki-ukrayini-ta-administraciyi-derzhspeczv-yazku-vid-19-grudnya-2024-roku-627-772-deyaki-pitannya-rozrobki-zatverdzhennya-ta-pogodzhennya-planiv-zakhistu-ob-yektiv-kritichnoyi-infrastrukturi-za-proektnoyu-zagrozoyu-nacionalnogo-rivnya-kiberataka-kiberincident/.

9. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України №865 від 29.12.2025. Про затвердження професійних стандартів у сфері захисту критичної інфраструктури.

10. O. Aouedi *et al*., "A Survey on Intelligent Internet of Things: Applications, Security, Privacy, and Future Directions," in *IEEE Communications Surveys & Tutorials*, vol. 27, no. 2, pp. 1238-1292, April 2025, URL: https://doi.org/10.1109/COMST.2024.3430368.

11. Пірет Гірв. Від пілотних проектів до практики: що потрібно, щоб штучний інтелект працював в уряді. The e-Governance Conference: A mirror, a map and a springboard. Digital Governance in Practice 2026. Сайт: e-Governance Academy. 10.02.2026. URL: https://ega.ee/from-pilots-practice-what-it-takes-make-ai-work-government/.

12. Від шуму до сигналу: пріоритизація загроз за допомогою AI-platformи Vectra AI. Сайт: NWU 21.10.2025. URL: https://nwu.ua/blog/vectraai/vid-shumu-do-signalu-prioritizatsiya-zagroz-za-dopomogoyu-ai-driven-platformi-vectra-ai/.

13. Хмарні технології 2026 - що це таке та які хмари найкращі? Сайт: UCloud 18.02.2026. URL: https://ucloud.ua/hmarni-tehnologiyi-shho-cze-take/.

14. Що таке Big Data аналітика та як її використовують? Платформа клієнтської підтримки NovaTalks. URL: https://novatalks.com.ua/ua/blog/what-is-big-data-analytics-and-how-is-it-used-in-business/.

15. Бар Зохар Міхаель, Мішаль Ніссім. Моссад. Найвидатніші операції ізраїльської розвідки / пер. З англ. Олександр Міхельсон. – 2-ге вид. – К.: Наш Формат, 2022.– 384 с.

16. Venezuela goes dark in massive power outage. Deutsche Welle. 08.03.2019. URL: https://www.dw.com/en/venezuela-power-outage-causes-widespread-chaos/a-47821661.

17. Cyberattacks quietly launched by Russia before its invasion of Ukraine may have been more damaging than intended. Сайт: Business Insider. 18.05.2022. URL: https://www.businessinsider.com/russian-cyberattacks-on-ukraine-may-have-gotten-out-of-hand-2022-5?IR=T.

18. French hospital suspends operations after cyber attack. 5 December 2022, Сайт: France24. 05.12.2022. URL: https://www.france24.com/en/france/20221205-french-hospital-suspends-operations-after-cyber-attacks.

19. Посилення захисту критичної інфраструктури України: Стратегічні висновки й кращі міжнародні практики: «e-Governance Academy» / Академія електронного управління, квітень 2025 р. м. Таллінн, Естонія. Сайт: e-Governance Academy (2025). URL:https://ega.ee/publication/%d0%bf%d0%be%d1%81%d0%b8%d0%bb%d0%b5%d0%bd%d0%bd%d1%8f-%d0%b7%d0%b0%d1%85%d0%b8%d1%81%d1%82%d1%83-%d0%ba%d1%80%d0%b8%d1%82%d0%b8%d1%87%d0%bd%d0%be%d1%97-%d1%96%d0%bd%d1%84%d1%80%d0%b0%d1%81%d1%82/.

20. Henri Astier & Paul Kirby. Germany suspects sabotage over severed undersea cables in Baltic. Сайт: BBC Home - Breaking News, World News, US News, Sports, Business, Innovation, Climate, Culture, Travel, Video & Audio. 18.11.2024. URL: https://www.bbc.com/news/articles/c9dl4vxw501o.

21. By Kathryn Armstrong & Vishala Sri-Pathma. Finland investigates suspected sabotage of Baltic-connector gas pipeline. Сайт: BBC Home - Breaking News, World News, US News, Sports, Business, Innovation, Climate, Culture, Travel, Video & Audio.1010.2023. URL: https://www.bbc.com/news/world-europe-67070389.

22. Радіо Свобода. Підрив Каховської ГЕС: наслідки руйнування греблі, евакуація, загрози. Сайт: Радіо Свобода. 06.06.2023. URL: https://www.radiosvoboda.org/a/pidryv-kakhovska-hes-evakuatsiya-zahroza-zaes/32446581.html.

23. Крісті Ківіло. Масштабування навичок штучного інтелекту через глобальну співпрацю. Сайт: e-Governance Academy. 26.03.2026. URL: https://ega.ee/scaling-ai-skills-global-cooperation/.

Автори статті

Конотопець Микола – кандидат технічних наук, доцент, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна.

ORCID: 0000-0002-6963-1877

Щиголь Юрій – кандидат юридичних наук, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна.

ORCID: 0000-0002-7621-0616

Кубрак Володимир – PhD, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна.

ORCID: 0000-0001-8877-5289

Крамський Антон Євгенійович – Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна.

ORCID: 0000-0003-1431-242X

Туровський Олександр Леонідович – доктор технічних наук, професор, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0000-0002-4961-0876

Authors of the article

Konotopets Mykola – Candidate of Sciences (technical), Associate Professor, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine.

ORCID: 0000-0002-6963-1877

Shchygol Yuriy – Candidate of Sciences (juridical), National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine.

ORCID: 0000-0002-7621-0616

Kubrak Volodymyr – PhD, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine.

ORCID: 0000-0001-8877-5289

Kramsky Anton – National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine.

ORCID: 0000-0003-1431-242X

Turovskyi Oleksandr – Doctor of Sciences (technical), Professor, State University of Information and Communication Technologies, Kyiv, Ukraine.

ORCID: 0000-0002-4961-0876

Надійшла до редакції: 17.04.2026
Прийнята до друку: 05.05.2026
Опубліковано: 25.05.2026