ШИФР: «DIIA.OSVITA»

Всеукраїнський конкурс наукових робіт зі спеціальності
«Професійна освіта»

КОНКУРСНА НАУКОВО-ДОСЛІДНА РОБОТА

на тему:

«ВИКОРИСТАННЯ ПЛАТФОРМИ «ДІЯ.ОСВІТА» ЗАДЛЯ ФОРМУВАННЯ КОМПЕТЕНТНОСТЕЙ З ЦИФРОВОЇ БЕЗПЕКИ У МАЙБУТНІХ ФАХІВЦІВ З ПРОФЕСІЙНОЇ ОСВІТИ»

2026

ЗМІСТ

ВСТУП

Актуальність дослідження. Стрімка цифровізація українського суспільства, посилена повномасштабним вторгненням росії та прискореним переходом освіти в онлайн-формат, зумовила загострення проблеми цифрової безпеки. За даних умов майбутні фахівці з професійної освіти опиняються у подвійній ролі: вони самі є потенційними жертвами кіберзагроз і водночас покликані формувати цифрову культуру у своїх здобувачів. Водночас аналіз освітньої нормативної бази свідчить про відсутність системного підходу до формування компетентностей із цифрової безпеки у закладах вищої та фахової передвищої освіти.

За таких обставин пошук ефективних педагогічних засобів розв'язання окресленої проблеми набуває першочергового значення. Особливий науково-практичний інтерес у цьому контексті становить безоплатна державна платформа «Дія.Освіта», створена для розвитку цифрової грамотності громадян України, яка розглядається нами як перспективний освітній ресурс для інтеграції в процес професійної підготовки майбутніх фахівців з професійної освіти та формування у них компетентностей з цифрової безпеки.

Теоретичні засади формування цифрових компетентностей досліджували вітчизняні та зарубіжні науковці: О. Митник, А. Островершенко, Г. Кірякова, Д. Кожухарова, Н. Макаренко, П. Мороз, А. Лукіянчук (психолого-педагогічні умови формування компетентностей); Л. Султанова, М. Прокоф'єва, Т. Уварова, Т. Стас (інтеграція цифрової безпеки в освіту); В. Коваленко, Т. Осипчук (технічні аспекти кіберзахисту); М. Редекер, С. Каретеро, Р. Вуорікарі, Й. Пуні (європейські рамки цифрових компетентностей DigComp). Водночас проблема використання національного платформи «Дія.Освіта» як засобу формування компетентностей з цифрової безпеки у майбутніх фахівців з професійної освіти не отримала належного наукового обґрунтування, що й зумовило вибір теми дослідження.

Мета дослідження – теоретично обґрунтувати та експериментально перевірити психолого-педагогічні умови використання платформи «Дія.Освіта» у формуванні компетентностей з цифрової безпеки у майбутніх фахівців з професійної освіти.

Завдання дослідження:

1. Проаналізувати проблему формування компетентностей з цифрової безпеки у майбутніх фахівців з професійної освіти у науково-педагогічній літературі та нормативно-правових документах.

2. Визначити й обґрунтувати психолого-педагогічні умови впровадження платформи «Дія.Освіта» у процес формування компетентностей з цифрової безпеки.

3. Розробити структурно-функціональну модель та методику використання платформи «Дія.Освіта» для формування компетентностей з цифрової безпеки.

4. Спроєктувати та реалізувати авторський чат-бот «Безпековичок» як цифровий засіб підтримки формування компетентностей з ЦБ.

5. Визначити критерії, показники й рівні сформованості компетентностей з цифрової безпеки та експериментально перевірити ефективність запропонованих психолого-педагогічних умов.

Об’єкт дослідження – формування компетентностей з цифрової безпеки у здобувачів освіти.

Предмет дослідження – використання платформи «Дія.Освіта» задля формування компетентностей з цифрової безпеки у майбутніх фахівців з професійної освіти.

Методи дослідження: теоретичні (аналіз, синтез, узагальнення наукової літератури, моделювання); емпіричні (педагогічний експеримент, тестування, анкетування, спостереження, самооцінка); статистичні (критерій χ^2 Пірсона для підтвердження значущості результатів; критерій Манна-Уітні для перевірки статистичної значущості виявлених змін).

Практичне значення – розроблені методика та чат-бот «Безпековичок» можуть бути впроваджені у навчальний процес закладів вищої та фахової

передвищої освіти за спеціальністю «Професійна освіта» для системного формування компетентностей з цифрової безпеки здобувачів.

Апробація результатів дослідження. Основні положення та результати дослідження обговорювалися на науково-практичних конференціях, зокрема: Міжнародній науково-технічній конференції «Розвиток промисловості та суспільства» (м. Кривий Ріг, 2026 р.); XXIII Міжнародній науково-практичній конференції «ПОЛІТ. Сучасні проблеми науки» (м. Київ, 2023 р.).

Структура роботи. Робота складається зі вступу, трьох розділів, висновків, списку використаної літератури та додатків (А–Г). Загальний обсяг роботи – 30 сторінок основного тексту.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ФОРМУВАННЯ КОМПЕТЕНТНОСТЕЙ З ЦИФРОВОЇ БЕЗПЕКИ У МАЙБУТНІХ ФАХІВЦІВ З ПРОФЕСІЙНОЇ ОСВІТИ ІЗ ВИКОРИСТАННЯМ ПЛАТФОРМИ «ДІЯ.ОСВІТА»

1.1. Проблеми формування компетентностей з цифрової безпеки майбутніх фахівців професійної освіти засобами платформи «Дія.Освіта»

Стрімка цифровізація, посилена пандемією COVID-19 та повномасштабною війною в Україні, суттєво змінила життя молоді: навчання, робота й дозвілля перейшли в онлайн. Для професійної освіти це стало серйозним викликом, адже практична підготовка вимагала швидкої адаптації до дистанційного формату, що розширило цифровий слід студентів. Водночас зросли кібератаки, витоки даних і маніпулятивний вплив, що особливо загрожує молоді з недостатнім рівнем цифрової грамотності. У таких умовах формування компетентностей із цифрової безпеки (ЦБ) є необхідною складовою професійної підготовки.

Аналіз законів України «Про освіту» [43], «Про фахову передвищу освіту» [45] та «Про вищу освіту» [42] показує, що питання ЦБ не має чіткого нормативного закріплення. Водночас воно опосередковано реалізується через компетентнісний підхід, цифровізацію освіти та орієнтацію на потреби інформаційного суспільства. Це свідчить про те, що розвиток ЦБ відбувається переважно на рівні освітніх стандартів і практик, а не законодавства, що підкреслює потребу подальших досліджень.

У сучасному науковому дискурсі важливим є чітке розмежування понять, пов’язаних із безпекою в цифровому середовищі. Зокрема, інформаційна безпека охоплює захист інформації в будь-яких формах із забезпеченням її конфіденційності, цілісності та доступності [9]. Кібербезпека є більш вузьким поняттям і стосується захисту цифрових систем, мереж і програм від кіберзагроз [44]. Водночас цифрова безпека акцентує увагу на безпечній і

відповідальній поведінці користувача в цифровому просторі, включаючи питання приватності, управління даними та розпізнавання ризиків [6].

Для ілюстрації актуальності цих понять у суспільстві та освітньому середовищі України доцільно звернутися до даних Google Trends за останні 5 років (рис. 1.1).

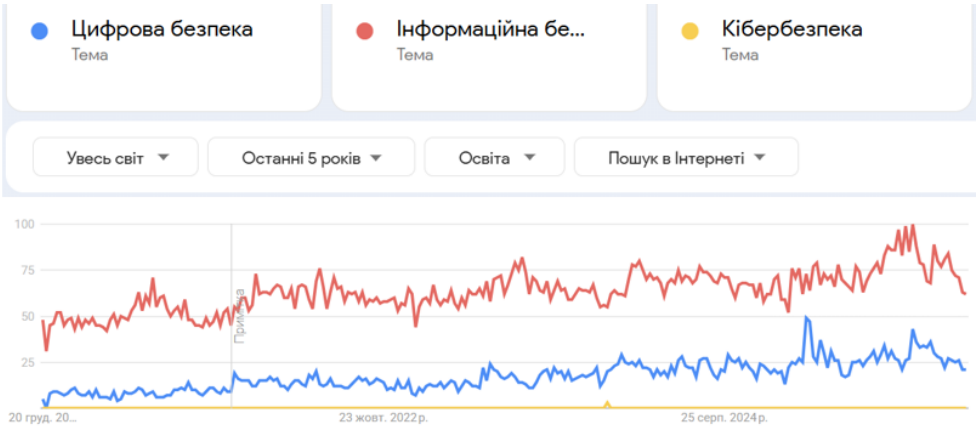


Рис. 1.1 Інтерес до понять, пов'язаних із безпекою в цифровому середовищі

У межах нашого дослідження основну увагу приділено саме поняттю «цифрова безпека» та проаналізовано його визначення у різних науковців (табл. 1.1).

Таблиця 1.1

Визначення терміну «цифрова безпека» в освітньому контексті

Автор(и)	Визначення
Н. Босько, Л. Бела [32]	ЦБ – здатність безпечно працювати з інформацією та даними, використовувати цифрові сервіси й інструменти з обережністю
О. Шикиринська, В. Ляпунова, О. Мельникова [25]	ЦБ – інтегрована здатність усвідомлювати ризики цифрового середовища, захищати персональні дані й відповідально взаємодіяти онлайн
М. Делембовський, В. Ткаченко, Д. Мельник [31; 33]	ЦБ – знання і навички захисту цифрових систем, ресурсів і користувачів від цифрових загроз
Ю. Руденко [47]	ЦБ – сформованість умінь і поведінкових моделей для розпізнавання загроз, захисту даних і безпечної взаємодії з ІКТ
Д. Ушшер-Ік [27]	ЦБ – здатність не лише знати про кіберзагрози, а й демонструвати стійку безпечну поведінку в цифровому середовищі

Цифрову безпеку в нашому дослідженні визначаємо як процес і результат забезпечення безпечної та відповідальної взаємодії учасників освітнього процесу

з цифровим середовищем, що передбачає захист даних, дотримання принципів конфіденційності, цілісності й доступності, а також формування навичок безпечної поведінки.

Таке трактування узгоджується з науковими підходами, які розглядають ЦБ як результат цілеспрямованої підготовки, що поєднує знання і практичні вміння та здатність адаптуватися до нових цифрових загроз. Водночас її визначають як складову цифрових компетентностей, що охоплює основи кіберзахисту, безпечне використання цифрових ресурсів і усвідомлення ризиків [2; 5].

Міжнародний досвід (США, країни ЄС, Естонія, Сінгапур та Швеція) засвідчує, що поширення дистанційного навчання підвищує цифрові ризики [34], тому ефективне забезпечення ЦБ ґрунтується на поєднанні нормативного регулювання, освітніх стратегій і розвитку цифрової грамотності, що обґрунтовує необхідність її інтеграції у підготовку здобувачів освіти (рис. 1.2).

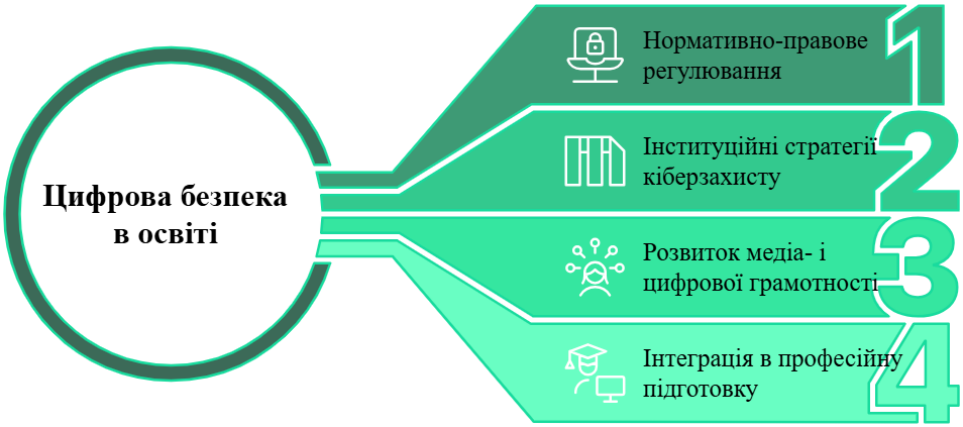


Рис. 1.2 Фундаментальні основи ЦБ в освіті на прикладі міжнародного досвіду

Український досвід інтеграції ЦБ в освіту та аналіз проблем ЦБ у вищих закладах, проведений Л. Султановою та М. Прокоф'євою [48], підкреслює необхідність розвитку цифрової складової через спецкурси з медіаграмотності, фактчекінгу, критичного мислення та міждисциплінарні курси на цифрових платформах. Схожі орієнтири розвитку цифрових компетентностей визначають і Т. Уварова та Т. Стас, наголошуючи, що сучасний студент – «цифрова людина», яка потребує критичного та системного мислення [52].

Аналіз показує, що ЦБ – це не лише захист інформації, а комплексна компетентність, що охоплює знання, навички й відповідальну поведінку в цифровому середовищі. Вона включає цифрову грамотність, критичне мислення та здатність протидіяти загрозам. Її формування потребує поєднання освітніх програм, стратегій закладів і міждисциплінарного підходу, що сприяє безпечній поведінці студентів і зменшенню ризиків цифрових загроз та витоку даних.

У роботі М. Редекера цифрова компетентність трактується як здатність ефективно, критично та безпечно використовувати технології, а ЦБ – як її складова [22]. У DigComp 2.1 ЦБ охоплює захист пристроїв, даних, безпечну взаємодію та добробут користувача [3]. В оновленій DigComp 2.2 уточнено компетентності з урахуванням нових ризиків (платформи, ШІ, цифрова ідентичність), однак модель залишається концептуальною і не визначає педагогічних механізмів [28].

Дослідники В. Коваленко та Т. Осипчук фокусуються на технічному захисті, формуючи базові навички розпізнавання загроз і застосування захисних засобів [37]. Такий підхід важливий, але обмежує розуміння ЦБ лише технічним рівнем і не охоплює соціально-поведінкові ризики.

Формування компетентностей з ЦБ ускладнюється їх міждисциплінарністю та потребою врахування знань, навичок і поведінкових аспектів. На практиці переважає фрагментарне засвоєння знань, тоді як їх застосування й відповідальна поведінка залишаються недостатньо сформованими [22; 15] . Ситуацію ускладнює відсутність цілісного підходу до інтеграції ЦБ в освітні програми та швидкі технологічні зміни, що створюють нові ризики (рис. 1.3).

Опрацювання наукових джерел показує, що формування компетентностей з ЦБ у здобувачів освіти лишається недостатньо систематизованим, хоча ця проблема стає дедалі актуальнішою. У дослідженнях ЦБ здебільшого розглядається як частина загальної цифрової компетентності, без акценту на особливості освітнього процесу в закладах освіти, що призводить до фрагментарності теоретичних і методичних підходів.

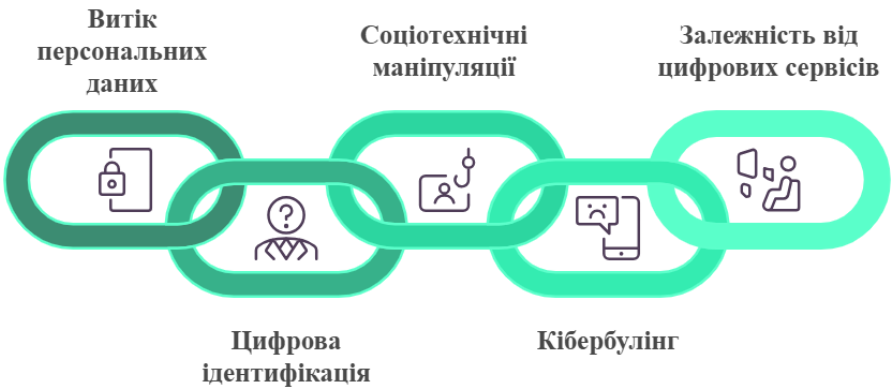


Рис. 1.3 Ризики цифрового освітнього середовища

Загалом ЦБ розглядається як інтегрований результат знань, умінь, навичок і ставлень [37], проте відсутність чіткої структури та критеріїв її сформованості ускладнює системне формування освіти. Виділяється кілька проблем [48], що ускладнюють системне формування компетентностей з ЦБ (рис. 1.4).

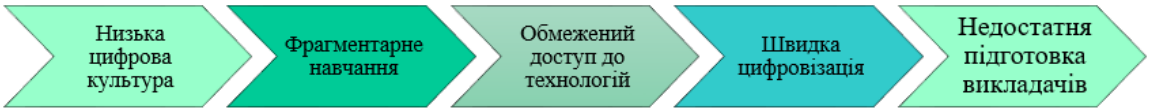


Рис. 1.4 Проблеми формування компетентностей з ЦБ

Отже, формування компетентностей з ЦБ є актуальним, особливо в умовах війни в Україні, що супроводжується зростанням цифрових загроз та інформаційних атак. Аналіз джерел свідчить про фрагментарну інтеграцію ЦБ у навчальні програми та недостатнє охоплення її аспектів. Це зумовлює потребу в системному й методично обґрунтованому підході з урахуванням особливостей професійної освіти та змін цифрового середовища.

1.2 Психолого-педагогічні умови впровадження платформи «Дія.Освіта» у процес формування компетентностей з цифрової безпеки

У цифровізованому освітньому середовищі зростає значення психолого-педагогічних умов, які забезпечують не лише засвоєння знань, а й розвиток відповідального ставлення до цифрових технологій. Вони розглядаються як

комплекс внутрішніх і зовнішніх чинників, що сприяють ефективності навчання, розвитку особистості та формуванню мотивації, когнітивних і діяльнісних компетентностей здобувачів [24].

Вітчизняні й зарубіжні дослідники О. Митник, А. Островершенко, Г. Кірякова, Д. Кожухарова, Ю. Нінг, С. Дансо підкреслюють, що психолого- педагогічні умови включають мотиваційну підтримку, педагогічну готовність, інтерактивне навчальне середовище та індивідуалізацію освітнього процесу [40; 10; 17].

Дослідники Н. Макаренко, П. Мороз, А. Лукіянчук акцентують на ролі внутрішньої мотивації, розвитку рефлексії, саморегуляції та психологічної готовності педагогів до роботи з цифровими технологіями [39; 41; 38].

Психолого-педагогічні умови формування компетентностей з ЦБ визначають не лише зміст, а й методи навчання, впливаючи на мотивацію, усвідомлення ризиків і відповідальну поведінку онлайн. Їх взаємозв'язок відображено у структурно-логічній моделі (рис. 1.5), що демонструє взаємодію складових освітнього середовища та учасників навчання.

Рис. 1.5 Структурно-логічна модель психолого-педагогічних умов формування компетентностей з ЦБ у здобувачів освіти

На схемі показано, що активна мотивація та академічна доброчесність формують основу, тоді як платформа «Дія.Освіта» та чат-бот виступають інтерактивними інструментами реалізації цих принципів.

Перша психолого-педагогічна умова – мотивація здобувачів до розвитку цифрових компетентностей і безпечної поведінки в мережі, що визначає їхню

активність, використання ресурсів і формування безпечних практик [50; 18]. Дослідження доводять, що мотивовані здобувачі ефективніше навчаються, критично оцінюють інформацію та демонструють саморегуляцію.

Теоретичною основою є теорія самодетермінації Е. Десі та Р. Райана, яка пов’язує мотивацію із задоволенням потреб автономії, компетентності та соціальної приналежності [4]. У цифровій освіті це проявляється у здатності самостійно опановувати інструменти та усвідомлювати їхню значущість.

Дослідження підтверджують, що мотивація формує ціннісне ставлення до безпечної поведінки, сприяє критичному мисленню та готовності застосовувати знання на практиці. Вона розвивається через самостійне навчання, постановку цілей і використання інтерактивних ресурсів, зокрема «Дія.Освіта» [30].

Ефективними засобами є проблемно-ситуативний підхід, гейміфікація, індивідуалізація та проєктна діяльність [16], а також підтримка викладача [46]. Тому, мотивація є ключовою умовою, що забезпечує перехід до внутрішньої потреби цифрового саморозвитку.

Друга психолого-педагогічна умова – дотримання академічної доброчесності та етичних норм користування цифровими ресурсами. Академічна доброчесність забезпечує відповідальне та етичне використання інформації, захист авторських прав, чесне виконання завдань та критичну оцінку джерел [23].

Сучасне цифрове навчання створює нові виклики: плагіат, маніпуляції даними, непрозорі оцінки [36]. Формування академічної доброчесності має бути інтегроване у навчальні програми й включати правила, розвиток критичного мислення, рефлексію та етичні стандарти. Цифровізація освітнього процесу посилює потребу у системних політиках та практиках, що формують культуру доброчесності як ключову компетентність [51].

Дослідження підтверджують, що дотримання доброчесності підвищує якість освітніх результатів та зменшує ризики порушень під час онлайн-оцінювання [1]. Етичний аспект підкреслює концепція цифрової етики

Л. Флоріді (рис. 1.6), що акцентує на моральній відповідальності та усвідомленому прийнятті рішень у цифровому середовищі [7].

Рис. 1.6 Етичні норми відповідальної поведінки в цифровому середовищі

Тому, дотримання академічної доброчесності та етичних норм користування цифровими ресурсами є другою ключовою психолого-педагогічною умовою формування компетентностей з ЦБ. Вона забезпечує відповідальну та етично обґрунтовану цифрову поведінку, підвищує якість освітніх результатів і формує цифрову культуру майбутніх фахівців.

Третя психолого-педагогічна умова – впровадження методики «Використання платформи «Дія.Освіта»» та чат-боту «Безпековичок». Вона передбачає інтеграцію цифрових інструментів у навчальний процес для ефективного формування компетентностей із ЦБ.

Дослідження показують, що поєднання освітніх платформ із чіткою методикою підвищує успішність і мотивацію студентів. Проєктно-орієнтоване навчання з ЦБ сприяє застосуванню знань на практиці та розвитку професійних навичок [52]. Методика «Дія.Освіта» базується на компетентнісному й діяльнісному підходах із виконанням практичних завдань і моделюванням загроз, що відповідає рекомендаціям OECD [19]. Використання чат-ботів, зокрема «Безпековичка», підвищує мотивацію, самостійність і забезпечує індивідуалізацію навчання та зворотний зв’язок [29].

Тому, об’єднане використання «Дія.Освіта» та «Безпековичка» створює умови для персоналізації навчання, врахування індивідуальних потреб здобувачів і формування позитивного ставлення до процесу навчання. Це знижує тривожність та підвищує впевненість у власних цифрових навичках, особливо для студентів.

Висновки до першого розділу

Формування компетентностей з ЦБ у майбутніх фахівців є актуальним і комплексним завданням, зумовленим зростанням цифрових загроз і потребою у розвитку практичних навичок захисту даних. В Україні ці питання регулюються переважно опосередковано, що потребує впровадження обґрунтованих та інноваційних підходів.

ЦБ охоплює знання, навички й відповідальну поведінку, однак міжнародні моделі не повністю враховують специфіку професійної освіти. Ефективність її формування забезпечують мотивація, педагогічна підтримка та використання інтерактивних цифрових інструментів.

РОЗДІЛ 2. МЕТОДИЧНІ ЗАСАДИ ВИКОРИСТАННЯ ПЛАТФОРМИ «ДІЯ.ОСВІТА» ДЛЯ ФОРМУВАННЯ КОМПЕТЕНТНОСТЕЙ З ЦИФРОВОЇ БЕЗПЕКИ У МАЙБУТНІХ ФАХІВЦІВ З ПРОФЕСІЙНОЇ ОСВІТИ

2.1. Модель формування компетентностей з цифрової безпеки та аналіз провідних програмних засобів

Зростання цифрових загроз у професійному середовищі зумовлює потребу цілеспрямованого формування компетентностей із ЦБ у здобувачів освіти. Це вимагає створення науково обґрунтованої моделі, яка забезпечує системність і логічну послідовність цього процесу та підвищує готовність до безпечної діяльності в умовах цифровізації.

У педагогічній науці модель розглядається як спрощене відображення об’єкта чи процесу, що допомагає зрозуміти, проаналізувати й передбачити результати. В освітній практиці її застосовують для опису структури навчання, компетентностей і механізмів їх оцінювання [21]. Водночас моделювання є процесом створення таких моделей через узагальнення та впорядкування елементів навчання, що дозволяє проєктувати ефективні педагогічні рішення, зокрема щодо формування компетентностей із ЦБ [11].

Процес моделювання в педагогіці зумовлює перехід від теоретичного відображення освітніх явищ до побудови цілісних освітніх моделей як систем, що інтегрують цілі, зміст, методи та результати навчання й забезпечують їх ефективне прогнозування та оптимізацію. Дослідники підкреслюють, що моделі допомагають структурувати складні компетентності та відобразити взаємозв’язки педагогічних процесів у зрозумілій формі [8]. У цьому контексті моделювання виконує описову й практичну функції [49].

Науковці також наголошують на важливості цифрових рамок для формування компетентностей, які охоплюють не лише володіння інструментами, а й їх безпечне використання у професійній діяльності. Дослідження у сфері освіти визначають мотиваційні, організаційні та технологічні чинники як

ключові складові відповідних моделей [26]. Європейська рамка DigComp слугує орієнтиром для структурування цифрових компетентностей, включно з безпекою [20], а сучасні моделі інтегрують міжнародні підходи з педагогічними технологіями та оцінюванням [35]. Цифровізація при цьому розглядається як складова педагогічних моделей формування ключових компетентностей [11]. Орієнтація на міжнародні рамки цифрових компетентностей і цифровізацію освіти логічно зумовлює використання різноманітних навчальних засобів, що поєднують теоретичну підготовку з практичною діяльністю та сприяють ефективному формуванню навичок з ЦБ.

Дослідження навчальних засобів свідчить, що вони включають цифрові платформи, онлайн-курси, мультимедійні ресурси, інтерактивні тести, симулятори кіберзагроз, що дозволяє поєднувати теоретичну підготовку з практичною діяльністю та формувати міцні навички з ЦБ.

Реалізація передбачає використання платформи «Дія.Освіта». Також здійснено порівняння цієї платформи з міжнародними аналогами (табл. 2.1).

Таблиця 2.1

Аналіз міжнародних цифрових освітніх сервісів

Освітній сервіс	**Країна (регіон)**	**Ціль та функції**	**Фокус на ЦБ**
Дія.Освіта	Україна	Освітня платформа з серіалами, тестами й симуляторами з ЦБ	Так
Digital Skills and Jobs Platform	ЄС	Освітня платформа, що збирає інформацію, пропозиції, навчальні шляхи з цифрових навичок	Так
Courses and Resources – NCSC	Велика Британія	Освітня платформа з інтерактивними та навчальними матеріалами з основ ЦБ	Так
IBM SkillsBuild	США	Безкоштовні курси з сертифікацією, охоплюють ЦБ	Частково
OpenClassrooms	Франція	Навчання цифрових навичок, ІТ- компетентностей через проєкти	Частково

Для об’єктивного порівняння освітніх платформ визначено шість критеріїв, відібраних за релевантністю, вимірюваністю та практичною цінністю. «Фокус на цифровій безпеці» є ключовим, адже платформи без тематики захисту і протидії цифровим загрозам не відповідають меті дослідження.

«Інтерактивність» підкреслює ефективність активного навчання через практичні завдання. «Доступність» враховує відсутність фінансових, мовних та технічних бар'єрів. «Сертифікація» стимулює завершення курсів, а «актуальність контенту» відображає швидкі зміни в ЦБ. «Адаптивність» оцінює відповідність різним рівням підготовки користувачів.

На основі цих критеріїв проведено порівняльну оцінку п'яти платформ за 5-бальною шкалою (табл. 2.2).

Таблиця 2.2

Порівняльна таблиця оцінки платформ

Критерій оцінювання	**Дія. Освіта**	**Digital Skills and Jobs Platform**	**NCSC UK**	**IBM SkillsBuild**	**Open Classrooms**
Фокус на ЦБ	5	4	5	3	2
Інтерактивність навчання	5	3	4	4	3
Доступність	5	4	4	4	3
Сертифікація	5	4	4	5	4
Актуальність	5	4	4	4	3
Адаптивність та цільова аудиторія	4	4	4	4	4
Оцінка	**4.9**	**3.9**	**4.2**	**4.0**	**3.2**

Аналіз показав, що платформа «Дія.Освіта» є ефективним інструментом формування компетентностей з ЦБ. Вона охоплює кібергігієну, захист даних і протидію кіберзагрозам, а інтерактивний формат (серіали, симуляції, тести, Додаток Г) сприяє розвитку практичних навичок. Локалізація, безкоштовний доступ і державна підтримка забезпечують доступність та довіру, що зумовлює доцільність її поетапного впровадження в освітній процес.

Використання платформи передбачає поетапне впровадження: підготовчий аналіз, мотиваційно-ознайомлювальний етап, навчально-практичний блок із інтеграцією ЦБ у дисципліни та виконання практичних завдань, а також рефлексивно-оцінювальний етап для корекції освітнього процесу. Використовуються лекції, практичні заняття та тренінги, що формують інформаційно-когнітивний, операційно-діяльнісний, мотиваційно-ціннісний та рефлексивний компоненти компетентностей.

На основі аналізу наукових підходів та платформ запропоновано авторську модель використання платформи «Дія.Освіта» для формування компетентностей із ЦБ у здобувачів освіти (рис. 2.1).

Рис. 2.1 Модель використання платформи «Дія.Освіта» для формування компетентностей із ЦБ

Розроблена модель використання платформи «Дія.Освіта» для формування компетентностей із ЦБ у здобувачів освіти є цілісною структурно-

функціональною системою, що поєднує мету, зміст, організаційні засоби, оцінювання та результати. Вона базується на компетентнісному, діяльнісному й особистісно орієнтованому підходах і враховує виклики цифровізації.

Соціальний запит визначається потребою підготовки фахівців, здатних до безпечної та відповідальної поведінки в цифровому середовищі, зокрема щодо захисту даних і протидії кіберзагрозам. Це обґрунтовує доцільність використання «Дія.Освіта» як сучасного освітнього ресурсу.

Змістовий блок охоплює умови ефективного навчання: формування мотивації до безпечної поведінки, дотримання академічної доброчесності та впровадження інтерактивних методик із використанням цифрових ресурсів.

Організаційно-методичний блок передбачає поєднання різних форм навчання, використання проблемного та проєктного навчання, а також застосування цифрових платформ і інтерактивних інструментів.

Постає потреба розроблення методики, що забезпечує практичне застосування підходів і досягнення результатів. Методика – це система методів і засобів для формування компетентностей, яка є інструментом організації ефективного навчання [14]. Її основою є DigComp 2.2, де ЦБ визначено важливою складовою [6], та модель, що поєднує цілі, зміст, методи й засоби навчання.

Оцінювально-діагностичний блок здійснюється за інформаційно- діяльнісним, мотиваційним, рефлексивно-етичним і комунікативним критеріями з визначенням рівнів від низького до високого.

Результативний блок показує підвищення рівня сформованості компетентностей із ЦБ та готовність до безпечної діяльності в цифровому середовищі.

Запропонована модель визначає теоретичні засади та структурну організацію процесу формування компетентностей із ЦБ у здобувачів освіти. Водночас її ефективна реалізація зумовлює необхідність аналізу засобів її впровадження.

Таким чином, розроблена модель використання платформи «Дія.Освіта» забезпечує цілісну організацію процесу формування компетентностей із ЦБ через поєднання мети, змісту, методів, засобів і результатів навчання. Вона передбачає поетапне впровадження та формування інформаційно-когнітивного, операційно-діяльнісного, мотиваційно-ціннісного і рефлексивного компонентів. У результаті це забезпечує підвищення рівня сформованості компетентностей із ЦБ і готовності до безпечної діяльності в цифровому середовищі.

2.2. Розроблення чат-бота як цифрового засобу формування компетентностей з цифрової безпеки з використанням «Дія.Освіта»

Реалізація методики потребує сучасних цифрових інструментів, що забезпечують безперервне навчання, інтерактивність і швидкий зворотний зв’язок. Для інтеграції ЦБ в навчальний процес доцільно використовувати доступні та зрозумілі інтерактивні сервіси. У дослідженні теоретичне навчання проводилось через платформу «Дія.Освіта», а практичне – за допомогою розробленого нами чат-бота «Безпековичок» (рис. 2.2), який дозволяє закріплювати знання на прикладах і сценаріях, служачи ефективним інструментом формування компетентностей з ЦБ.

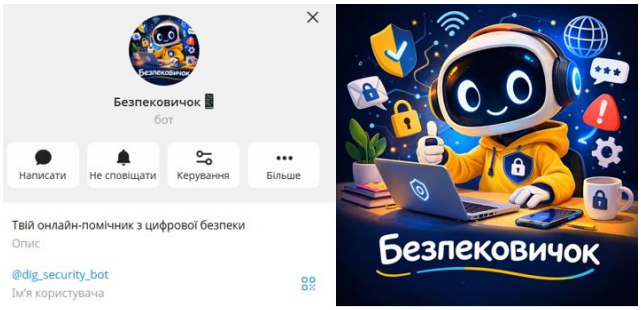


Рис. 2.2 Авторський чат-бот «Безпековичок»

Для проєкту обрали популярний серед молоді месенджер Telegram, що забезпечує зручну мобільну взаємодію. Це дозволило інтегрувати освітній контент у звичне цифрове середовище студентів. Технічна реалізація виконана

на Python із бібліотекою telebot для взаємодії з Telegram Bot API та обробки повідомлень користувачів (рис. 2.3). Структура чат-боту (рис. 2.4).

```
import telebot
from telebot import types

TOKEN = ""
bot = telebot.TeleBot(TOKEN)
```

Рис. 2.3 Бібліотека telebot

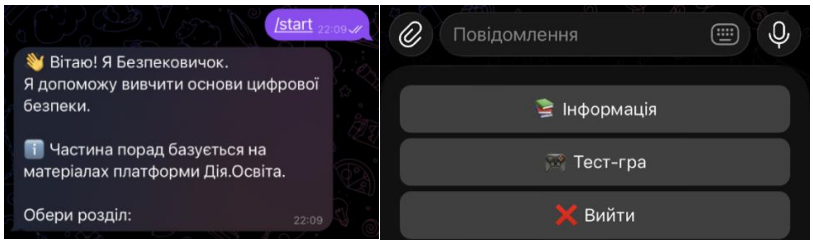


Рис. 2.4 Розділи чат-боту «Безпековичок»

Структура чат-бота включає два основні модулі. Інформаційний модуль містить тематичні блоки з основ ЦБ, зокрема про створення надійних паролів, двофакторну автентифікацію, розпізнавання фішингових атак, захист персональних даних та безпечне користування соцмережами і публічними Wi-Fi. Матеріал подано коротко та структуровано, відповідно до принципів мікронавчання, що сприяє швидкому засвоєнню інформації (рис. 2.5).

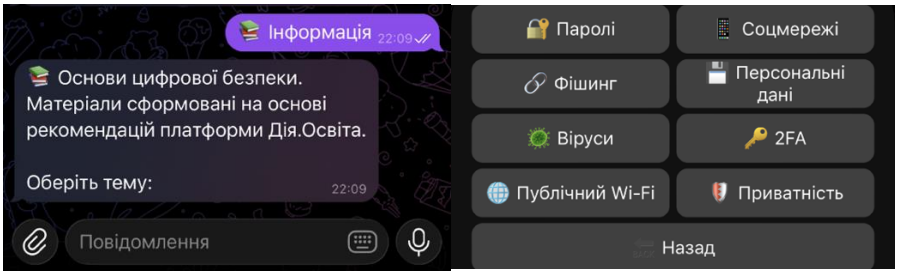


Рис. 2.5 Інформаційний розділ чат-боту «Безпековичок»

Ігровий модуль представлено у вигляді тест-вікторини з трьома рівнями складності: легким, середнім і складним (рис. 2.6). Кожен рівень містить по десять запитань формату «Правда/Брехня», що охоплюють основні аспекти ЦБ.

Система автоматично перевіряє відповіді, підраховує правильні результати та надає пояснення у разі помилки, допомагаючи краще засвоїти матеріал.

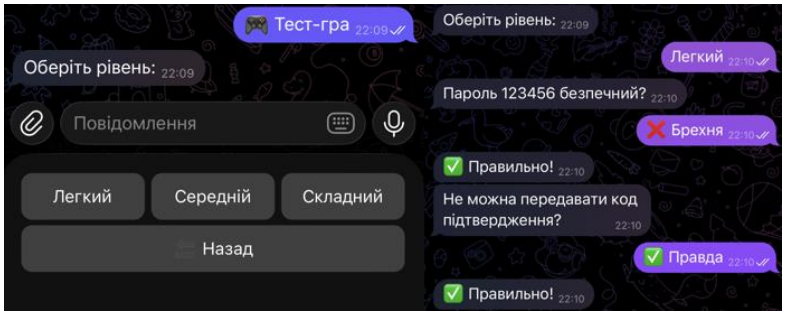


Рис. 2.6 Ігровий розділ чат-боту «Безпековичок»

Чат-бот поєднує теорію з гейміфікацією та самоконтролем, підвищуючи мотивацію, критичне мислення та практичні навички ЦБ. Як доповнення до «Дія.Освіта», він інтегрує формальне та неформальне навчання, закріплюючи знання у зручному цифровому форматі.

Отже, використання платформи «Дія.Освіта» та чат-бота «Безпековичок» створює ефективну систему для формування компетентностей, підвищуючи якість підготовки студентів та відповідаючи сучасним викликам цифровізації освіти.

Висновки до другого розділу

Таким чином, дослідження підтверджує, що модель формування компетентностей з ЦБ у майбутніх фахівців з професійної освіти є цілісною системою, що поєднує цілі, зміст, організаційні засоби та оцінювання результатів. Використання платформи «Дія.Освіта» забезпечує інтеграцію теоретичних знань і практичних навичок, сприяє розвитку мотивації та формуванню готовності до безпечної діяльності в цифровому середовищі.

Розроблена методика дозволяє системно формувати компетентності з ЦБ. Чат-бот «Безпековичок» доповнює платформу «Дія.Освіта», поєднуючи навчальний контент із гейміфікацією, що підвищує мотивацію, критичне мислення та практичні навички студентів.

РОЗДІЛ 3. ЕКСПЕРИМЕНТАЛЬНА ПЕРЕВІРКА ПСИХОЛОГО-ПЕДАГОГІЧНИХ УМОВ ВИКОРИСТАННЯ ПЛАТФОРМИ «ДІЯ.ОСВІТА» У ФОРМУВАННІ ЦИФРОВОЇ БЕЗПЕКИ МАЙБУТНІХ ФАХІВЦІВ ПРОФЕСІЙНОЇ ОСВІТИ

3.1. Критерії та рівні сформованості компетентностей з цифрової безпеки: організація та результати констатувального експерименту

Для забезпечення науково обґрунтованої перевірки ефективності психолого-педагогічних умов використання платформи «Дія.Освіта» у формуванні ЦБ майбутніх фахівців професійної освіти було організовано та проведено констатувальний експеримент. Ефективна перевірка результатів педагогічного впливу потребує чітких критеріїв, показників і рівнів сформованості компетентностей. На основі аналізу наукових праць та попередніх розділів виокремлено три ключові критерії компетентностей з ЦБ: 1) *когнітивний* – оцінює знання про цифрові загрози, принципи захисту даних та законодавство; *2) операційно-діяльнісний* – практичне застосування знань; *3) мотиваційно-ціннісний* – ставлення до ЦБ і готовність до відповідальної поведінки.

Визначено також три рівні сформованості компетентностей: низький, середній та високий. Низький рівень (репродуктивний) – здобувач має фрагментарні знання про цифрові загрози; практичні навички з ЦБ не сформовані. Середній рівень (конструктивний) – здобувач має достатньо систематизовані знання з основ ЦБ; здатний застосовувати набуті знання у типових ситуаціях. Високий рівень (творчий) – здобувач має глибокі, системні знання з ЦБ; впевнено застосовує їх.

Для проведення педагогічного експерименту було обрано студентів факультету інформаційні технології спеціальності «Професійна освіта. Цифрові технології» та «Комп’ютерні науки» другого курсу закладу вищої освіти. Дослідження включало такі етапи: констатувальний експеримент (КЕ), формувальний експеримент (ФЕ).

На констатувальному етапі сформовано дві групи: експериментальну (ЕГ, n=22) та контрольну (КГ, n=22). Інструментарій діагностики включав: авторський тест з ЦБ (30 запитань, три блоки, Додаток А); анкету мотиваційно- ціннісного ставлення до ЦБ (адаптовано за методикою Є. Климова, Додаток Б); практичне завдання – виконання серії завдань у чат-боті «Безпековичок» (Додаток В). Результати КЕ наведено в таблиці 3.1.

Таблиця 3.1

Результати КЕ в ЕГ (n=22) та КГ (n=22)

Рівень	**ЕГ (осіб)**	**ЕГ (%)**	**КГ (осіб)**	**КГ (%)**	**Різниця ЕГ−КГ**
Низький	12	55%	10	45%	+10%
Середній	8	36%	10	45%	−9%
Високий	2	9%	2	9%	0%
Усього	**22**	100%	**22**	100%	—
Середній бал	**1,55**		**1,64**		−0,09

Як свідчать дані таблиці 3.1, в обох групах переважають студенти з низьким рівнем сформованості компетентностей з ЦБ. Середні зважені бали є близькими (ЕГ: 1,55, КГ: 1,64), різниця між ними становить лише 0,09 бали, що вказує на вихідну однорідність груп.

Для статистичного підтвердження однорідності груп застосовано критерій Пірсона χ^2. Розрахунки показали: $\chi^2 = 0{,}404$ при критичному значенні $\chi^2_{крит} = 5{,}991$ ($df = 2$, $p = 0{,}05$). Оскільки $\chi^2 < \chi^2_{крит}$, нульова гіпотеза про однорідність груп приймається. Отже, на початку експерименту ЕГ і КГ статистично не відрізнялися між собою.

Для наочного відображення розподілу рівнів на констатувальному зрізі наведено рис. 3.1.

Результати констатувального зрізу за окремими критеріями наведено в таблиці 3.2.

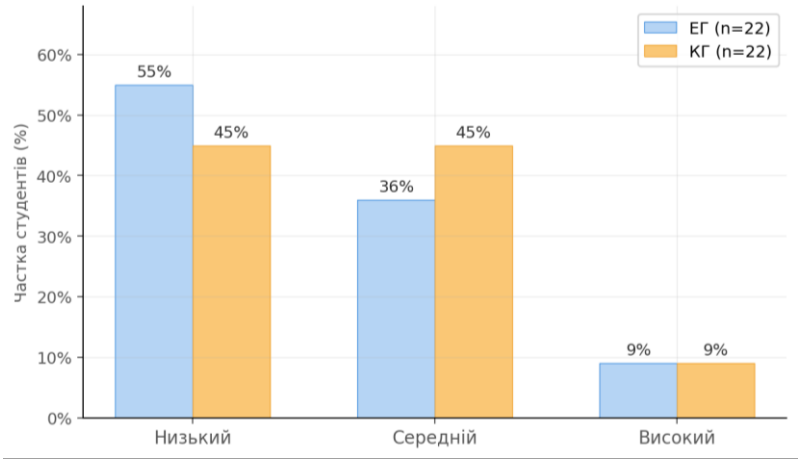


Рис. 3.1 Розподіл студентів за рівнями сформованості компетентностей з ЦБ (констатувальний зріз)

Таблиця 3.2

Розподіл студентів за рівнями сформованості

Критерій	ЕГ Низьк.	ЕГ Серед.	ЕГ Висок.	КГ Низьк.	КГ Серед.	КГ Висок.
Когнітивний	59%	31%	10%	60%	30%	10%
Операційно-діяльнісний	64%	27%	9%	64%	27%	9%
Мотиваційно-ціннісний	45%	45%	9%	41%	45%	14%

Аналіз даних таблиці 3.2 свідчить про симетричний розподіл в обох групах за всіма критеріями, що додатково підтверджує їх вихідну однорідність. Найбільш проблемним є операційно-діяльнісний критерій: у обох групах 64% студентів мають низький рівень практичних навичок з ЦБ. Мотиваційно-ціннісний критерій демонструє дещо кращий стан: частка студентів з низьким рівнем тут нижча (45%), що пояснюється загальним зростанням обізнаності молоді про кіберзагрози в умовах інформаційної війни. Когнітивний критерій займає проміжне положення (59–60% низького рівня).

Отже, результати констатувального етапу підтвердили, що рівень сформованості компетентностей з ЦБ в обох групах є переважно низьким (ЕГ – 55%, КГ – 45%), групи є статистично однорідними ($\chi^2 = 0{,}404 < \chi^2_{крит} = 5{,}991$), а найбільш проблемним виявився операційно-діяльнісний критерій, що обґрунтовує необхідність упровадження відповідних педагогічних умов.

3.2. Формувальний експеримент та узагальнення результатів дослідження

Формувальний етап педагогічного експерименту тривав упродовж квітня 2026 р. і проводився за паралельним дизайном: ЕГ (n=22) навчалася за розробленою методикою (Додаток Г) з використанням платформи «Дія.Освіта» та чат-боту «Безпековичок» відповідно до трьох визначених психолого-педагогічних умов, КГ (n=22) у традиційному форматі. Вимірювання проводилися в обох групах одночасно: Методики вимірювання включали: – тестування (30 запитань); – анкета; – практичні завдання у чат-боті «Безпековичок» (Додатки А, Б, В). Узагальнення та статистична обробка отриманих даних дозволили визначити динаміку змін у рівнях сформованості компетентностей із ЦБ у здобувачів освіти ЕГ та КГ, що відображено в результатах порівняльного аналізу на КЕ та ФЕ експерименту (табл. 3.3).

Таблиця 3.3

Порівняння результатів ЕГ (n=22) і КГ (n=22) на КЕ та ФЕ

Рівень	ЕГ до	КГ до	Різниця (до)	ЕГ після	КГ після	Різниця (після)
Низький	12 (55%)	10 (45%)	+10%	4 (18%)	8 (36%)	**−18%**
Середній	8 (36%)	10 (45%)	−9%	8 (36%)	10 (45%)	−9%
Високий	2 (9%)	2 (9%)	0%	10 (45%)	4 (18%)	**+27%**
Середній бал	1,55	1,64	−0,09	**2,27**	1,82	**+0,45**

Дані таблиці 3.3 свідчать про суттєво відмінний розподіл рівнів між групами на контрольному зрізі. До початку експерименту ЕГ і КГ були практично однаковими: частка студентів з високим рівнем в обох групах становила 9%, різниця середніх балів лише 0,09 бали. Після формувального впливу ситуація змінилася: в ЕГ частка студентів з високим рівнем зросла до 45%, тоді як у КГ лише до 18% (різниця +27 п.п. на користь ЕГ). Частка студентів з низьким рівнем в ЕГ становить 18% проти 36% у КГ. Середній бал в ЕГ (2,27) перевищує середній бал КГ (1,82) на 0,45 бали. Порівняльна діаграма (рис. 3.2).

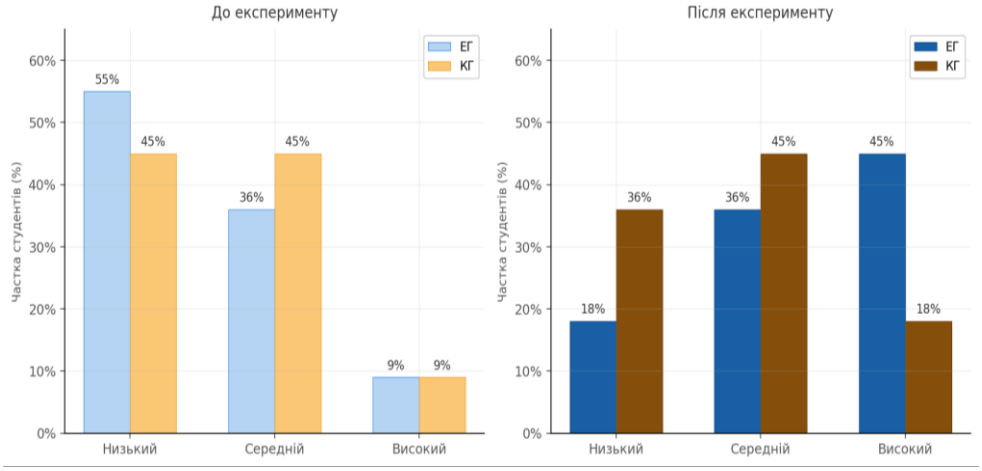


Рис. 3.2. Порівняння рівнів сформованості компетентностей з ЦБ в ЕГ і КГ до та після формувального експерименту

Для перевірки статистичної значущості відмінностей між групами застосовано непараметричний критерій Манна-Уітні (табл. 3.4).

Таблиця 3.4

Результати статистичного аналізу (критерій Манна-Уітні)

Порівняння	Критерій	Емп. знач.	Крит. знач.	p	Висновок
ЕГ vs КГ після експерименту	Манна-Уітні	U = 320,0	–	0,026	**Значущі (p < 0,05)**

На формувальному етапі експерименту зафіксовано статистично значущу перевагу ЕГ над КГ. Це підтверджує, що відмінності між групами після формувального впливу не є випадковими і зумовлені саме застосуванням розробленої методики. Динаміку середнього балу сформованості компетентностей з ЦБ в обох групах наведено на рис. 3.3.

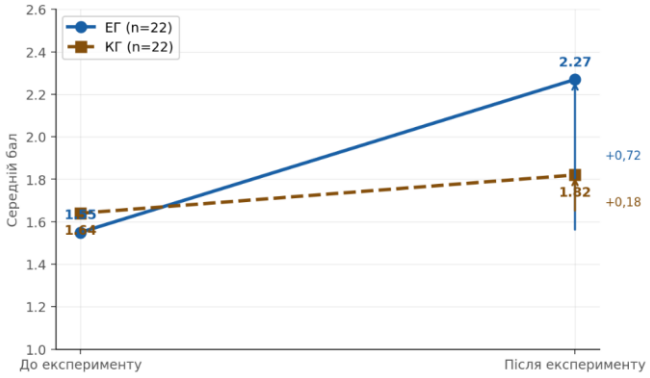


Рис. 3.3. Динаміка середнього балу сформованості компетентностей з ЦБ

Для відображення змін за критеріями наведено таблицю 3.5 і рисунок 3.4.

Таблиця 3.5

Динаміка рівнів сформованості за критеріями у ЕГ (до / після, %)

Критерій	Низьк. до	Низьк. після	Серед. до	Серед. після	Висок. до	Висок. після
Когнітивний	55%	18%	36%	36%	9%	45%
Операційно-діяльнісний	55%	18%	36%	36%	9%	**45%**
Мотиваційно-ціннісний	55%	18%	36%	**45%**	9%	36%

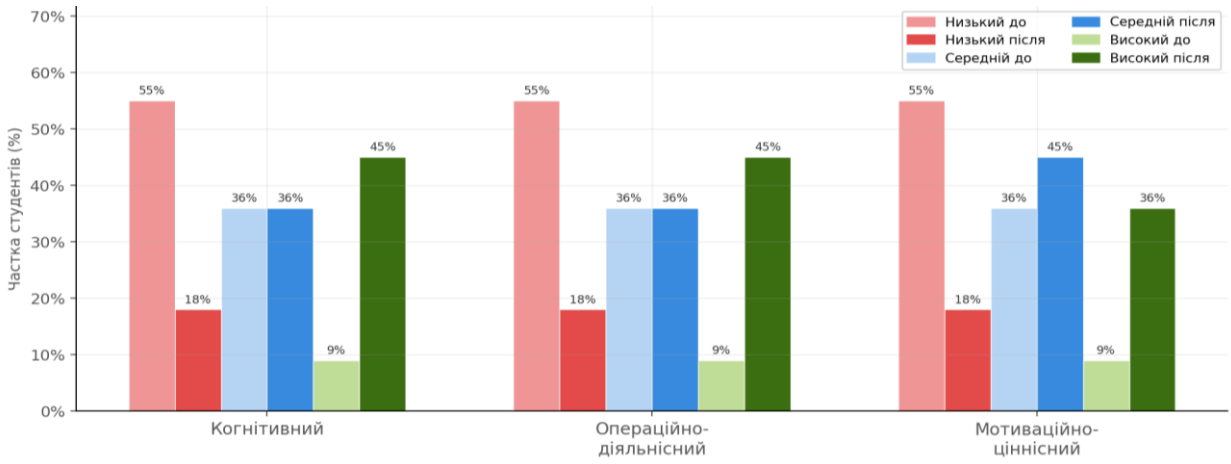


Рис. 3.4. Динаміка рівнів сформованості компетентностей з ЦБ за критеріями у ЕГ (до / після, %)

Особливо показовим є зростання мотиваційно-ціннісного компонента – ознака того, що навчання набуло особистісно значущого характеру.

Висновки до третього розділу

На констатувальному етапі сформовано ЕГ і КГ по 22 студенти, підтверджено їх вихідну однорідність ($\chi^2 = 0{,}404 < 5{,}991$). В обох групах переважав низький рівень компетентностей з ЦБ, найслабшим був операційно-діяльнісний критерій (64%). Формувальний експеримент показав статистично значущу перевагу ЕГ над КГ ($U = 320{,}0$, $p = 0{,}026$): 45% студентів з високим рівнем проти 18%, середній бал – 2,27 проти 1,82. Результати підтверджують ефективність методики.

ВИСНОВКИ

1. Здійснено аналіз проблеми формування компетентностей з цифрової безпеки у науково-педагогічній літературі та нормативно-правових документах. Встановлено, що чинне законодавство України не містить системного підходу до формування цих компетентностей, а питання цифрової безпеки реалізується опосередковано – через загальний компетентнісний підхід. Узагальнення наукових підходів дозволило уточнити поняття «цифрова безпека» як процес і результат забезпечення безпечної та відповідальної взаємодії учасників освітнього процесу з цифровим середовищем, що охоплює захист даних, дотримання принципів конфіденційності та формування навичок безпечної поведінки.

2. Визначено й обґрунтовано три психолого-педагогічні умови впровадження платформи «Дія.Освіта» у процес формування компетентностей з цифрової безпеки: мотивація здобувачів до розвитку цифрових компетентностей і безпечної поведінки в мережі; дотримання академічної доброчесності та етичних норм користування цифровими ресурсами; впровадження авторської методики із використанням платформи «Дія.Освіта» та чат-бота «Безпековичок».

3. Розроблено модель використання платформи «Дія.Освіта», яка є цілісною педагогічною системою, що поєднує мету, зміст, організаційно-методичний та оцінювально-діагностичний блоки. Порівняльний аналіз засвідчив, що «Дія.Освіта» отримала найвищу сумарну оцінку (4,9 балів) серед аналізованих міжнародних платформ завдяки повному фокусу на цифровій безпеці, інтерактивності та безкоштовному доступу.

4. Спроєктовано та реалізовано авторський чат-бот «Безпековичок» на платформі Telegram. Чат-бот містить інформаційний модуль із тематичними блоками з основ цифрової безпеки та ігровий модуль із тест-вікториною трьох рівнів складності. Поєднання теоретичного та практичного компонентів із гейміфікацією забезпечило ефективне доповнення до платформи «Дія.Освіта» та сприяло підвищенню мотивації й практичних навичок студентів.

5. Проведено експериментальне дослідження. На констатувальному етапі сформовано ЕГ і КГ по 22 студенти. Статистично підтверджено їх вихідну однорідність ($\chi^2 = 0{,}404 < \chi^2_{крит} = 5{,}991$). В обох групах зафіксовано переважно низький рівень сформованості компетентностей з ЦБ, найбільш проблемним виявився операційно-діяльнісний критерій (64% студентів з низьким рівнем). Формувальний експеримент показав статистично значущу перевагу ЕГ над КГ за критерієм Манна-Уітні ($U = 320{,}0$, $p = 0{,}026$): частка студентів з високим рівнем в ЕГ становить 45% проти 18% у КГ, середній бал 2,27 проти 1,82 (різниця +0,45 бали). Отримані результати підтверджують ефективність розробленої методики та правомірність визначених психолого- педагогічних умов.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Bretag T., Harper R., Burton M., Ellis C., Newton P., Rozenberg P., Saddiqui S., van Haeringen K. Contract cheating: A survey of Australian university students. *Studies in Higher Education*. 2019. Vol. 44, № 11. P. 1837–1856.

2. Buriachok V., Korshun N., Zhyltsov O., Sokolov V., Skladannyi P. Implementation of Active Cybersecurity Education in Ukrainian Higher School. *Proceedings of the International Conference on Emerging Cybersecurity: Education and Technology*. 2023. P. 533–551. URL: https://doi.org/10.1007/978-3-031-35467-0_32

3. Carretero S., Vuorikari R., Punie Y. *DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use*. Luxembourg : Publications Office of the European Union, 2017. URL: https://doi.org/10.2760/38842

4. Deci E. L., Ryan R. M. The «what» and «why» of goal pursuits: Human needs and the self-determination of behavior. *Psychological Inquiry*. 2000. Vol. 11, № 4. P. 227–268.

5. Esmaili R., van Dijk G. Bridging Knowledge Gaps: Advancing Cybersecurity Education via Absorptive Capacity & Collaboration. *Proceedings of the European Conference on Information Warfare and Security*. 2025. Vol. 24, № 1. P. 762–770. URL: https://doi.org/10.34190/eccws.24.1.3462

6. European Commission. *DigComp 2.2: The Digital Competence Framework for Citizens*. Luxembourg : Publications Office of the European Union, 2022. URL: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC128415/JRC128415_01.pdf

7. Floridi L., Cath C., Taddeo M. Digital Ethics: Its Nature and Scope. *The 2018 Yearbook of the Digital Ethics Lab*. 2019. P. 9–17. 10.1007/978-3-030-17152-0_2

8. Garmanson G. Building a model of the digital culture of teachers. *Adaptive Management: Theory and Practice. Series Pedagogics*. 2024. URL: https://doi.org/10.33296/2707-0255-16(31)-10

9. ISO/IEC 27000 series – International standards for information security management systems. URL: https://www.iso.org/isoiec-27001-information-security.html (дата звернення: 05.04.2026).

10. Kiryakova G., Kozhuharova D. The Digital Competences Necessary for the Successful Pedagogical Practice of Teachers in the Digital Age. *Education Sciences*. 2024. Vol. 14, № 5. P. 507. URL: https://doi.org/10.3390/educsci14050507

11. Kotelevets K. Model of adaptive management of formation of digital competence basics of primary school students. *ScienceRise: Pedagogical Education*. 2021. https://doi.org/10.15587/2519-4984.2021.248257

12. Kravchenko L., Shevchenko N. Digitalization as a technology for forming key competencies of future professionals. *Vytoky Pedagogichnoi Maisternosti*. 2025. № 35. https://doi.org/10.33989/2075-146x.2025.35.331129

13. Li Y., Li W. *Proceedings of the 2023 International Conference on e-Learning and Digital Education*. 2023. https://doi.org/10.2991/978-94-6463-172-2_80

14. Matos J. F., Freitas A., Estrela E., Galego C., Piedade J. Teaching research methods courses in education: Towards a research-based culture. *Social Sciences*. 2023. Vol. 12. P. 338. https://doi.org/10.3390/socsci12060338

15. Mulder M. *Competence-Based Vocational and Professional Education: Bridging the Worlds of Work and Education*. Cham: Springer, 2017. https://doi.org/10.1007/978-3-319-41713-4

16. Mutanga M. B. Students' Perspectives and Experiences in Project-Based Learning: A Qualitative Study. *Trends in Higher Education*. 2024. Vol. 3, № 4. P. 903–911. https://doi.org/10.3390/higheredu3040052

17. Ning Y., Danso S. D. Assessing Pedagogical Readiness for Digital Innovation: A Mixed-Methods Study. 2025. https://doi.org/10.48550/arXiv.2502.15781

18. Nurul Soliha, Wolor C. W., Swaramarinda D. R. *The Influence of Digital Competence and Learning Motivation on Student Performance*. 2025. https://doi.org/10.21009/ISC-BEAM.013.125

19. OECD. *Innovating Education and Educating for Innovation*. Paris: OECD

Publishing, 2016. https://doi.org/10.1787/9789264265097-en

20. Ovcharuk O. European strategy for determining the level of competence in the field of digital technologies: a framework for digital competence for citizens. *Educational Dimension*. 2020. https://doi.org/10.31812/educdim.v55i0.4381

21. Rabiodun-Oyebanji O. J., Odiase K. B. Models and model-building in education. *Educational Management and Leadership*. 2024. https://www.researchgate.net/publication/388846472_MODELS_AND_MODEL-BUILDING_IN_EDUCATION

22. Redecker M. *European Framework for the Digital Competence of Educators: DigCompEdu*. Luxembourg: Publications Office of the European Union, 2017. https://doi.org/10.2760/159770

23. Sharma S. Fostering Academic Integrity in the Digital Age: Empowering Student Voices to Navigate Technology as a Tool for Classroom Policies. *Brock Education Journal*. 2024. Vol. 33, № 3. P. 99–121. https://doi.org/10.26522/brocked.v33i3.1180

24. Shevchenko N. F., Volobuyeva O. S., Ivanchuk M. H. (2023). Research of psychological and pedagogical conditions for the formation of personal and professional identity of vocational students. *Insight: The Psychological Dimensions of Society*. 2023. № 9. P. 148–167. https://doi.org/10.32999/KSU2663-970X/2023-9-9

25. Shykyrynska O., Liapunova V., Melnykova O., Mnyshenko K., Petryshyna T. Readiness of the future preschool and primary education specialists to form the foundations of children's cyber security. *Vide. Tehnoloģija. Resursi*. 2024. Vol. 2. P. 481–484. https://doi.org/10.17770/etr2024vol2.8087

26. Tokovska M., Sheben T., Yamborova L. Digital Competencies Development in Higher Education Institutions: A Mixed Methods Research Study. *Emerging Science Journal*. 2022. Vol. 6. P. 150–165. https://doi.org/10.28991/ESJ-2022-SIED-011

27. Ussher-Eke D. From awareness to action: Designing effective cybersecurity training programs. *International Journal of Science and Research Archive*. 2025. Vol. 16, № 2. P. 494–504. https://doi.org/10.30574/ijsra.2025.16.2.2348

28. Vuorikari R., Kluzer S., Punie Y. *DigComp 2.2: The Digital Competence Framework for Citizens*. Luxembourg: Publications Office of the European Union, 2022. https://doi.org/10.2760/115376

29. Winkler R., Sollner M. Unleashing the Potential of Chatbots in Education. *Business. Information Systems Engineering*. 2018. Vol. 60. P. 489–494. https://doi.org/10.1007/s12599-018-0542-4

30. Антонченко М., Павленко І. Роль цифрової компетентності та цифрової грамотності в сучасній освіті. *Scientific Collection InterConf*. 2024. https://doi.org/10.31110/2616-650X-vol13i3-010

31. Біла З. В. Захист інформації в інформаційних системах. *ПОЛІТ. Сучасні проблеми науки. Кібербезпека та програмна інженерія* : тези доп. XXIII Міжнар. наук.-практ. конф. здобувачів вищої освіти і молодих учених, м. Київ, 2023 р. Київ : НАУ, 2023. С. 93.

32. Боско Н., Бела Л. Формування цифрової компетентності здобувачів закладів фахової передвищої освіти. *Фізико-Математична Освіта*. 2024. Т. 39, № 2. С. 7–13. https://doi.org/10.31110/fmo2024.v39i2-01

33. Делембовський М., Ткаченко В., Мельник Д. Навчання та сертифікація спеціалістів з кібербезпеки в Україні. *Grail of Science*. 2024. № 41. С. 282–286. https://doi.org/10.36074/grail-of-science.05.07.2024.044

34. Дорош О. В., Василенко В. Ю. Цифрова безпека в освіті: досвід зарубіжних країн. *Прикладні аспекти сучасних міждисциплінарних досліджень* : матеріали II Міжнар. наук.-практ. конф. м. Вінниця. 2023. С. 22–24.

35. Єчкало Ю. В., Ткачук В. В., Семеріков С. О., Хоцкіна С. М., Маркова О. М., Кравець А. С. Розвиток цифрової компетентності в освіті з інформатики: інтегрована структура для педагогічних інновацій, заснованих на теорії. *Освітній вимір*. 2025. https://doi.org/10.55056/ed.945

36. Закрижевська І., Овод Л. Роль освіти у формуванні цифрової етики та підтримці академічної доброчесності. *Вісник Хмельницького національного університету. Серія «Економічні науки»*. 2024. Т. 334, № 5. С. 232–237. https://doi.org/10.31891/2307-5740-2024-334-33

37. Коваленко В., Осипчук Т. Проблема розвитку цифрової компетентності з кібербезпеки вчителів закладів загальної середньої освіти. https://doi.org/10.31110/fmo2024.v39i2-05

38. Лукіянчук А. М. Психологічні умови розвитку цифрової компетентності педагогічних працівників. 2021. https://lib.iitta.gov.ua/id/eprint/725425

39. Макаренко Н. М. Психолого-педагогічні умови розвитку компетенцій. *Проблеми сучасної психології*. 2018. № 40 С. 226–235. https://doi.org/10.32626/2227-6246.2018-40.226-235

40. Митник О. Я., Островершенко А. П. Психолого-педагогічні умови формування цифрової компетентності здобувачів вищої освіти. *Освітньо-науковий простір.* 2025. № 1(8). https://doi.org/10.31392/ONP.2786-6890.8(1)/1.2025.08

41. Мороз П. В., Мороз І. В. Психолого-педагогічні умови формування в учнів старшої школи історичної дослідницької компетентності. 2020. https://doi.org/10.32405/2411-1317-2025-3-101-121

42. Про вищу освіту: Закон України від 01.07.2014 р. № 1556-VII. *Законодавство України*. URL: https://zakon.rada.gov.ua (дата звернення: 05.04.2026).

43. Про освіту: Закон України від 05.09.2017 № 2145-VIII. *Законодавство України.* URL: https://zakon.rada.gov.ua (дата звернення: 05.04.2026).

44. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/go/2163-19 (дата звернення: 05.04.2026).

45. Про фахову передвищу освіту: Закон України від 02.02.2018 № 2523-VIII. *Законодавство України*. URL: https://zakon.rada.gov.ua (дата звернення: 05.04.2026).

46. Пугач В. Психологічні аспекти дистанційного навчання: мотивація, самоорганізація та підтримка студентів. – *Педагогіка безпеки*. 2025. Т. 10, № 1. С. 26–32. https://doi.org/10.31649/2524-1079-2025-10-1-026-032

47. Руденко Ю., Ситник Л., Пасічний Р., Бєляєва О. М., Дегтярьова Н. та Барабаш А. С. Аналіз результатів дослідження ефективності розвитку навичок кібербезпеки у студентів. 2025. С. 390–395. https://doi.org/10.1109/mipro65660.2025.11132016

48. Султанова Л., Прокоф'єва М. Цифрова безпека в галузі вищої освіти. *Освіта дорослих: теорія, досвід, перспективи.* 2022. 2022. Т. 21, № 1. С. 106–117. https://doi.org/10.35387/od.1(21).2022.106-117

49. Тітова Л. Модель формування інформаційно-цифрової компетентності майбутніх учителів математики. *Молодь і ринок*. 2024. https://doi.org/10.24919/2308-4634.2024.314633

50. Ткачук В. В., Біла З. В., Єчкало Ю. В., Хоцкіна С. М. Формування та розвиток цифрової компетентності у здобувачів вищої освіти. *Розвиток промисловості та суспільства* : матеріали Міжнар. наук.-техн. конф. (28–30 трав. 2026 р., м. Кривий Ріг). Кривий Ріг : КНУ, 2026. С. 167.

51. Тулін К. Академічна доброчесність у цифрову добу: проблеми та стратегії гарантії. *Вісник Київського національного університету імені Тараса Шевченка. Серія «Педагогіка». 2024. №* 1(19). https://doi.org/10.17721/2415-3699.2024.19.12

52. Уварова Т., Стас Т. Медіаграмотність та медіакомпетентність у сучасній освіті: виклики та тенденції. *Актуальні питання гуманітарних наук.* 2020. Вип. 30, т. 3. С. 246–252.

ДОДАТКИ

Додаток А

Авторський тест для визначення рівня сформованості компетентностей з цифрової безпеки

№	Критерій	Питання / твердження	а	б	в	Правильна відповідь
БЛОК 1. КОГНІТИВНИЙ (ЗНАННЯ)						
1	Когнітивний	Що таке фішинг?	Програма	Шахрайство	Вірус	б
2	Когнітивний	Найбільш надійний пароль	123456	qwerty	S!k9#Lm2@	в
3	Когнітивний	Двофакторна аутентифікація	Пароль	Додаткова перевірка	Антивірус	б
4	Когнітивний	Персональні дані	Ім’я	Адреса	Усі	в
5	Когнітивний	HTTPS означає	Небезпека	Захист	Швидкість	б
6	Когнітивний	Функція антивірусу	Прискорення	Захист	Очищення	б
7	Когнітивний	Кібергігієна	Очищення	Правила безпеки	Програма	б
8	Когнітивний	Соціальна інженерія	Антивірус	Обман	Оновлення	б
9	Когнітивний	Резервне копіювання	Видалення	Копія	Пароль	б
10	Когнітивний	Мета кібербезпеки	Розваги	Захист	Швидкість	б
БЛОК 2. ОПЕРАЦІЙНО-ДІЯЛЬНІСНИЙ (УМІННЯ)						
11	Операційний	Підозрілий лист	Перейти	Перевірити	Переслати	б
12	Операційний	Перевірка сайту	Дизайн	HTTPS	Будь-який	б
13	Операційний	Злам акаунта	Нічого	Змінити пароль	Видалити	б
14	Операційний	Надійний пароль	Дата	Складний	Ім’я	б
15	Операційний	Вірус	Ігнор	Антивірус	Вимкнути	б

16	Операційний	Захист у соцмережах	Відкрити	Приватність	Публікувати	б
17	Операційний	Чужий код SMS	Ввести	Ігнорувати	Передати	б
18	Операційний	Перевірка інформації	Повірити	Перевірити	Поширити	б
19	Операційний	Публічний Wi-Fi	Вводити	Обмежити/VPN	Нічого	б
20	Операційний	Кібербулінг	Ігнор	Повідомити	Відповісти	б
БЛОК 3. МОТИВАЦІЙНО-ЦІННІСНИЙ (СТАВЛЕННЯ)						
21	Мотиваційний	ЦБ важлива для мене	☐	☐	☐	–
22	Мотиваційний	Я створюю надійні паролі	☐	☐	☐	–
23	Мотиваційний	Я перевіряю інформацію	☐	☐	☐	–
24	Мотиваційний	Я хочу більше знати про ЦБ	☐	☐	☐	–
25	Мотиваційний	Дотримуюся правил безпеки	☐	☐	☐	–
26	Мотиваційний	Відповідально ставлюся до даних	☐	☐	☐	–
27	Мотиваційний	Розумію кіберризики	☐	☐	☐	–
28	Мотиваційний	Готовий змінювати поведінку	☐	☐	☐	–
29	Мотиваційний	Важливо навчати інших	☐	☐	☐	–
30	Мотиваційний	Дотримуюся цифрової етики	☐	☐	☐	–

Результати

Рівень	Кількість балів
Низький	30–59
Середній	60–79
Високий	80–90

Додаток Б

Анкета мотиваційно-ціннісного ставлення до цифрової безпеки (за методикою Є. Климова, адаптована)

Інструкція: Оцініть кожне твердження за шкалою від 1 до 5 (1 – повністю не згоден, 5 – повністю згоден).

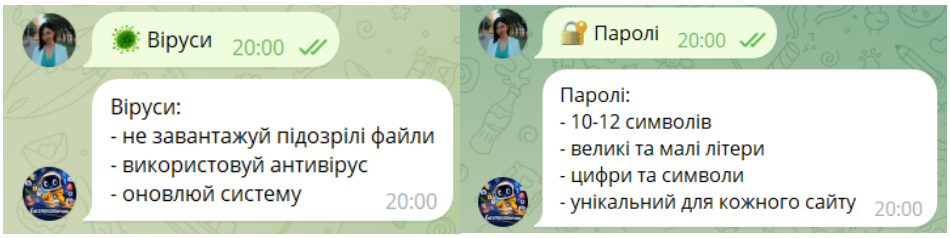
1. Я вважаю, що цифрова безпека є важливою складовою моєї майбутньої професії.
2. Я дотримуюся правил захисту особистих даних у цифровому середовищі.
3. Мені цікаво дізнаватися нову інформацію про кіберзагрози.
4. Я регулярно змінюю паролі та використовую складні комбінації.
5. Я усвідомлюю відповідальність за поширення інформації в інтернеті.
6. Я прагну підвищувати свій рівень цифрової безпеки.
7. Я вважаю важливим навчати інших основам кібергігієни.
8. Я критично оцінюю інформацію з інтернет-джерел.
9. Я готовий(а) витрачати час на навчання цифровій безпеці.
10. Я дотримуюся етичних норм у цифровому середовищі.

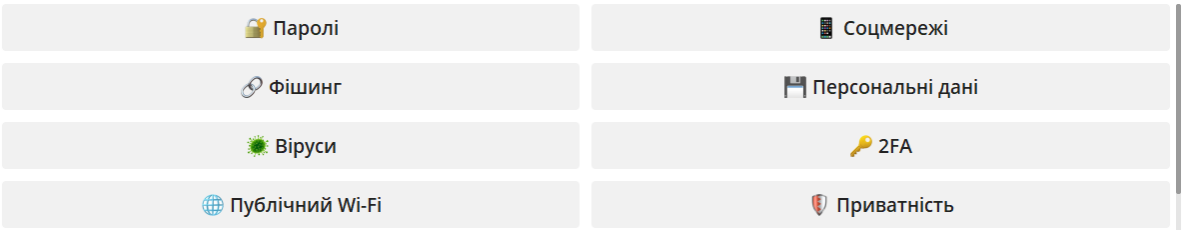
Додаток В

Практична інтерактивна частина з чат-ботом «Безпековичок»

Блок 1. Інформаційний

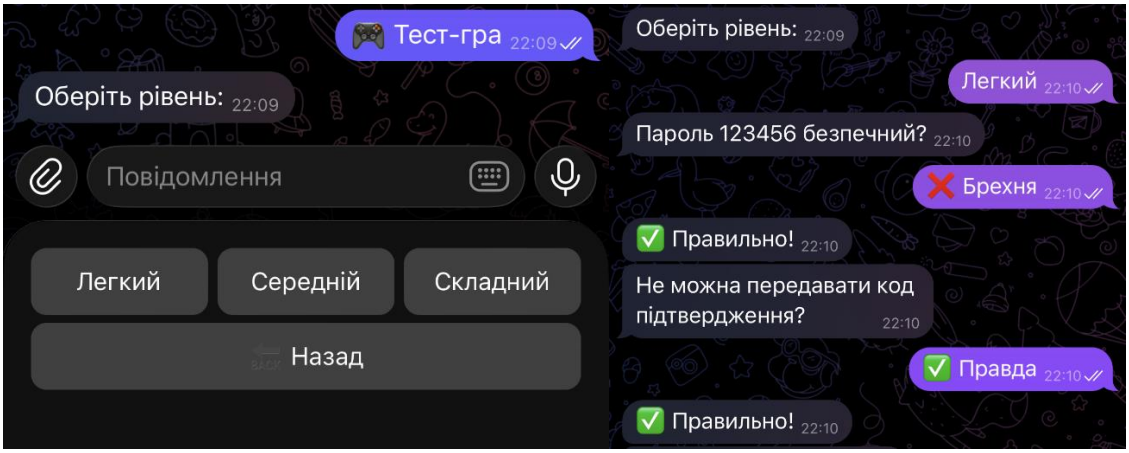
Студенти проходять короткі модулі, де містяться короткі пояснення.

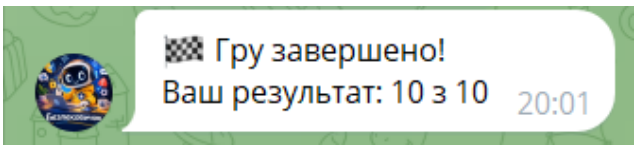




Блок 2. Тест-гра

Формат: 10 запитань; автоматичне оцінювання; пояснення, якщо обрано хибну відповідь.





Додаток Г

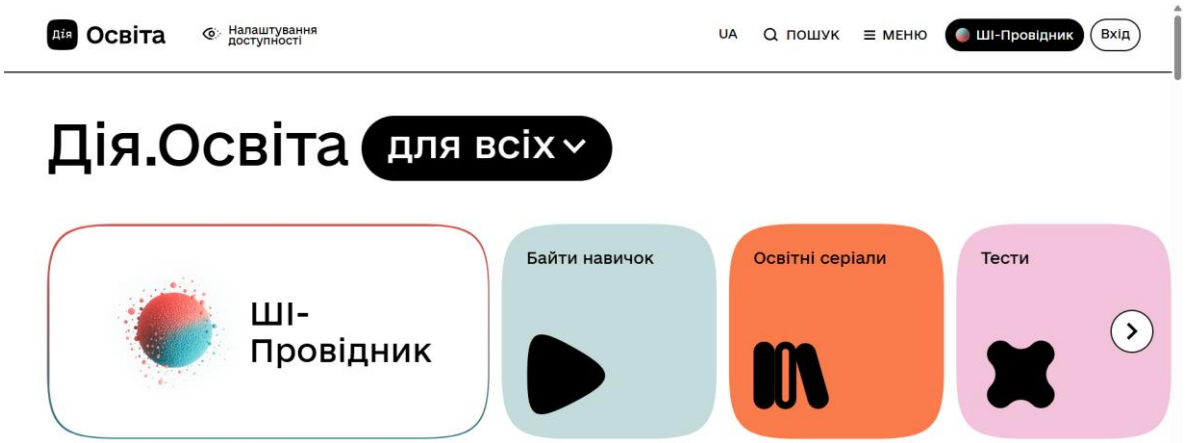
Методика формування компетентностей з цифрової безпеки із використанням «Дія.Освіта» та чат-боту «Безпековичок»

Мета: формування когнітивного, операційно-діяльнісного та мотиваційно- ціннісного компонентів цифрової безпеки.

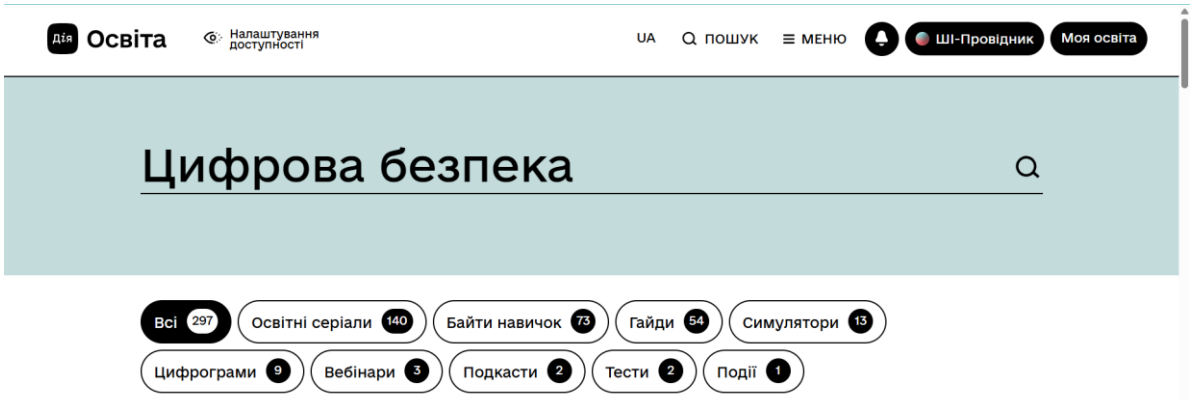
Етапи:

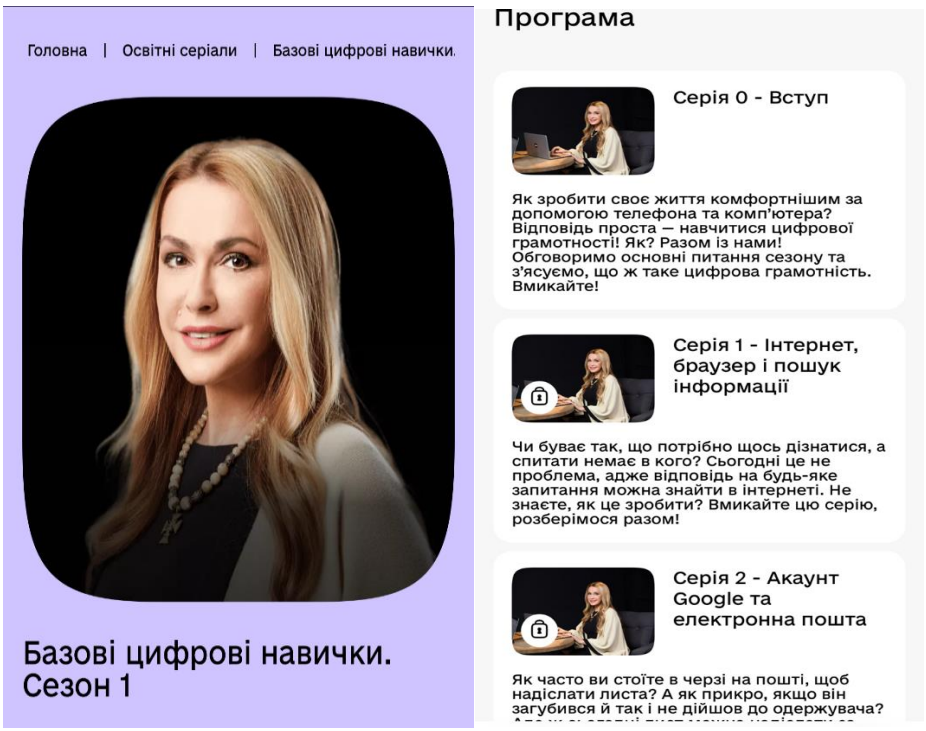
1. Мотиваційно-орієнтувальний (1 тиждень):

– реєстрація на платформі «Дія.Освіта»;



– проходження вступного модуля;





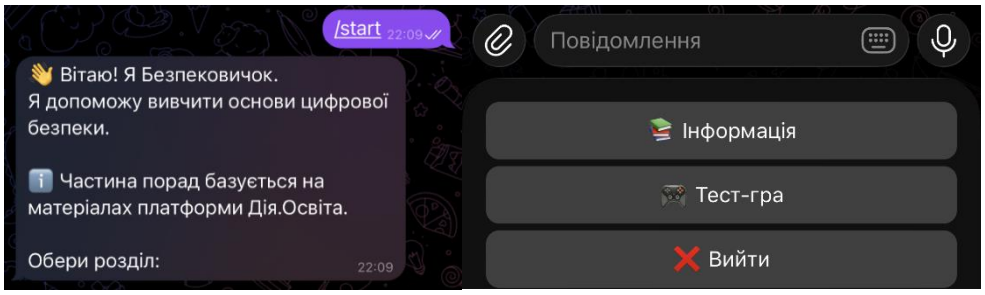
– обговорення освітнього серіалу.

2. Змістово-практичний (2–3 тиждень):

– проходження курсів («Цифрова безпека», «Кібергігієна»);

– виконання практичних завдань;

– робота з чат-ботом «Безпековичок».



3. Підсумково-рефлексивний (4 тиждень):

– виконання тестів;

– написання есе;

– самооцінювання результатів.

АНОТАЦІЯ

Актуальність. В умовах стрімкої цифровізації українського суспільства, посиленої повномасштабним вторгненням росії та масштабними кібератаками на державні й освітні установи, проблема формування компетентностей з цифрової безпеки набуває першочергового значення. Особливої актуальності вона набуває для майбутніх фахівців з професійної освіти, які покликані не лише самостійно протидіяти цифровим загрозам, а й формувати відповідну культуру безпеки у своїх здобувачів.

Мета дослідження – теоретично обґрунтувати та експериментально перевірити психолого-педагогічні умови використання платформи «Дія.Освіта» у формуванні компетентностей з цифрової безпеки у майбутніх фахівців з професійної освіти.

Методика дослідження. У роботі використано теоретичні методи (аналіз, синтез, узагальнення, моделювання), емпіричні (педагогічний експеримент, тестування, анкетування, спостереження, самооцінка) та статистичні (критерій χ^2 Пірсона для підтвердження однорідності груп; критерій Манна-Уітні для перевірки статистичної значущості змін після формувального експерименту).

Визначено й обґрунтовано три психолого-педагогічні умови: мотивація здобувачів до безпечної поведінки в цифровому середовищі; дотримання академічної доброчесності й етичних норм використання цифрових ресурсів; впровадження авторської методики на основі платформи «Дія.Освіта» та чат-бота «Безпековичок». Розроблено модель та авторський чат-бот у месенджері Telegram, що поєднує інформаційний модуль із тематичними блоками з цифрової безпеки та ігровий модуль на основі гейміфікації.

Результати. Проведений педагогічний експеримент підтвердив ефективність запропонованої методики: після формувального етапу в експериментальній групі частка студентів з високим рівнем сформованості компетентностей зросла до 45% проти 18% у контрольній, а статистично

значуща різниця між групами (U = 320,0; p = 0,026) засвідчує достовірність отриманих результатів.

Результати дослідження можуть бути впроваджені в навчальний процес закладів вищої та фахової передвищої освіти за спеціальністю «Професійна освіта» для системного формування компетентностей з цифрової безпеки здобувачів.

Ключові слова: цифрова безпека, компетентності, «Дія.Освіта», чат- бот, педагогічний експеримент, психолого-педагогічні умови, професійна освіта.