

Освіта / Педагогічні науки	
377.091.3:004.056.5	
Дата першого надходження статті до видання	2026-08-30
Дата прийняття статті до друку після рецензування	2026-09-30
Дата публікації/оприлюднення	2026-09-30

Сучасні тенденції формування компетентностей з кібербезпеки у закладах професійної освіти

Бацуровська Ілона Вікторівна

доктор педагогічних наук, професор кафедри інтелектуальних систем та цифрових технологій

Академія праці, соціальних відносин і туризму, Київ, Україна

e-mail: ilona@outlook.com

<https://orcid.org/0000-0002-8407-4984>

Курєпін Вячеслав Миколайович

кандидат економічних наук (PhD), доцент кафедри методики професійного навчання

Миколаївський національний аграрний університет, Миколаїв, Україна

e-mail: kurepin@mnau.edu.ua

<https://orcid.org/0000-0003-4383-6177>

Анотація. У статті здійснено теоретико-аналітичне узагальнення сучасних тенденцій формування компетентностей з кібербезпеки у закладах професійної освіти в умовах цифрової трансформації ринку праці, поширення хмарних сервісів, штучного інтелекту, промислового Інтернету речей, кіберфізичних систем та дистанційно-мережевих форм навчання. Актуальність проблеми визначається тим, що професійна освіта готує майбутніх працівників до діяльності у виробничих і сервісних середовищах, де помилки користувача, слабка кібергігієна або нездатність своєчасно ідентифікувати інцидент можуть спричинити не лише втрату даних, а й порушення технологічних процесів, безпеки праці та безперервності діяльності організації. Метою статті є визначення та систематизація провідних тенденцій формування компетентностей з кібербезпеки у професійній освіті, а також обґрунтування компетентнісно-практичної моделі їх інтеграції в освітні програми. Методологічну основу становлять компетентнісний, системний, діяльнісний, контекстний та ризик-орієнтований підходи. Використано інтегративний огляд сучасних досліджень і нормативно-методичних документів, порівняльний аналіз рамок DigComp 2.2, European Cybersecurity Skills Framework (ECSF) та NICE Workforce Framework for Cybersecurity, категоріальний аналіз педагогічних практик і концептуальне моделювання. Визначено вісім взаємопов'язаних тенденцій: перехід від засвоєння знань до демонстрації спроможності діяти; рольове й професійно-контекстне структурування компетентностей; інтеграція кібергігієни в усі професійні профілі; поширення сценарного, проблемного та проєктного навчання; використання cyber range, Capture the Flag і симуляцій; гейміфікація та адаптивне мікронавчання; автентичне оцінювання через практичні докази виконання; посилення партнерства з роботодавцями та безперервного оновлення змісту. Запропоновано шестикомпонентну структуру компетентності з кібербезпеки для здобувачів професійної освіти, що охоплює кібергігієну, захист даних і цифрової ідентичності, безпечне використання професійних цифрових систем, управління ризиками й реагування на інциденти, правово-етичну відповідальність, командну взаємодію та професійне самонавчання. Наукова новизна полягає в обґрунтуванні переходу від

«курсу з кібербезпеки» до наскрізної моделі формування кіберстійкої професійної поведінки, де базові та галузеві компетентності поєднуються з практичною діяльністю і оцінюються за спостережуваними результатами. Практичне значення результатів полягає у можливості використання запропонованої моделі для модернізації освітніх програм, розроблення модулів, практичних занять, виробничого навчання, внутрішніх політик кібербезпеки та критеріїв оцінювання готовності здобувачів до безпечної професійної діяльності.

Ключові слова: професійна освіта, кібербезпека, компетентність з кібербезпеки, кібергігієна, цифрова компетентність, cyber range, Capture the Flag, гейміфікація, практико-орієнтоване навчання, цифрова безпека.

Current Trends in the Formation of Cybersecurity Competencies in Vocational Education Institutions

Iлона Батсуровська

Doctor of Science in Education, Professor, Department of Intelligent Systems and Digital Technologies

Academy of Labour, Social Relations and Tourism, Kyiv, Ukraine

e-mail: ilona@outlook.com

<https://orcid.org/0000-0002-8407-4984>

Viacheslav Kurepin

PhD in Economics, Associate Professor, Department of Vocational Training Methodology

Mykolaiv National Agrarian University, Mykolaiv, Ukraine

e-mail: kurepin@mnaeu.edu.ua

<https://orcid.org/0000-0003-4383-6177>

Abstract. The article provides a theoretical and analytical synthesis of current trends in the formation of cybersecurity competencies in vocational education institutions amid the digital transformation of the labour market, the spread of cloud services, artificial intelligence, the industrial Internet of Things, cyber-physical systems, and network-based learning. The relevance of the problem is determined by the fact that vocational education prepares future employees for work in production and service environments where user errors, poor cyber hygiene, or the inability to identify an incident in time may lead not only to data loss but also to disruptions in technological processes, occupational safety, and organisational continuity. The purpose of the article is to identify and systematise the leading trends in the development of cybersecurity competencies in vocational education and to substantiate a competence- and practice-oriented model for integrating them into educational programmes. The methodological framework combines competence-based, systems, activity-based, contextual, and risk-oriented approaches. The study employs an integrative review of recent research and policy documents, comparative analysis of DigComp 2.2, the European Cybersecurity Skills Framework (ECSF), and the NICE Workforce Framework for Cybersecurity, categorical analysis of pedagogical practices, and conceptual modelling. Eight interrelated trends are identified: a shift from knowledge acquisition to demonstrated capability; role-based and profession-contextual structuring of competencies; integration of cyber hygiene into all occupational profiles; expansion of scenario-, problem-, and project-based learning; use of cyber ranges, Capture the Flag activities, and simulations; gamification and adaptive microlearning; authentic assessment through practical evidence; and stronger partnerships with employers combined with continuous content renewal. A six-component structure of cybersecurity competence for vocational learners is proposed, covering cyber hygiene, data and digital identity protection, secure use of professional digital systems, risk management and incident response, legal and

ethical responsibility, teamwork, and continuous professional learning. The scientific novelty lies in substantiating a transition from an isolated “cybersecurity course” to a cross-curricular model of cyber-resilient professional behaviour in which foundational and occupation-specific competencies are integrated with practical performance and assessed through observable outcomes. The practical significance is the possibility of applying the model to modernise curricula, develop modules and practical classes, organise workplace training, formulate institutional cybersecurity policies, and design assessment criteria for learners’ readiness for safe professional activity in digitally saturated workplaces.

Keywords: vocational education, cybersecurity, cybersecurity competence, cyber hygiene, digital competence, cyber range, Capture the Flag, gamification, practice-oriented learning, digital safety.

Вступ

Актуальність проблеми. Цифровізація виробництва, аграрного сектору, логістики, енергетики, торгівлі, адміністративних і сервісних процесів радикально змінює зміст професійної діяльності. У більшості професій працівник взаємодіє з обліковими системами, хмарними сервісами, мобільними застосунками, датчиками, обладнанням із мережевими інтерфейсами, системами автоматизації та електронними документами. За цих умов кібербезпека перестає бути винятково сферою IT-підрозділу: щоденні дії працівника стають частиною загальної кіберстійкості організації. Для професійної освіти це означає необхідність формувати не лише загальну цифрову грамотність, а готовність діяти безпечно в конкретному професійному контексті, розпізнавати ризики, дотримуватися процедур, відповідально поводитися з даними та коректно реагувати на інциденти.

Чинний Закон України «Про професійну освіту» від 21 серпня 2025 р. № 4574-IX посилює орієнтацію професійної освіти на сучасні потреби економіки, практичну підготовку та взаємодію з роботодавцями. Водночас Закон України «Про основні засади забезпечення кібербезпеки України» визначає освітні, організаційні та професійно-кваліфікаційні заходи як складники національної системи кібербезпеки. Отже, формування кібербезпекових компетентностей здобувачів професійної освіти є одночасно педагогічним завданням, умовою професійної якості та елементом ширшої культури безпеки.

Особливої ваги проблема набуває для професій, пов’язаних із виробничими мережами, електротехнічними установками, автоматизованими лініями, транспортом, агротехнологіями, медичними або фінансовими даними. У таких середовищах порушення принципів кібергігієни може перейти з інформаційної площини у фізичну: компрометація облікового запису, неправильне підключення зовнішнього носія, ігнорування оновлень або невірна реакція на підозріле повідомлення здатні порушити технологічний процес і створити ризик для людей. Саме тому кібербезпека у професійній освіті має розглядатися як складова професійної компетентності та безпеки праці, а не як ізольований теоретичний блок.

Аналіз останніх досліджень і публікацій. Сучасні підходи до формування кібербезпекової компетентності поєднують нормативні вимоги, цифрову грамотність і професійну підготовку. В Україні цей контекст визначається законодавством про професійну освіту та основні засади забезпечення кібербезпеки (Закон України № 4574-IX, 2025; Закон України № 2163-VIII, 2017). На міжнародному рівні DigComp 2.2 розглядає безпеку як складник цифрової компетентності, NICE Framework пов’язує кібербезпекову діяльність із завданнями, знаннями й навичками, а ECSF структурує компетентності через професійні ролі (Vuorikari et al., 2022; Petersen et al., 2020; Wetzel, 2023; ENISA, 2026). Підходи до оцінювання компетентностей студентів також акцентують поєднання знань, практичних умінь і здатності діяти в умовах ризику (Alammari et al., 2022).

Емпіричні дослідження підтверджують результативність практико-орієнтованих форматів. Capture the Flag сприяє відпрацюванню криптографії, мережевої та веббезпеки, а cyber range дає змогу переносити теоретичні знання у наближені до професійних ситуації (Švábenský et al., 2021; Lazarov et al., 2026). Значна увага приділяється гейміфікації: вона підвищує залученість і мотивацію, але потребує чіткого зв'язку з результатами навчання та оцінюванням реальних компетентностей (Weitl-Harms et al., 2023; Kim et al., 2025; van Steen & Deeleman, 2021; Razack & Mat Saad, 2024). Систематичні огляди та новітні дослідження також підтверджують перспективність ігрових платформ, сценарного навчання, хакерських симуляцій і завдань для кіберфізичних систем (Amzeyeva & Zhumabayeva, 2025; Arduin & Costé, 2026; Peter et al., 2024; Weeratunge et al., 2026). Окремі праці демонструють ефективність наративних підходів, зокрема під час навчання стеганографії, а також важливість раннього формування кібербезпекової обізнаності (Weijsenfeld & Sarmah, 2025; Quayyum et al., 2021).

В українських дослідженнях кібергігієна трактується як складник цифрової компетентності, безпеки життєдіяльності та безпеки цифрового освітнього середовища; наголошується на інтеграції технологічних, поведінкових, етичних і організаційних компонентів у професійну підготовку (Самойленко та ін., 2025; Курепін та ін., 2025). Узагальнення цих праць створює підґрунтя для систематизації тенденцій і побудови моделі формування кібербезпекової компетентності здобувачів професійної освіти.

Виділення невирішеної частини проблеми. Попри зростання кількості досліджень, у педагогічній практиці зберігається розрив між трьома рівнями: загальною цифровою безпекою користувача, спеціалізованими компетентностями кіберфахівця та кібербезпечною поведінкою працівника конкретної професії. Навчальні програми нерідко обмежуються правилами паролів, фішингу й захисту персональних даних або, навпаки, пропонують технічно складні модулі, слабо пов'язані з майбутньою професією. Недостатньо опрацьовано логіку, за якою базова кібергігієна переходить у контекстні професійні дії, а оцінювання підтверджує реальну готовність здобувача діяти в умовах ризику.

Мета статті. Визначити та систематизувати сучасні тенденції формування компетентностей з кібербезпеки у закладах професійної освіти та на їх основі обґрунтувати компетентнісно-практичну модель інтеграції кібербезпеки в освітні програми, виробниче навчання й оцінювання результатів.

Наукова новизна. Запропоновано розглядати компетентність з кібербезпеки здобувача професійної освіти як інтегровану здатність розпізнавати цифрові ризики, обирати та виконувати безпечні дії у типових і нестандартних професійних ситуаціях, комунікувати про інцидент та підтримувати власну компетентність відповідно до змін технологій і загроз. Систематизовано вісім тенденцій її формування та розроблено шестикомпонентну структуру, яка поєднує загальну кібергігієну з професійно-контекстними й організаційними діями.

Практичне значення. Результати можуть бути використані закладами професійної освіти під час оновлення освітніх програм, модулів цифрової компетентності, планів виробничого навчання, завдань для практики, міжпредметних проєктів та внутрішніх політик цифрової безпеки. Запропоновані критерії також можуть бути основою для створення чек-листів, симуляційних завдань, портфоліо доказів і партнерських модулів із роботодавцями.

Методологія

Методи дослідження. Дослідження має теоретико-аналітичний характер. Використано інтегративний огляд наукової літератури, порівняльний аналіз рамок компетентностей, категоріальний аналіз педагогічних практик, структурно-функціональне моделювання та узагальнення. Логіка аналізу спрямовувалася від

визначення того, що саме має вміти здобувач, до способів формування й доказового оцінювання цієї спроможності.

Джерела даних. До аналітичного корпусу включено міжнародні рамки DigComp 2.2, NICE Workforce Framework for Cybersecurity, NICE Framework Competency Areas і European Cybersecurity Skills Framework; чинні нормативні акти України у сфері професійної освіти та кібербезпеки; рецензовані дослідження 2021–2026 років щодо кібербезпекової компетентності, cyber range, Capture the Flag, гейміфікації, кіберобізнаності та практико-орієнтованого навчання. Окремо враховано сучасні публікації авторів, пов'язані з кібергігієною й кібербезпекою цифрового освітнього середовища.

Інструменти аналізу. Для порівняння джерел використовувалася аналітична матриця з такими категоріями: одиниця компетентності; зв'язок із професійною роллю; тип навчальної діяльності; рівень реалістичності середовища; характер оцінюваного результату; поведінковий компонент; роль роботодавця; механізм оновлення змісту. На основі повторюваних патернів виокремлено тенденції й сформовано модель.

Обмеження дослідження. Робота не є систематичним оглядом за протоколом PRISMA і не претендує на статистичне узагальнення ефектів окремих методик. Вона має концептуально-аналітичний характер. Запропонована модель потребує подальшої емпіричної апробації в різних професійних профілях, оскільки зміст кіберризиків суттєво відрізняється для ІТ, аграрного виробництва, електротехніки, транспорту, сфери послуг і адміністративної діяльності.

Результати

1. Від знаннєвої моделі до демонстрації спроможності. Першою тенденцією є зміна самої одиниці проектування навчання. Традиційний курс часто структурується за темами: види загроз, паролі, антивірусний захист, шифрування, резервне копіювання. Компетентнісна логіка ставить інше запитання: яку дію здобувач має виконати в реальній ситуації та за якими ознаками можна переконалися, що він виконав її безпечно. NICE Framework формалізує цей підхід через Task, Knowledge and Skill statements. Для професійної освіти такий перехід особливо продуктивний, бо освітній результат можна безпосередньо пов'язати з робочими процедурами.

Наприклад, формулювання «знати ознаки фішингу» є недостатнім кінцевим результатом. Спостережувана компетентність передбачає, що здобувач аналізує повідомлення, виявляє ознаки маніпуляції, не відкриває потенційно небезпечне вкладення, перевіряє каналом зворотного зв'язку легітимність запиту та повідомляє про інцидент відповідно до встановленої процедури. Саме послідовність дій дає змогу оцінити безпечну поведінку. Аналогічно «знати правила резервного копіювання» трансформується у здатність налаштувати або виконати копіювання, перевірити відновлюваність даних і дотриматися правил зберігання.

2. Рольове та професійно-контекстне структурування. Другою тенденцією є відхід від універсального набору однакових технічних тем для всіх. ECSF і NICE демонструють рольовий підхід: компетентності визначаються через завдання, відповідальність і контекст діяльності. Для закладів професійної освіти це означає, що базові правила цифрової безпеки мають доповнюватися ризиками конкретної професії. Електромонтер, оператор верстатів із ЧПК, кухар, обліковець, аграрний технік і фахівець з логістики працюють із різними системами, даними та наслідками порушень.

Професійний контекст визначає пріоритети. Для виробничих професій критичними є безпечне використання промислових мереж, зовнішніх носіїв, віддаленого доступу й налаштувань обладнання; для сфери послуг — захист персональних і платіжних даних; для аграрних спеціальностей — безпечна робота з телеметрією, GPS, хмарними платформами та цифровим управлінням технікою; для адміністративних професій — документообіг, електронний підпис, контроль доступу й соціальна інженерія. Кібербезпека стає частиною професійної технології.

3. Інтеграція кібергігієни як наскрізного результату. Третя тенденція полягає в тому, що базова кібергігієна більше не може бути одноразовою темою на початку курсу інформатики. Вона має регулярно відтворюватися у різних дисциплінах і під час виробничого навчання. DigComp 2.2 акцентує безпеку пристроїв, даних, приватності та добробуту; українські дослідження додатково підкреслюють зв'язок кібергігієни з цифровою культурою безпеки та безпекою життєдіяльності (Самойленко та ін., 2025; Курепін та ін., 2025).

Наскрізність означає, що парольна гігієна, багатофакторна автентифікація, оновлення, перевірка джерел, безпечне використання Wi-Fi, контроль дозволів, захист цифрової ідентичності, правила роботи з персональними даними та резервування мають застосовуватися в реальних навчальних операціях. Якщо здобувач створює хмарний документ, працює в LMS, підключає обладнання, користується корпоративною поштою або передає файл роботодавцю, викладач одночасно оцінює коректність професійної дії та її безпечність.

4. Сценарне, проблемне та проєктне навчання. Четверта тенденція — зміщення від пояснення правил до розв'язання проблем. У кібербезпеці ситуація часто є неповною, неоднозначною та часово обмеженою. Здобувачеві потрібно не пригадати правильну відповідь, а інтерпретувати ознаки, оцінити ризик і вибрати дію. Тому кейси, проблемні ситуації, рольові сценарії та міжпредметні проєкти природно відповідають самій структурі професійної компетентності.

У закладі професійної освіти сценарій може моделювати компрометацію облікового запису майстра, підозрілу активність на спільному комп'ютері, втрату смартфона з робочими даними, зараження зовнішнього носія, помилково надісланий документ із персональними даними, підміну рахунку, несанкціоновану зміну параметрів мережевого обладнання. Педагогічна цінність сценарію полягає не в драматизації загрози, а в тому, що він змушує здобувача поєднати технічні, комунікаційні та процедурні дії.

5. Cyber range, симуляції та Capture the Flag. П'ята тенденція — зростання ролі контрольованих середовищ, у яких можна без ризику виконувати дії, неприйнятні в реальній мережі. Cyber range дає змогу створювати віртуальні мережі, сервери, робочі станції й сценарії атаки/захисту; CTF забезпечує задачний формат із чіткою метою й зворотним зв'язком. Дослідження демонструють, що такі формати можуть посилювати мотивацію, впевненість і практичне застосування знань (Švábenský et al., 2021; Lazarov et al., 2026).

Для професійної освіти важливо уникати прямого копіювання університетських CTF, орієнтованих на майбутніх пентестерів. Значна частина здобувачів не потребуватиме експлуатації вразливостей як професійної функції. Їм потрібні сценарії користувацького й операційного рівня: розпізнати підозрілий процес, локалізувати робочу станцію, правильно повідомити про інцидент, відновити файл із резервної копії, перевірити налаштування доступу, виявити небезпечний пристрій або пояснити, чому певна операція порушує політику безпеки. Отже, cyber range має бути адаптований до професійної ролі.

6. Гейміфікація й адаптивне мікронавчання. Шоста тенденція — використання ігрових механік, коротких повторюваних вправ і персоналізованої складності. Огляди сучасної кіберосвіти показують, що гейміфікація може збільшувати залученість і створювати додатковий стимул до практики, але сама по собі не гарантує глибокого навчання (Weitl-Harms et al., 2023; Kim et al., 2025; Weeratunge et al., 2026). Тому бали, рівні, рейтинги й нагороди мають бути вторинними щодо змісту.

У професійній освіті ефективними можуть бути щотижневі п'ятихвилинні мікросценарії: вибір безпечної дії, розпізнавання фішингової ознаки, перевірка дозволів застосунку, визначення правильного каналу повідомлення. Перевага мікронавчання —

регулярність і можливість швидко оновлювати матеріал відповідно до нових загроз. Адаптивність дозволяє змінювати складність: здобувач, який упевнено виконує базові завдання, переходить до комбінованих сценаріїв; той, хто помиляється, отримує пояснення й повторну практику.

7. Автентичне оцінювання і доказовість. Сьома тенденція — перехід від тесту як головного інструменту до оцінювання виконання. Тест корисний для перевірки термінології та базових принципів, але не показує, чи здобувач діятиме правильно в реальній ситуації. NICE Framework Competency Areas підкреслює необхідність пов'язувати компетентність із виконанням релевантних завдань. Тому у професійній освіті доцільні практичні демонстрації, сценарні іспити, цифрове портфоліо, журнали спостереження, взаємооцінювання та захист рішень.

Оцінювання має охоплювати щонайменше чотири аспекти: точність технічної дії; обґрунтованість оцінки ризику; дотримання процедури й комунікації; здатність пояснити наслідки. Здобувач може технічно «виправити» ситуацію, але порушити правила збереження доказів або приховати інцидент — така поведінка не є компетентною. Саме тому професійна кібербезпека потребує інтегрованих рубрик, де технічний результат оцінюється разом із відповідальністю.

8. Партнерство з роботодавцями та безперервне оновлення. Восьма тенденція визначається швидкістю зміни технологій і загроз. Жодна статична програма не може залишатися актуальною протягом тривалого циклу без перегляду. Роботодавці мають інформацію про типові інциденти, корпоративні процедури, обладнання та вимоги до працівника; заклад освіти — педагогічну спроможність перетворити ці вимоги на навчальні результати й безпечні сценарії. Тому партнерство повинно включати не лише місця практики, а спільне оновлення компетентнісних профілів.

Механізм оновлення може передбачати щорічний аудит ризиків професійного профілю, експертне обговорення з підприємствами, аналіз актуальних рекомендацій ENISA/NIST, перегляд сценаріїв, короткі модулі під нові технології та регулярне підвищення кваліфікації педагогів. У такій моделі кібербезпека стає «живим» компонентом професійної освіти, а не завершеним набором правил.

Таблиця 1. Провідні тенденції формування компетентностей з кібербезпеки у професійній освіті

Тенденція	Педагогічний зсув	Типова практика	Очікуваний результат
Від знань до спроможності	Тема → професійне завдання	Сценарій, практична операція	Безпечне виконання дії
Рольова контекстуалізація	Однаковий зміст → ризику професії	Галузеві кейси	Релевантність робочому місцю
Наскрізна кібергігієна	Разовий урок → повторювана практика	Інтеграція в дисципліни	Стійкі безпечні звички
Активне навчання	Пояснення → розв'язання проблем	PBL, кейси, проекти	Рішення в умовах невизначеності
Cyber range / CTF	Демонстрація → безпечний експеримент	Віртуальні лабораторії	Практичні технічні дії
Гейміфікація й мікронавчання	Епізодичність → регулярна практика	Короткі сценарії, рівні	Залученість і повторення
Автентичне оцінювання	Тест → доказ виконання	Портфоліо, рубрика, симуляція	Верифікована компетентність

Партнерство з роботодавцями	Статична програма → постійне оновлення	Спільні модулі й аудит ризиків	Відповідність ринку праці
-----------------------------	--	--------------------------------	---------------------------

Джерело: авторська розробка на основі узагальнення DigComp 2.2, ECSF, NICE Framework та сучасних досліджень кіберосвіти.

9. Структура компетентності з кібербезпеки здобувача професійної освіти. Синтез розглянутих тенденцій дає підстави запропонувати шестикомпонентну структуру. Перший компонент — базова кібергігієна: автентифікація, оновлення, безпечне підключення, резервування, фішинг, захист пристроїв. Другий — захист даних і цифрової ідентичності: класифікація даних, приватність, дозволи доступу, безпечний обмін і цифровий слід. Третій — безпечне використання професійних цифрових систем: дії в конкретних платформах, обладнанні, мережах і сервісах відповідно до ролі.

Четвертий компонент — управління ризиками та реагування на інциденти: виявлення аномалій, первинна оцінка, мінімізація наслідків, повідомлення, дотримання процедур. П'ятий — правово-етична та організаційна відповідальність: персональні дані, інтелектуальна власність, політики організації, межі дозволених дій, відповідальне використання ШІ. Шостий — командна взаємодія та безперервне навчання: комунікація з керівником і IT/кіберфахівцями, документування інциденту, рефлексія, оновлення знань.

Таблиця 2. Шестикомпонентна структура компетентності з кібербезпеки здобувача професійної освіти

Компонент	Зміст	Приклад дії	Доказ компетентності
Кібергігієна	Автентифікація, оновлення, фішинг, резервування	Увімкнути MFA, перевірити підозріле повідомлення	Правильна послідовність дій у сценарії
Дані та ідентичність	Приватність, доступ, передавання, цифровий слід	Надати мінімально необхідні права	Налаштований доступ + пояснення
Професійні системи	Безпечна робота з галузевими платформами й обладнанням	Підключити/використати систему без порушення політики	Практична демонстрація
Ризики та інциденти	Виявлення, локалізація, повідомлення, відновлення	Ізолювати підозрілий пристрій і повідомити відповідальну особу	Сценарний іспит
Право й етика	Політики, персональні дані, авторські права, AI-етика	Відмовитися від неправомірної операції й пояснити причину	Кейс із аргументацією
Команда й самонавчання	Комунікація, документування, оновлення знань	Скласти короткий звіт про інцидент і план профілактики	Портфоліо / рефлексивний звіт

Джерело: авторська розробка.

10. Рівні формування та принцип прогресії. Запропоновану структуру доцільно реалізовувати не як одночасне опанування всього набору, а як прогресію. На базовому рівні здобувач виконує безпечні дії за чіткою інструкцією; на функціональному —

самостійно застосовує правила у типових професійних ситуаціях; на адаптивному — переносить їх у нову ситуацію, оцінює ризик і пояснює вибір; на командно-професійному — координує дії, документує інцидент і взаємодіє з відповідальними особами. Така прогресія краще відповідає сутності кваліфікації, ніж просте накопичення тем.

Важливим принципом є спіральність. Ключові теми повертаються на різних етапах із підвищенням складності. Фішинг спочатку вивчається як розпізнавання ознак, потім як частина корпоративної комунікації, далі — як сценарій компрометації облікового запису з необхідністю реагування. Робота з даними переходить від персональної приватності до професійної класифікації, обмеження доступу та відповідальності за витік. Таким чином формується не пам'ять про правило, а стійка модель поведінки.

11. Інтеграція в освітню програму. Зміст кібербезпеки доцільно розмішувати на трьох рівнях. Перший — загальноінституційний: єдині правила облікових записів, пристроїв, пошти, LMS, хмарних сервісів, персональних даних і повідомлення про інциденти. Другий — міжпредметний: викладачі загальнопрофесійних дисциплін використовують спільні принципи й термінологію. Третій — професійно-спеціалізований: викладачі та майстри виробничого навчання інтегрують специфічні ризики у технологічні операції.

У цьому підході не кожен педагог має бути кіберфахівцем, але кожен має розуміти безпечні цифрові практики своєї дисципліни. Заклад освіти, своєю чергою, повинен забезпечити методичну підтримку, набір сценаріїв, мінімальні технічні стандарти та механізм оновлення. Для складніших модулів доцільне залучення партнерів — ІТ-фахівців, фахівців підприємств, представників центрів кіберзахисту або сертифікованих тренерів.

12. Педагогічні умови ефективності. Перша умова — реалістичність без небезпеки: навчальна ситуація має бути схожою на робочу, але не створювати ризику для реальних систем і даних. Друга — диференціація складності: здобувачі входять у професійну освіту з неоднаковою цифровою підготовкою, тому надто складний сценарій формує фрустрацію, а надто простий — ілюзію компетентності. Третя — швидкий зворотний зв'язок, що пояснює не лише правильну відповідь, а причинно-наслідковий зв'язок між дією і ризиком.

Четверта умова — право на навчальну помилку. Кібербезпека часто викладається через залякування наслідками, що може підсилювати пасивність. Контрольована симуляція дозволяє помилятися, аналізувати наслідки й повторювати дію. П'ята — рефлексія: після практики здобувач пояснює, які ознаки він помітив, яке рішення прийняв, чому воно було безпечним і що змінив би за інших умов. Саме рефлексія перетворює одиничну вправу на переносиму компетентність.

13. Оцінювання готовності до безпечної професійної діяльності. Для кожної компетентності необхідно визначати критерій успіху, тип доказу та рівень самостійності. Мінімальний рівень — правильна дія за інструкцією; достатній — самостійне виконання типового завдання; високий — правильна реакція на комбінований сценарій із поясненням ризику й комунікацією. Підсумкове оцінювання доцільно будувати як короткий практичний сценарій, а не як великий тест із термінології.

Таблиця 3. Орієнтовна матриця автентичного оцінювання компетентностей з кібербезпеки

Рівень	Характер завдання	Ступінь самостійності	Тип доказу
Базовий	Окрема типова дія	За алгоритмом/підказкою	Чек-лист, коротка демонстрація
Функціональний	Типова професійна	Самостійно	Практичне завдання +

	ситуація		пояснення
Адаптивний	Нова або комбінована ситуація	Самостійно з вибором стратегії	Сценарний іспит, журнал дій
Командно-професійний	Інцидент із кількома учасниками	Розподіл ролей і комунікація	Командна симуляція, звіт, дебрифінг

Джерело: авторська розробка.

Обговорення

Інтерпретація результатів. Проведений аналіз дозволяє трактувати сучасне формування компетентностей з кібербезпеки як перехід від дисциплінарної моделі до моделі професійної кіберстійкості. Її центральною одиницею є не тема і не окрема технологія, а здатність здобувача діяти безпечно в межах своєї професійної ролі. Такий підхід узгоджується з логікою NICE, де завдання, знання й навички утворюють функціональну структуру діяльності, та з ECSF, який пов'язує компетентності з ролями й відповідальністю.

Водночас для професійної освіти пряме перенесення рамок кіберпрофесіоналів є недоцільним. Більшість випускників не працюватиме аналітиками SOC або пентестерами, але всі працюватимуть у цифровізованому середовищі. Тому базова модель повинна мати два шари: універсальний — кібергігієна, дані, ідентичність, соціальна інженерія, інциденти; контекстний — безпечні дії в конкретній професійній системі. Така двошаровість дозволяє уникнути і надмірної спрощеності, і зайвої технічної спеціалізації.

Порівняння з іншими дослідженнями. Отримані результати узгоджуються з дослідженням Alammar et al. (2022), у якому компетентність з кібербезпеки розглядається як комплекс знань, навичок та здатності застосовувати їх у навчальних і професійних ситуаціях. Вони також відповідають висновкам Švábenský et al. (2021) щодо сильних сторін CTF у технічному навчанні й необхідності ширше охоплювати людський фактор; результатам Lazarov et al. (2026) про користь інтерактивності cyber range та потребу адаптувати складність; а також сучасним оглядам гейміфікації, що підкреслюють її ефективність за умови педагогічно вмотивованого дизайну.

Важливе уточнення стосується балансу технічних і нетехнічних компетентностей. Дослідження потреб роботодавців показують, що організаційна та людська безпека можуть оцінюватися не менш високо, ніж суто технічні домени. Для професійної освіти це принципово: працівник повинен уміти не лише «не натиснути» на підозріле посилання, а повідомити, зафіксувати, взаємодіяти з колегами, дотриматися регламенту й не створити додаткового ризику. Тому комунікація, відповідальність і культура повідомлення мають бути частиною оцінювання.

Наукова новизна (розгорнуто). По-перше, систематизовано вісім тенденцій у єдиній логіці трансформації: від змісту до діяльності, від універсальності до професійного контексту, від окремого курсу до наскрізної інтеграції, від тесту до доказу виконання, від статичної програми до постійного оновлення. По-друге, запропоновано шестикомпонентну модель, у якій технічні, поведінкові, правові та комунікаційні елементи не існують окремо, а формують єдину готовність до безпечної професійної діяльності.

По-третє, обґрунтовано принцип прогресії компетентності від дії за інструкцією до самостійного й командного реагування на нову ситуацію. По-четверте, введено поняття доказовості компетентності: освітній результат має підтверджуватися не декларацією «здобувач знає», а спостережуваною дією, цифровим артефактом, журналом виконання, сценарним завданням або аргументованим рішенням. Це зближує педагогічне оцінювання з реальними очікуваннями робочого середовища.

Практичне значення (розгорнуто). На рівні освітньої програми заклад може провести карту ризиків кожної професії та визначити мінімальний набір універсальних і контекстних результатів. На рівні дисципліни викладач може переформулювати теми у практичні дії та інтегрувати короткі сценарії. На рівні виробничого навчання майстер може оцінювати цифрову безпеку як частину правильності технологічної операції. На рівні закладу єдина політика інцидентів створює автентичне середовище: здобувачі вчаться користуватися реальними каналами повідомлення та правилами доступу.

Для роботодавців модель створює зрозумілу основу для партнерства: підприємство може описати типові ризики й очікувані безпечні дії без розкриття конфіденційної інформації, а заклад перетворює їх на навчальні сценарії. Для педагогів необхідні короткі програми підвищення кваліфікації, що поєднують власну кібергігієну, методику сценарного навчання, безпечну організацію лабораторій і оцінювання. Для здобувачів корисним може бути цифрове портфоліо, яке фіксує результати практичних завдань, мікросертифікати та рефлексивні звіти.

Висновки

1. Сучасна професійна освіта потребує переходу від епізодичного вивчення правил інформаційної безпеки до системного формування кіберстійкої професійної поведінки. Кібербезпекова компетентність має проявлятися у здатності розпізнавати ризик, виконувати безпечну дію, реагувати на інцидент і взаємодіяти з іншими учасниками професійного середовища.

2. Визначено вісім провідних тенденцій: перехід від знань до демонстрації спроможності; рольова й професійна контекстуалізація; наскрізна кібергігієна; сценарне, проблемне й проектне навчання; використання cyber range, CTF та симуляцій; гейміфікація й мікронавчання; автентичне оцінювання; партнерство з роботодавцями та безперервне оновлення змісту.

3. Запропонована шестикомпонентна структура охоплює кібергігієну, захист даних і цифрової ідентичності, безпечне використання професійних цифрових систем, управління ризиками та реагування, правово-етичну відповідальність, командну взаємодію й самонавчання. Вона може бути адаптована до різних професій через зміну контексту, сценаріїв і критеріїв.

4. Ефективне формування компетентностей потребує практики в контрольованих середовищах, права на навчальну помилку, диференціації складності та рефлексії. Технології cyber range і CTF є перспективними, якщо їх завдання відповідають реальній професійній ролі, а не лише спеціалізованій підготовці кіберфахівців.

5. Оцінювання доцільно будувати на доказах виконання: практичній демонстрації, сценарному іспиті, портфоліо, журналах дій, аргументованому рішенні та командній симуляції. Перспективою подальших досліджень є емпірична апробація моделі у закладах професійної освіти різних профілів та розроблення валідного інструментарію вимірювання рівнів кібербезпекової компетентності.

Декларація щодо використання штучного інтелекту

Під час підготовки робочої версії рукопису використовувався ChatGPT (OpenAI) як допоміжний інструмент для структурування матеріалу, мовного редагування та пошуку напрямів для перевірки джерел. Наукові положення, інтерпретації, добір джерел, остаточні формулювання та відповідальність за зміст мають бути перевірені й затверджені авторами перед поданням рукопису до редакції.

Список використаних джерел

1. Самойленко О. О., Бацуровська І. В., Курепін В. М. Кібергігієна та безпека життєдіяльності як ключові елементи цифрової компетентності здобувачів освіти. Національні інтереси України. 2025. № 11(16). С. 461–477. DOI: 10.52058/3041-1793-2025-11(16)-461-476.

2. Курепін В. М., Самойленко О. О., Бацуровська І. В. Кібербезпека цифрового освітнього середовища як складова системи безпеки праці та життєдіяльності. Суспільство та національні інтереси. 2025. № 11(19). С. 255–268. DOI: 10.52058/3041-1572-2025-11(19)-255-267.
3. Про професійну освіту : Закон України від 21.08.2025 № 4574-IX. База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/go/4574-20> (дата звернення: 05.10.2026).
4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/go/2163-19> (дата звернення: 05.10.2026).
5. Vuorikari R., Kluzer S., Punie Y. DigComp 2.2: The Digital Competence Framework for Citizens – With new examples of knowledge, skills and attitudes. Luxembourg : Publications Office of the European Union, 2022. DOI: 10.2760/115376.
6. Petersen R., Santos D., Wetzel K., Smith M., Witte G. Workforce Framework for Cybersecurity (NICE Framework). NIST Special Publication 800-181 Rev. 1. Gaithersburg : National Institute of Standards and Technology, 2020. DOI: 10.6028/NIST.SP.800-181r1.
7. Wetzel K. NICE Framework Competency Areas: Preparing a Job-Ready Cybersecurity Workforce. NIST IR 8355. Gaithersburg : National Institute of Standards and Technology, 2023. DOI: 10.6028/NIST.IR.8355.
8. European Union Agency for Cybersecurity (ENISA). European Cybersecurity Skills Framework (ECSF). URL: <https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf> (accessed: 05.10.2026).
9. Alammari A., Sohaib O., Younes S. Developing and evaluating cybersecurity competencies for students in computing programs. PeerJ Computer Science. 2022. Vol. 8. e827. DOI: 10.7717/peerj-cs.827.
10. Švábenský V., Čeleda P., Vykopal J., Brišáková S. Cybersecurity knowledge and skills taught in capture the flag challenges. Computers & Security. 2021. Vol. 102. Article 102154. DOI: 10.1016/j.cose.2020.102154.
11. Lazarov W., Schafeitel-Tähtinen T., Squillace J., Martinasek Z., Coufalikova A., Helenius M., Gallus P., Fujdiak R. Lessons Learned from Using Cyber Range to Teach Cybersecurity at Different Levels of Education. Technology, Knowledge and Learning. 2026. Vol. 31. P. 1683–1718. DOI: 10.1007/s10758-025-09840-y.
12. Weitzl-Harms S., Spanier A., Hastings J., Rokusek M. Framing Gamification in Undergraduate Cybersecurity Education. Journal of The Colloquium for Information Systems Security Education. 2023. Vol. 10, No. 1. Article 7. DOI: 10.53735/cisse.v10i1.161.
13. Kim J. B., Zhong C., Liu H. The Impact of Gamification on Cybersecurity Learning: Multi-Study Analysis. Communications of the Association for Information Systems. 2025. Vol. 56. P. 57–96. DOI: 10.17705/1CAIS.05603.
14. van Steen T., Deeleman J. R. A. Successful Gamification of Cybersecurity Training. Cyberpsychology, Behavior, and Social Networking. 2021. Vol. 24, No. 9. DOI: 10.1089/cyber.2020.0526.
15. Amzeyeva A. A., Zhumabayeva A. E. Cybersecurity Awareness Among Students: A Systematic Literature Review and PRISMA-Based Analysis. Gumilyov Journal of Pedagogy. 2025. Vol. 152, No. 3. P. 126–144. DOI: 10.32523/3080-1710-2025-152-3-126-144.
16. Razack A. K. A., Mat Saad M. F. Enhancing Cybersecurity Awareness through Gamification: Design an Interactive Cybersecurity Learning Platform for Multimedia University Students. Journal of Informatics and Web Engineering. 2024. Vol. 3, No. 3. DOI: 10.33093/jiwe.2024.3.3.2.
17. Arduin P.-E., Costé B. Learning to Hack, Playing to Learn: Gamification in Cybersecurity Courses. Journal of Cybersecurity and Privacy. 2026. Vol. 6, No. 1. Article 16. DOI: 10.3390/jcp6010016.

18. Peter O., Pradhan A., Mbohwa C. A Gamification Approach to Teaching Cybersecurity in CPS. *Procedia CIRP*. 2024. Vol. 128. P. 799–803. DOI: 10.1016/j.procir.2024.06.039.
19. Weeratunge N. H., Hjelsvold R., Katt B. A systematic scoping review on game-based cybersecurity awareness education. *International Journal of Information Security*. 2026. Vol. 25. Article 71. DOI: 10.1007/s10207-026-01239-9.
20. Weijsenfeld F. G. J., Sarmah D. K. Gamifying cybersecurity: A narrative-driven approach to teaching steganography. *Computers & Education Open*. 2025. Vol. 9. Article 100288. DOI: 10.1016/j.caeo.2025.100288.
21. Quayyum F., Cruzes D. S., Jaccheri L. Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*. 2021. Vol. 30. Article 100343. DOI: 10.1016/j.ijcci.2021.100343.

References

1. Samoilenko, O. O., Batsurovska, I. V., & Kurepin, V. M. (2025). Kiberhihiiena ta bezpeka zhyttiediialnosti yak kliuchovi elementy tsyfrovoy kompetentnosti здобувачів освіти [Cyber hygiene and life safety as key elements of students' digital competence]. *Natsionalni interesy Ukrainy*, 11(16), 461–477. [https://doi.org/10.52058/3041-1793-2025-11\(16\)-461-476](https://doi.org/10.52058/3041-1793-2025-11(16)-461-476)
2. Kurepin, V. M., Samoilenko, O. O., & Batsurovska, I. V. (2025). Kiberbezpeka tsyfrovoho osvitnoho seredovyshcha yak skladova systemy bezpeky pratsi ta zhyttiediialnosti [Cybersecurity of the digital educational environment as a component of occupational and life safety]. *Suspilstvo ta natsionalni interesy*, 11(19), 255–268. [https://doi.org/10.52058/3041-1572-2025-11\(19\)-255-267](https://doi.org/10.52058/3041-1572-2025-11(19)-255-267)
3. Verkhovna Rada of Ukraine. (2025). Pro profesiinu osvitu [On vocational education], Law No. 4574-IX. <https://zakon.rada.gov.ua/go/4574-20>
4. Verkhovna Rada of Ukraine. (2017). Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On the basic principles of cybersecurity of Ukraine], Law No. 2163-VIII. <https://zakon.rada.gov.ua/go/2163-19>
5. Vuorikari, R., Kluzer, S., & Punie, Y. (2022). DigComp 2.2: The Digital Competence Framework for Citizens – With new examples of knowledge, skills and attitudes. Publications Office of the European Union. <https://doi.org/10.2760/115376>
6. Petersen, R., Santos, D., Wetzel, K., Smith, M., & Witte, G. (2020). Workforce Framework for Cybersecurity (NICE Framework) (NIST SP 800-181 Rev. 1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-181r1>
7. Wetzel, K. (2023). NICE Framework Competency Areas: Preparing a Job-Ready Cybersecurity Workforce (NIST IR 8355). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8355>
8. European Union Agency for Cybersecurity. (2026). European Cybersecurity Skills Framework (ECSF). <https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf>
9. Alammari, A., Sohaib, O., & Younes, S. (2022). Developing and evaluating cybersecurity competencies for students in computing programs. *PeerJ Computer Science*, 8, e827. <https://doi.org/10.7717/peerj-cs.827>
10. Švábenský, V., Čeleda, P., Vykopal, J., & Brišáková, S. (2021). Cybersecurity knowledge and skills taught in capture the flag challenges. *Computers & Security*, 102, 102154. <https://doi.org/10.1016/j.cose.2020.102154>
11. Lazarov, W., Schafeitel-Tähtinen, T., Squillace, J., Martinasek, Z., Coufalikova, A., Helenius, M., Gallus, P., & Fujdiak, R. (2026). Lessons learned from using cyber range to teach cybersecurity at different levels of education. *Technology, Knowledge and Learning*, 31, 1683–1718. <https://doi.org/10.1007/s10758-025-09840-y>

12. Weitzl-Harms, S., Spanier, A., Hastings, J., & Rokusek, M. (2023). Framing gamification in undergraduate cybersecurity education. *Journal of The Colloquium for Information Systems Security Education*, 10(1), 7. <https://doi.org/10.53735/cisse.v10i1.161>
13. Kim, J. B., Zhong, C., & Liu, H. (2025). The impact of gamification on cybersecurity learning: Multi-study analysis. *Communications of the Association for Information Systems*, 56, 57–96. <https://doi.org/10.17705/1CAIS.05603>
14. van Steen, T., & Deeleman, J. R. A. (2021). Successful gamification of cybersecurity training. *Cyberpsychology, Behavior, and Social Networking*, 24(9). <https://doi.org/10.1089/cyber.2020.0526>
15. Amzeyeva, A. A., & Zhumabayeva, A. E. (2025). Cybersecurity awareness among students: A systematic literature review and PRISMA-based analysis. *Gumilyov Journal of Pedagogy*, 152(3), 126–144. <https://doi.org/10.32523/3080-1710-2025-152-3-126-144>
16. Razack, A. K. A., & Mat Saad, M. F. (2024). Enhancing cybersecurity awareness through gamification: Design an interactive cybersecurity learning platform for Multimedia University students. *Journal of Informatics and Web Engineering*, 3(3). <https://doi.org/10.33093/jiwe.2024.3.3.2>
17. Arduin, P.-E., & Costé, B. (2026). Learning to hack, playing to learn: Gamification in cybersecurity courses. *Journal of Cybersecurity and Privacy*, 6(1), 16. <https://doi.org/10.3390/jcp6010016>
18. Peter, O., Pradhan, A., & Mbohwa, C. (2024). A gamification approach to teaching cybersecurity in CPS. *Procedia CIRP*, 128, 799–803. <https://doi.org/10.1016/j.procir.2024.06.039>
19. Weeratunge, N. H., Hjelsvold, R., & Katt, B. (2026). A systematic scoping review on game-based cybersecurity awareness education. *International Journal of Information Security*, 25, 71. <https://doi.org/10.1007/s10207-026-01239-9>
20. Weijssenfeld, F. G. J., & Sarmah, D. K. (2025). Gamifying cybersecurity: A narrative-driven approach to teaching steganography. *Computers & Education Open*, 9, 100288. <https://doi.org/10.1016/j.caeo.2025.100288>
21. Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, 30, 100343. <https://doi.org/10.1016/j.ijcci.2021.100343>