МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КРИВОРІЗЬКИЙ ДЕРЖАВНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ
Фізико-математичний факультет
Кафедра інформатики та прикладної математики

МЕТОДИКА ДИФЕРЕНЦІЙОВАНОГО НАВЧАННЯ ВИБІРКОВОГО МОДУЛЯ "ІНФОРМАЦІЙНА БЕЗПЕКА" УЧНІВ ЛІЦЕЇВ

Кваліфікаційна робота студента групи Ім-24
ступінь вищої освіти «магістр»
спеціальності 014 Середня освіта (Інформатика)
Колгатіна Андрія Олександровича

Керівник: доктор педагогічних наук, професор,
старший дослідник
Семеріков Сергій Олексійович

Кривий Ріг – 2025

ЗАПЕВНЕННЯ

Я, Колгатін Андрій Олександрович, розумію і підтримую політику Криворізького державного педагогічного університету з академічної доброчесності. Запевняю, що ця кваліфікаційна робота виконана самостійно, не містить академічного плагіату, фабрикації, фальсифікації. Я не надавав і не одержував недозволену допомогу під час підготовки цієї роботи. Використання ідей, результатів і текстів інших авторів мають покликання на відповідне джерело.

Із чинним Положенням про запобігання та виявлення академічного плагіату в роботах здобувачів вищої освіти Криворізького державного педагогічного університету ознайомлений. Чітко усвідомлюю, що в разі виявлення у кваліфікаційній роботі порушення академічної доброчесності робота не допускається до захисту або оцінюється незадовільно.

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дослідження. Стрімкий розвиток цифрових технологій та їх інтеграція в усі сфери життя суспільства зумовлюють необхідність формування у підростаючого покоління компетентностей з інформаційної безпеки. Сучасні старшокласники активно використовують цифрові пристрої та інтернет-сервіси, однак, як свідчать дослідження, їхні знання про кібербезпеку залишаються на недостатньому рівні [20]. Проблема навчання основ інформаційної безпеки учнів загальноосвітніх закладів набуває особливої актуальності в умовах зростання кіберзагроз та поширення цифрового шахрайства [13].

Реформування системи освіти в Україні, зокрема впровадження концепції Нової української школи [15], передбачає оновлення змісту навчання та застосування сучасних педагогічних технологій. Державний стандарт повної загальної середньої освіти [28] визначає інформаційно-комунікаційну компетентність як одну з ключових, що включає безпечне та відповідальне використання цифрових технологій. Модельні навчальні програми з інформатики [30] передбачають вивчення питань інформаційної безпеки, однак обсяг навчального часу, відведеного на цю тематику, є обмеженим.

Водночас, наукові дослідження останніх років засвідчують необхідність розробки спеціалізованих курсів та модулів з кібербезпеки для учнів середньої школи [6; 8]. Ефективне навчання кібербезпеки потребує інноваційних підходів, що враховують вікові та індивідуальні особливості учнів [9]. Зарубіжний досвід свідчить про успішне впровадження інтерактивних методів та практико-орієнтованих завдань у навчанні інформаційної безпеки [1; 19].

Диференційований підхід до навчання є одним із провідних напрямів сучасної педагогіки, що забезпечує можливість урахування індивідуальних особливостей учнів [17]. Українські науковці активно досліджують проблеми диференціації навчання в контексті реформування освіти [34; 35]. Диференційоване навчання розглядається як комплексна система, що передбачає визначення складності та темпу навчання відповідно до індивідуальних особливостей учнів, застосування відповідних форм, методів і засобів навчання [33]. Реалізація диференційованого навчання в компетентнісній

освіті сприяє підвищенню якості освітнього процесу [21].

Проведений аналіз наукової літератури та освітньої практики виявив низку суттєвих суперечностей:

- між зростаючими вимогами суспільства до рівня сформованості компетентностей з інформаційної безпеки в учнів та реальним рівнем підготовки випускників ліцеїв;
- між потенціалом диференційованого навчання у формуванні компетентностей з інформаційної безпеки та недосконалістю існуючих методичних інструментів його реалізації;
- між необхідністю впровадження сучасних підходів до навчання інформаційної безпеки учнів ліцеїв та обмеженістю методичного забезпечення вибіркових модулів з даної тематики.

Об'єкт дослідження – освітній процес у ліцеях.

Предмет дослідження – диференційоване навчання вибіркового модулю "Інформаційна безпека" учнів ліцеїв.

Мета дослідження – полягає в теоретичному обґрунтуванні та розробці методичних засад диференційованого навчання вибіркового модулю "Інформаційна безпека" учнів ліцею.

Відповідно до мети визначено такі основні **завдання дослідження**:

1. Дослідити сучасні підходи до навчання інформаційної безпеки учнів ліцеїв.
2. Узагальнити та систематизувати теоретичні засади диференційованого навчання.
3. Розробити завдання для диференційованого навчання модулю "Інформаційна безпека" учнів ліцею.
4. Розробити методичні рекомендації щодо впровадження диференційованого навчання учнів ліцеїв під час вивчення вибірковому модулю "Інформаційна безпека".

Методи дослідження:

- аналіз науково-методичної літератури з проблем диференційованого навчання учнів ліцеїв;
- систематизація педагогічного досвіду диференційованого навчання;
- теоретичне обґрунтування методичних підходів до диференційованого навчання вибіркового модулю “Інформаційна безпека”.

Новизна результатів дослідження полягає в тому, що вперше:

- узагальнено та систематизовано інформацію щодо підходів до диференційованого навчання учнів ліцеїв;
- обгрунтовано змістовне наповнення вибіркового модулю “Інформаційна безпека” для учнів ліцеїв;
- розроблені диференційовані завдання до вибіркового модуля “Інформаційна безпека” для учнів ліцеїв;
- запропоновані методичні рекомендації до вибіркового модуля “Інформаційна безпека” для учнів ліцеїв;

Практичне значення результатів дослідження полягає в тому, що розроблені завдання для проведення занять з вибіркового модулю “Інформаційна безпека” можуть бути використані в освітньому процесі закладів загальної середньої та профільної освіти, а також здобувачами вищої педагогічної освіти під час вивчення методичних навчальних дисциплін, методистами та вчителями в системі підвищення кваліфікації та перепідготовки педагогічних працівників.

Структура та обсяг роботи. Робота складається зі вступу, трьох розділів, висновків до них, загальних висновків, списку використаних джерел (35 найменувань), 1 додатку. Робота містить 15 таблиць та 3 рисунки. Загальний обсяг роботи – 74 сторінки.

РОЗДІЛ 1
ТЕОРІЯ Й ПРАКТИКА ДИФЕРЕНЦІЙОВАНОГО НАВЧАННЯ УЧНІВ ЛІЦЕЇВ

1.1. Навчання учнів інформаційної безпеки як педагогічна проблема

Стрімкий розвиток інформаційних технологій та їх глибока інтеграція в усі сфери життя сучасного суспільства актуалізує проблему навчання учнів закладів загальної середньої освіти основам інформаційної безпеки. Цифрова трансформація освітнього процесу, масовий перехід на дистанційне навчання під час пандемії COVID-19, а також зростання кіберзагроз створюють нові виклики для педагогічної спільноти.

З метою визначення сучасного стану досліджень у галузі навчання інформаційній безпеці учнів було проведено комплексний бібліографічний аналіз наукових публікацій, представлених у науково-метричній базі Scopus. Пошук здійснювався за запитом: *("learning" OR "education") AND ("information security" OR "Cybersecurity") AND "school"*, що дав змогу ідентифікувати 585 релевантних публікацій.

Для аналізу та візуалізації бібліографічних даних було використано програмне забезпечення VOSviewer /citeVOSviewer, яке надає інструменти для створення карт відповідності ключових слів та виявляти тематичні кластери в масиві наукових публікацій. Аналіз проводився за такими параметрами:

- тип аналізу: відповідність ключових слів (co-occurrence);
- одиниця аналізу: усі ключові слова (all keywords);
- метод підрахунку: повний підрахунок (full counting);
- мінімальна кількість зустрічей ключового слова: 10.

З початкових 3407 ключових слів після застосування порогового значення було відібрано 71 термін, які сформували основу для кластерного

аналізу.

Аналіз географічного розподілу публікацій виявив домінування англомовних країн у дослідженнях з навчання інформаційній безпеці в школах. Країни, які є лідерами за кількістю публікацій, зазначені в таблиці 1.1

Таблиця 1.1

Географічний розподіл публікацій з навчання інформаційній безпеці.

Країна	**Документи**	**Цитування**	**Сила зв'язків**
США	215	1285	17
Австралія	10	102	11
Велика Британія	24	238	9
Канада	7	54	7
Південна Африка	14	80	7
Німеччина	8	23	6
Індія	9	71	6

Кластерний аналіз дав змогу виділити п'ять основних тематичних напрямів досліджень у галузі навчання інформаційній безпеці учнів (рис. 1.1):

- **кластер 1: "Інформаційні технології та їхній вплив на суспільство"** (червоний) – об'єднує дослідження, присвячені впливу сучасних технологій на освітній процес та суспільство в цілому. Ключовими термінами є: *artificial intelligence* (середній рік публікації – 2021.4), *machine learning* (2022.1), *e-learning* (52 появи), *data privacy*, *virtual reality*, *social media*. Високий середній рік публікацій свідчить про актуальність та новизну досліджень у цій сфері;

- **кластер 2: "Освіта та обізнаність у сфері інформаційної безпеки"** (зелений) – наукові праці, що зосереджені на формальній освіті та підвищенні обізнаності в питаннях інформаційної безпеки. Основні терміни: *information security awareness* (45 зв'язків), *information security education* (12 появ), *security of data* (99 появ, 425 зв'язків), *authentication*, *higher education*. Значна кількість зв'язків підкреслює центральну роль цієї тематики в загальному масиві досліджень;

- **кластер 3: "Навчання кібербезпеці в освітніх закладах"** (синій) – найпотужніший кластер за кількістю зв'язків, присвячений

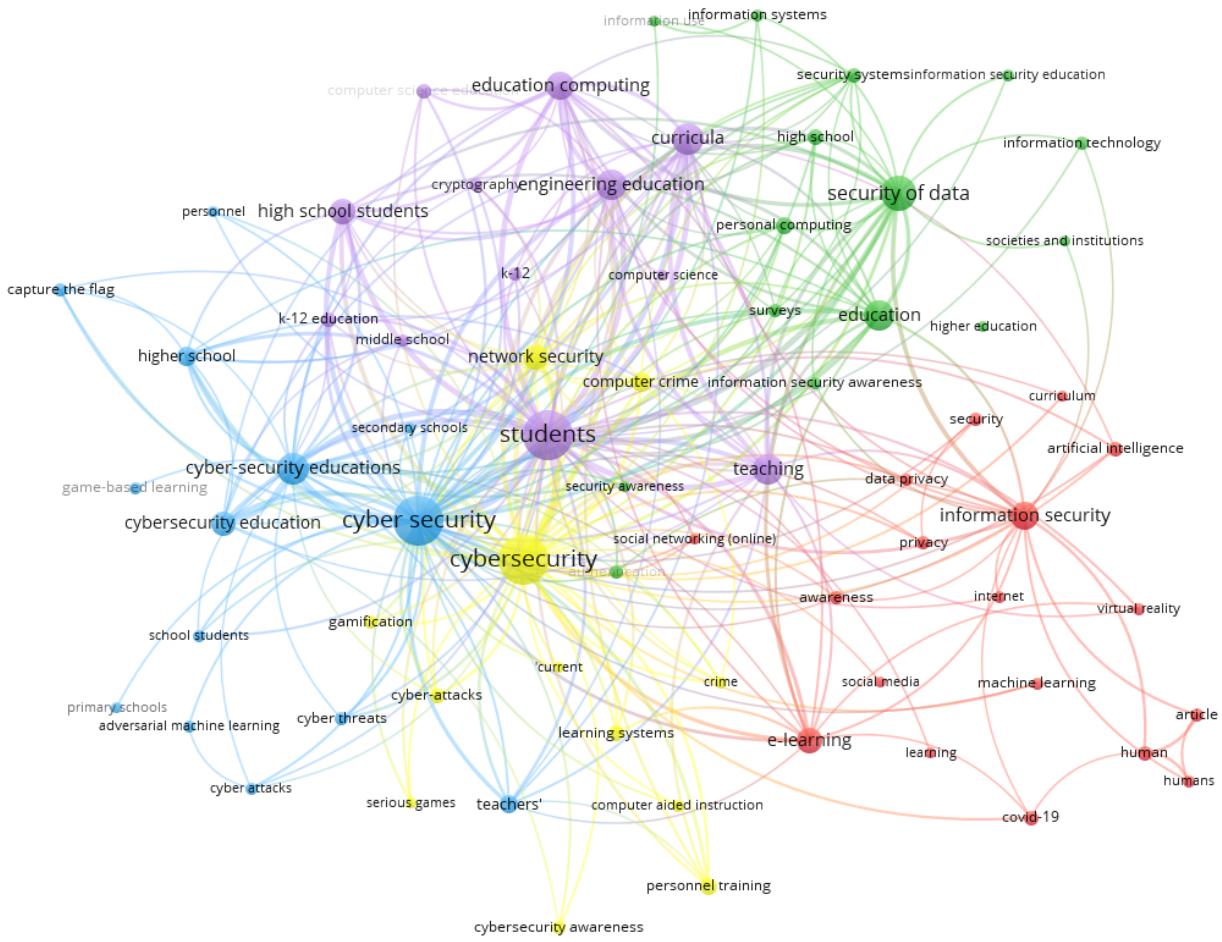

Рис. 1.1. Кластерний аналіз за тематичними напрямами досліджень

практичним аспектам навчання кібербезпеці. Провідні терміни: *cyber security* (195 поява, 1008 зв'язків), *cybersecurity education* (49 поява), *capture the flag*, *game-based learning*. Присутність ігрових методів навчання вказує на інноваційні підходи до викладання кібербезпеки;

– **кластер 4: "Тренування та освіта персоналу в галузі кібербезпеки"** (жовтий) – охоплює питання професійної підготовки та підвищення кваліфікації. Ключові терміни: *cybersecurity* (195 поява, 862 зв'язки), *computer crime* (середнє цитування – 14.3), *personnel training*, *serious games*, *gamification*. Високі показники цитування свідчать про значущість тематики в науковій спільноті;

– **кластер 5: "Освіта в комп'ютерних науках та інженерії"** (фіолетовий) – представляє академічні аспекти комп'ютерної освіти. Основні терміни: *curricula* (76 поява), *students* (190 поява, 1008 зв'язків),

computer science education, *engineering education*, *k-12 education*. Високі показники для терміну "students" підкреслюють студентоцентрований підхід у дослідженнях.

Аналіз хронологічного розподілу публікацій виявив, що активне дослідження проблем навчання інформаційній безпеці в закладах загальної середньої освіти розпочалося у 2021–2022 роках. Це пов'язано з масовим переходом на дистанційне навчання під час пандемії COVID-19 та зростанням кіберзагроз в освітньому середовищі.

Сучасні дослідження демонструють зміщення акценту від традиційних методів навчання до інноваційних підходів:

- *гейміфікація навчального процесу* – використання ігрових механік для підвищення мотивації та залученості учнів. Терміни "gamification", "serious games", "game-based learning" мають високі показники цитування та актуальності;
- *змагання CTF (Capture The Flag)* – практично-орієнтований метод навчання через вирішення реальних задач з кібербезпеки в змагальному форматі. Середній рік публікацій – 2022.8, що свідчить про новизну підходу;
- *персоналізоване навчання* – адаптація навчального контенту до індивідуальних потреб та рівня підготовки учнів з використанням технологій штучного інтелекту та машинного навчання;
- **симуляційне навчання** – створення безпечного віртуального середовища для відпрацювання навичок протидії кіберзагрозам.

Аналіз зв'язків між кластерами виявив високий рівень міждисциплінарності досліджень. Терміни "cyber-security educations" та "cybersecurity education" з'являються одночасно в кількох кластерах, що свідчить про інтеграцію технічних, педагогічних та соціальних аспектів проблеми. На основі проведеного аналізу можна виділити особливості навчання інформаційній безпеці:

– *динамічність предметної області* – швидка зміна технологій та загроз вимагає постійного оновлення навчальних програм та методичних матеріалів;

– *обмежена кількість кваліфікованих педагогічних кадрів* – необхідність підготовки вчителів, які володіють як технічними знаннями, так і педагогічними методиками викладання кібербезпеки;

– *вікова диференціація* – необхідність розробки навчальних програм для різних вікових груп;

– **практична спрямованість** – забезпечення балансу між теоретичними знаннями та практичними навичками безпечної поведінки в цифровому середовищі.

Проведений бібліографічний аналіз свідчить про зростання наукового інтересу до проблем навчання учнів інформаційній безпеці. Виявлені тематичні кластери демонструють комплексний характер проблеми, що охоплює технологічні, педагогічні, психологічні та соціальні аспекти.

Домінування термінів “cyber security” (195 поява) та “students” (190 поява) з найвищими показниками зв’язків підкреслює центральну роль учнівської аудиторії в дослідженнях кібербезпеки. Поява інноваційних методів навчання, таких як гейміфікація, CTF-змагання та симуляційне навчання, свідчить про пошук ефективних педагогічних рішень для формування культури кібербезпеки в молодого покоління.

Перспективними напрямами подальших досліджень є розробка диференційованих методик навчання інформаційній безпеці з урахуванням вікових особливостей учнів, створення інтегрованих навчальних програм, що поєднують технічні та гуманітарні аспекти кібербезпеки, а також підготовка педагогічних кадрів для ефективного викладання цієї дисципліни в закладах загальної середньої освіти.

1.2. Диференційоване навчання в середній освіті

Поняття диференційованого навчання розвивалося від простого групування учнів до гнучкого пристосування педагогічних елементів до їхніх

потреб. Класичною науковою працею в галузі диференційованого навчання, яка зазначає сучасний погляд міжнародної освітянської спільноти на проблему, є монографія Керол Енн Томлінсон "Як диференціювати навчання в класах зі змішаними здібностями" [17]. Автор розуміє диференційоване навчання як "упорядкування викладання для задоволення індивідуальних потреб" учнів [17]. Це означає, що диференціація – це проактивна, якісна та орієнтована на учня філософія, а не просто набір хаотичних дій. Виділяють чотири основні елементи навчального процесу, які вчитель може адаптувати для задоволення індивідуальних потреб учнів [17]:

1) зміст (content) – різні шляхи, якими учні отримують доступ до ключових концепцій та інформації – використання різних матеріалів (різного рівня складності), варіативність джерел (відео, аудіо, текст);

2) процес (process) – різні види діяльності, якими учні опрацьовують і осмислюють ідеї – робота в різних групах (за рівнем готовності, інтересами), надання вибору завдань, різні стилі навчання (візуальний, аудіальний, кінестетичний);

3) продукт (product) – різні шляхи, якими учні демонструють своє розуміння та знання – можливість створити есе, презентацію, постер, макет або усний звіт для підсумкової оцінки;

4) середовище (environment) – створення сприятливої та гнучкої атмосфери в класі, яка підтримує індивідуальні потреби – гнучке розташування меблів, встановлення правил роботи в групах, створення теплого клімату співпраці.

Згідно [17] адаптація (диференціація) повинна базуватися на трьох основних характеристиках кожного учня:

1) рівень готовності (readiness) – рівень знань, навичок та розуміння, які учень має на даний момент для роботи з конкретним навчальним матеріалом: диференціація за готовністю регулює складність та темп;

2) інтереси (interests) – теми, об'єкти або сфери, які викликають у дитини природну цікавість та бажання навчатися: диференціація за інтересами підвищує мотивацію та залученість;

3) профіль навчання (learning profile) – переваги учня щодо стилю навчання (наприклад, візуальний, кінестетичний), групової роботи, та впливу середовища: диференціація за профілем навчання регулює спосіб викладання.

Слід наголосити, що у центрі моделі К. Томлінсон знаходиться учень і його успіх, що досягається завдяки гнучкості навчального процесу.

Термінологічний апарат стосовно диференційованого навчання детально пропрацьований у вітчизняних науково-педагогічних дослідженнях [21; 33—35].

Для визначення сучасних вітчизняних тенденцій у галузі диференційованого навчання в закладах загальної середньої освіти було побудовано запит на сайті проєкту "Ініціатива з відкритого доступу до українського наукового контенту (OUCI)", що забезпечує доступ до бібліографічних даних наукових публікацій, які використовують сервіс Cited-by від Crossref та підтримують Initiative for Open Citations:

```
https://ouci.dntb.gov.ua/?q=диференційоване+навчання
&f_pub_type=journal-article
&f_pub_year=2025%7C2023%7C2024%7C2021%7C2022
&f_specialty=014
```

Згідно цього запиту розглядаємо статті в наукових журналах, які стосуються диференційованого навчання, відповідають спеціальності 014 (Середня освіта) та опубліковані в період із 2021 по 2025 рік. Особливістю побудови запитів на сайті є автоматичне варіювання словоформ, що значно полегшує пошук українською мовою. Відповідно до дослідницького завдання, а саме визначення актуальних підходів до організації диференційованого навчання в закладах середньої освіти, було сформульовано умови включення публікацій до розгляду:

1) наявність інформації про способи організації диференційованого навчання;

2) наявність прикладів методики диференційованого навчання;

3) наявність інформації про психолого-педагогічні умови диференціації навчання.

Умовами виключення є:

1) невідповідність матеріалу середній освіті;

2) відсутність інформації про диференційоване навчання щодо формування знань і розумових умінь;

3) повторення даних попередніх публікацій;

4) відсутність повного тексту статті у відкритому доступі.

За запитом до бази даних на 31 жовтня 2025 року було отримано 22 джерела. Результати попереднього аналізу зазначених публікацій щодо умов включення до огляду та умов виключення з огляду подано в таблиці 1.2.

Таблиця 1.2

Умови включення знайдених публікацій до розгляду.

Назва, doi	**Умови включення до огляду**	**Умови виключення з огляду**	**Висновок щодо включення до огляду**
1	2	3	4
Theoretical principles of differentiated work of primary school students: main aspects, 10.32626/2309-9763.2020-29-157-167	1 – розглядається диференціація навчальної діяльності	1 – спрямовано на початкову школу	Ні
Диференціація та індивідуалізація освіти в сучасному ЗВО: можливості інформаційного середовища, 10.32689/ maup.ped.2024.3.2	1 – розглядається диференціація навчальної діяльності	1 – спрямовано на вищу освіту	Ні
Current state of training of future teachers professional training for innovative pedagogical activities in educational theory, 10.31376/2410-0897-2024-2-55-10-19	-	1 – спрямовано на вищу освіту	Ні
Особливості підготовки майбутніх учителів природничих спеціальностей на засадах диференціації та індивідуалізації навчання, 10.24919/2308-4634.2024.301830	1 – розглядається диференціація навчальної діяльності	1 – спрямовано на вищу освіту	Ні

Продовження табл. 1.2

1	2	3	4
До проблеми оцінювання навчальних досягнень учнів гімназій у компетентнісному вимірі, 10.32405/2411-1309-2024-32-66-82	-	2 – не містить інформації про диференційоване навчання. Містить вимоги вимоги до оцінювання, які диференційовано	Ні
Методичні підходи, реалізовані у підручнику з математики для учнів 6 класів (за підручником «Математика. 6 клас» Світлани Скворцової та Катерини Нєдялкової), 10.32405/2411-1317-2023-3-217-226	1 + 2 – Тренувальні завдання диференційовано за трьома рівнями складності. Проєктне навчання втілюється через виконання школярами проєктів різної тематики: «Поглиначи часу», «Волонтерська діяльність», «Подорож річками України», «Український борщ», «Золотий перетин», «Подорож повітряним океаном», «Зелений одяг планети», «Світ професій і математика».	-	Так [31]
Значення штучного інтелекту у вивченні іноземних мов, 10.26661/2786-5622-2024-1-03	1 – цифровизація (ШІ) робіть процес здобуття знань персоналізованим і диференційованим	1 – орієнтовано на вищу школу	Ні
Шкільний підручник з української літератури як інструмент формування медіаграмотності сучасних учнів, 10.15330/obrii.59.2.49-54	-	2 – у статті тільки згадується, що підручник має рубрику “диференційовані завдання” проте суть цих завдань і принципи диференціації не повідомлюються	Ні

Продовження табл. 1.2

1	2	3	4
Потенціал підручника «досліджуємо історію і суспільство» у формуванні екологічної компетентності учнів 6 класу, 10.32405/2411-1309-2023-31-211-222	-	2 – автори зазначають, що “Зміст завдань дає змогу використовувати їх диференційовано, організувати самостійну / парну / групову роботу учнів, досягати очікуваних результатів навчання”, проте принципи диференціації не наводяться, приклади завдань не супроводжуються коментарями, в чому може полягати диференціація	Ні
Проблеми та перспективи розвитку інклюзивної освіти в умовах реформування освітньої галузі України, 10.33216/2220-6310-2021-102-3-85-94	1 – впровадження диференційованих методів та технологій навчання особистісно-орієнтованого спрямування із урахуванням індивідуальних особливостей дитини — інклюзивна освіта	-	Так [25]
Роль електронного портфоліо вчителя як освітнього ресурсу в навчально-методичному забезпеченні процесу подолання освітніх втрат учнів, 10.32405/2411-1309-2024-32-299-305	1 – учитель розробляє диференційовані завдання, які допоможуть учням поступово нарощувати рівень своєї освітньої самостійності	-	Так [32]
Formation of an integrated course for the 5–6th grades as a component of integral natural science education, 10.32626/2309-9763.2020-29-171-186	1 – диференційоване вивчення окремих предметів	-	Так [26]
Formation of an integrated course for the 5–6th grades as a component of integral natural science education, 10.32405/2411-1317-2021-4-65-76	-	2 – стаття присвячена цифрової трансформації, диференціація тільки згадується	Ні
Directions for optimization of the corrective-developmental process in speech therapy groups, 10.31494/2412-9208-2023-1-3-183-193	1 – диференційована роботи під час фронтального корекційно-розвиткового навчання в логопедії	1 – діти дошкольного віку	Ні

Продовження табл. 1.2

1	2	3	4
Content, forms and methods of work on the of physical education of primary school students in the socio-cultural environment, 10.31376/2410-0897-2023-2-52-248-254	-	1 – початкова школа	Ні
Інформаційно-комунікаційні технології як засіб формування лінгводидактичної компетентності майбутніх учителів початкових класів, 10.33407/itlt.v82i2.3288	-	1 – вища школа	Ні
Strategie of social adaptation of preschool students with speech disorders in the conditions of inclusive education, 10.31494/2412-9208-2023-1-3-194-202	-	1 – дошкільна освіта	Ні
Морфофункціональні показники учнів як чинник диференціації корекційно-педагогічного підходу в ортопедагогіці, 10.31865/2077-1827.2(108) 2025.340168	-	2 – розглядаються показники учнів середнього шкільного віку з незначними порушеннями опорно-рухового апарату як ключовий чинник диференціації корекційно-педагогічного підходу в ортопедагогіці. Мова йде про формування опорно-рухового апарату, а не про формування системи знань та розумових умінь	Ні
Теоретичні аспекти використання педагогічних інновацій у післядипломній педагогічній освіті, 10.26661/2786-5622-2023-1-19	-	2 – диференціоване навчання тільки згадується	Ні
Перспективи комплексного використання засобів спортивних ігор у фізичному вихованні учнів початкових класів закладів загальної середньої освіти, 10.32782/olimpspu/2024.1.9	-	1 – початкова школа	Ні
Міждисциплі-нарний контент понять «інтенція», «мовленнєва інтенція» у логокорекційних системах сучасної логопедії, 10.31392/npu-nc.series 19.2023.44.09	-	1 – діти із тяжкими порушеннями мовлення	Ні

Продовження табл. 1.2

1	2	3	4
Особливості організації інклюзивного фізичного виховання в умовах нової української школи, 10.24195/ olympicus/2025-2.19		2 – автори зазначають, що інклюзивне фізичне виховання вимагає застосування диференційованих вправ та адаптованого обладнання. Отже мова не йде про формування знань та розумових умінь	Ні

За результатами проведеного аналізу можна зробити висновок, що попри значного інтересу до диференційованого навчання акцент останніх наукових праць із цього напряму більше спрямований на фізичне виховання, початкову та вищу школу. Щодо середньої освіти, то маємо зазначити інтерес до інклюзивного навчання та диференційованого підходу. Так у праці [25] зазначається важливість «... впровадження диференційованих методів та технологій навчання особистісно-орієнтованого спрямування із урахуванням індивідуальних особливостей дитини». Проте конкретних рекомендацій про особливості диференціації відповідного навчального матеріалу або процесу та підходи до діагностики з метою рекомендування того чи іншого матеріалу не наводяться – автори закликають до активізації досліджень у цьому напрямі.

Як напрям диференціації навчання С. Трубачева, Т. Мішеніна, О. Коник розглядають наповнення портфоліо вчителя: «Важливою складовою портфоліо може бути постійно оновлюваний розділ для учнів, з диференційованими завданнями для вивчення найбільш актуального предметного матеріалу, який допоможе учням у подоланні освітніх втрат ...» [32]. На думку авторів, диференційовані завдання мають сприяти підвищенню самостійності учнів. Отже напрямом диференціації є характер та детальність інструкцій, які отримує учень [32]. Автори, також, пов'язують рівень самостійності із рівнем розумової діяльності, яку мають здійснити учні під час виконання завдань. Низькому рівню самостійності відповідають завдання переважно репродуктивного характеру, «завдання для учнів із середнім рівнем самостійності повинні мати продуктивний характер з додаванням опорних схем до їх виконання» [32]. Для визначення рівня самостійності учнів автори пропонує такі показники: планування на-

вчальної діяльності, виконавча робота, уміння логічно аналізувати та систематизувати навчальний матеріал, уміння піддавати рефлексії шлях виконання завдання та отримані результати, уміння працювати з електронними освітніми платформами та додатками [32]. Маємо зазначити, що проблему управління самостійною роботою було розглянуто детальніше у працях Л. Білоусової і Л. Колгатіної [22]. А саме, окрім диференціації інструкцій щодо постановки завдань було підкреслено важливість диференціації допомоги в процесі виконання завдань учнями на всіх етапах від постановки завдання до аналізу результатів і підготовки звіту, а також, диференціації середовища, в якому виконується завдання (наявність та ступінь структурованості ресурсів, потрібних для виконання завдання) [22]. Такий підхід дає змогу навчати учнів із низьким рівнем самостійності виконувати завдання дослідницького характеру через поступовий перехід від прямого управління їх самостійною роботою до співуправління, побічного управління, самоуправління [3].

Т. Засєкіна зазначає необхідність диференціації під час побудови системи природничої освіти для учнів 5-6 класів [26]. Авторка пропонує розроблення пропедевтичного природознавчого курсу, який має бути опорою для подальшого диференційованого вивчення деяких природничих предметів, що відтворює класичну логіку предметного змісту природничої освіти [26]. Отже, висновком для нашого дослідження є необхідність детального аналізу програм дисциплін природничого циклу, на які має спиратися матеріал вибіркового модуля «Інформаційна безпека».

С. Скворцова й К. Нєдялкова, автори методичної системи [31], яку покладено ними в основу підручника з математики для учнів 6 класів, спираються на ознаки когнітивних процесів сучасних шестикласників, які було визначено шляхом опитування вчителів України [5; 31]:

1) учні не сприймають великі за обсягом тексти, матеріал сприймається ними фрагментарно;

2) діти мислять окремими думками, що логічно не пов'язані одна з одною, не намагаються систематизувати й узагальнити матеріал; у них з'являється така особливість мислення, як кліп – фрагментація;

3) в учнів спостерігається поверхове читання текстів – початок та кінець,

а середина – по діагоналі; знижується здатність до аналізу тексту – виділення головного, виокремлення зв'язків між елементами змісту, вони не можуть осягнути зв'язок між фактами і поняттями, але створюється ілюзія їх пізнання і розуміння;

4) школярі мислять зоровими образами, асоціаціями різного роду; в них переважає зорове сприйняття інформації через її подання у вигляді схем, картинок, відеозображень; наявність будь-якої інформації в інтернеті створює ілюзію в школярів, що запам'ятовувати її немає необхідності;

5) кліпове мислення дозволяє людині запам'ятовувати великий обсяг інформації на основі зорових образів, не сприймаючи її зміст;

6) учні одночасно виконують кілька справ, не зосереджуючись на жодній з них – багатозадачність.

Враховуючи зазначені особливості когнітивного стилю сучасних школярів, автори [31] пропонують підводити учнів до певних теоретичних узагальнень через опанування системи навчальних завдань і особливо визначають навчальні проєкти, тематика яких безпосередньо пов'язана зі змістом навчального матеріалу. Диференціацію автори передбачають через завдання, які спираються на різні рівні розумової активності: "тренувальні вправи структуровано за трьома рівнями складності: обов'язкові завдання, позначені зеленим пазликом, дослідницькі – жовтим, а червоним пазликом позначено завдання з логічним навантаженням" [31]. Важливим висновком, який навіюють автори статті (і відповідного підручника) є зв'язок завдань із життєвими ситуаціями, особливості аналізу яких сприяють формуванню підприємливості й фінансової грамотності, громадянських й соціальних компетентностей [31]. "Система навчальних завдань кожного уроку передбачає навчальне дослідження, яке вимагає зіставлення відомої учням умови із дещо зміненою і визначення впливу відмінності на спосіб міркування" [31].

Отже, проаналізовані підходи можна розглядати як прототип побудови методичної системи вибіркового модуля "Інформаційна безпека". Проведений огляд дає підстави для висновку, що автори сучасних педагогічних

досліджень зазначають негайну потребу в особистісної орієнтації навчальних завдань, проте практичні розробки описані тільки щодо диференціації рівня розумової діяльності, яку потрібно здійснити для виконання завдання. Потреба у врахуванні кола інтересів учнів зазначається авторами наукових статей, проте конкретні приклади такої диференціації не наводяться. Не вистачає, також, теоретичного аналізу щодо визначення напряму тематичної спрямованості завдань для тих чи інших учнів і підходів до забезпечення опанування обов'язкового матеріали в разі диференціації тематичної спрямованості завдань згідно інтересів учнів. Розвиток зазначених проблем складає новизну нашого підходу до побудову системи диференційованих навчальних завдань вибіркового модуля "Інформаційна безпека".

1.3. Приклади реалізації диференційованого навчання інформаційної безпеки

З метою пошуку прикладів завдань (диференційованих завдань) із інформаційної безпеки, які можуть бути запропоновані учням ліцею в межах вибіркового модуля було здійснено пошук згідно запиту "https://ouci.dntb.gov.ua/?q="Інформаційна безпека" завдання школа" на сайті проєкту "Ініціатива з відкритого доступу до українського наукового контенту (OUCI)". За запитом отримано 15 публікацій, серед яких тільки 2 присвячені навчанню старшокласників інформаційної безпеки. О. М. Спірін і В. Н. Ковальчук [13] зазначають надзвичайну важливість формування компетентності особистості старшокласника з інформаційної безпеки, культури інформаційної безпеки особистості та дисциплінованості користувача як складової комплексної системи забезпечення онлайн безпеки старшокласників у навчально-виховному процесі школи. Автори наводять дидактичні матеріали (слайди), посилання на тест, який пропонується застосовувати для перевірки знань, та домашнє завдання – створити безпечну електронну скриньку. Автори зазначають, що "кількість англомовних вебресурсів, присвячених цій проблематиці, налічує десятки тисяч, а кількість україномовних ресурсів не перевищує й десяти" [13]. Це було сказано в 2011 році. Як бачимо за результатами пошуку, ситуація не змінилась суттєво. Так, серед статей, які було знайдено за наведеним запитом, праця

Ю. Британ [23], яку присвячено англомовним комунікативним ситуаціям безпечного поводження в Інтернеті за ресурсами Британської Ради.

Аналіз україномовних сайтів дає цікаві матеріали, які містять тексти, відео щодо інформаційної безпеки, наприклад [24]. Практична складова навчання на цих ресурсах обмежується реєстрацією на певному сайті, переглядом та обговоренням відео, відповідями на запитання.

Отже, для подальшого пошуку прикладів завдань, які можуть бути запропоновані учням ліцеїв під час вивчення вибіркового модуля "Інформаційна безпека" було обрано наукометричну базу даних Scopus. Пошуковий запит було побудовано на підґрунті запиту бібліографічного аналізу з підрозділу 1.1. Додаткові обмеження було зазначено, щоб окреслити вікові особливості учнів та наявність у статті практичних завдань для учнів або певних видів активності. Пошук було обмежено за роком публікації (2020-2025) та наявністю відкритого доступу до повного тексту:

```
TITLE-ABS-KEY (
( ‘‘information security’’ OR ‘‘cybersecurity’’ )
AND ( learning OR studying OR teaching OR education )
AND ( ‘‘high school’’ OR college )
AND ( ‘‘laboratory work’’ OR assignment OR activity
OR ‘‘game-based learning’’ )
)
AND
PUBYEAR > 2019 AND PUBYEAR < 2027
AND ( LIMIT-TO ( LANGUAGE , ‘‘English’’ ) )
AND (
LIMIT-TO ( OA , ‘‘all’’ ) )
```

Маємо зазначити, що окрім учнів ліцеїв, що відповідає "high scool" в англомовних джерелах, до запиту внесено учнів коледжів "colledge". Це вносить певну неоднозначність, бо в Україні учні коледжів мають саме такий вік як і учні ліцеїв і отримують середню освіту разом із професійною освітою, проте в більшості іноземних країн коледжі розглядаються як вища освіта. Отже, немає сенсу нехтувати матеріалами, які використовуються в коледжах, проте ці матеріали мають бути окремо проаналізовані стосовно

доцільності їх використання саме для учнів ліцеїв. За результатами пошуку було отримано 24 джерела.

Відповідно до дослідницького завдання, а саме визначення прикладів побудови завдань із інформаційної безпеки для учнів ліцеїв, було сформульовано умови включення публікацій до розгляду:

1) наявність прикладів або детального опису практичних завдань із інформаційної безпеки для учнів;

2) наявність опису досвіду застосування практичних завдань із інформаційної безпеки у навчальному процесі учнів у межах середньої освіти.

Умовами виключення є:

1) невідповідність матеріалу середній освіті;

2) невідповідність матеріалу тематиці “Інформаційна безпека”;

3) повторення даних попередніх публікацій.

Результати попереднього аналізу зазначених публікацій щодо умов включення до огляду та умов виключення з огляду подано в таблиці 1.3.

Таблиця 1.3

Умови включення знайдених публікацій до розгляду.

Назва	**Умови включення до огляду**	**Умови виключення з огляду**	**Висновок щодо включення до огляду**
1	2	3	4
Perceptions of Daily and On-Demand HIV Pre-Exposure Prophylaxis and Digital Adherence-Support Needs Among Cisgender Men in Brazil: Qualitative Interview and Focus Group Study	-	1 – Статтю присвячено профілактиці ВІЧ серед дорослих	Ні

Продовження табл. 1.3

1	2	3	4
Teaching and learning cybersecurity for European youth by applying interactive technology and smart education	1 – Стаття представляє нову методологію навчання кібербезпеки для старшокласників (high school students). Нова навчальна програма пропонує інструменти для активного навчання, такі як інтерактивні відео, вікторини (quizzes), ігри (games) та живі приклади кіберзагроз. Навчальний контент був розроблений у вигляді 24 фіш (fiches), 12 з яких присвячені кібербезпеці, і включають практичні приклади для вчителя, такі як ігри, практичні вправи (hands-on exercises) та вікторини. 2 – Досліджено досвід застосування: вчителі відзначили, що чітко структурований контент фіш та готові запитання були дуже корисними. Студенти позитивно оцінили заняття після того, як вони спробували симульовану реальність, надану іграми.	-	Так [9]
Personalized Mathematics Teaching with The Support of AI Chatbots to Improve Mathematical Problem-Solving Competence for High School Students in Vietnam	-	2 – Основна тематика статті — персоналізоване навчання математики та AI-чатботи. Хоча в теоретичній моделі згадується важливість “безпеки та конфіденційності” (Security and Privacy) як механізму, що забезпечує безпеку та ефективність навчального процесу, тематика статті не є “Інформаційна безпека” як навчальний предмет чи набір практичних завдань.	Ні

Продовження табл. 1.3

1	2	3	4
Cybersecurity activities for education and curriculum design: A survey	1 – Стаття проводить систематичний огляд і класифікує практичні види діяльності та методики, які використовуються в кібербезпеці, що є основою для побудови завдань. До них належать: Hands-on Labs (Практичні лабораторії); Gamification (Гейміфікація) та Simulations (Симуляції); Capture the Flag (CTF) — змагальні формати, які імітують кібератаки та захист. Окремі розділи описують, які типи кібератак та захисних методів (наприклад, криптографія, інциденти, кібергігієна) мають бути включені до навчальних програм, зокрема, для K-12 (що охоплює середню освіту). 2 – Стаття охоплює всі рівні освіти, включаючи середню освіту (Secondary Education). Як оглядова робота, вона узагальнює досвід впровадження вищезазначених практичних заходів (ігор, CTF, лабораторій) в навчальні програми по всьому світу і пропонує концептуальну рамку для їхнього інтегрування у дизайн навчальних планів.	-	Так [6]
Remote Controlled Cyber: Toward Engaging and Educating a Diverse Cybersecurity Workforce	1 – Навчання базується на використанні IoT-пристроїв (наприклад, хакабельних дронів), що дозволяє учням виконувати hands-on завдання, такі як: тестування на проникнення (Penetration testing) – пошук вразливостей у реальних пристроях; аналіз мережевого трафіку та протоколів; вивчення кібербезпекових компетенцій через групові, а не лише змагальні формати. 2 – Автори зазначають, що змагання Capture-the-Flag (CTF) є основним каталізатором для залучення та рекрутингу студентів як середньої (high school), так і університетської освіти. Автори діляться своїм детальним дизайном, діяльністю, досвідом та отриманими уроками (detailed design, activities, experiences, and lessons learned), що є описом досвіду застосування.	-	Так [12]

Продовження табл. 1.3

1	2	3	4
Toward effective learning of cybersecurity: new curriculum agenda and learning methods	1 – Ця стаття пропонує конкретну освітню програму, розроблену для вивчення кібербезпеки та кіберзахисту на рівні середньої освіти на основі масштабного дослідження серед європейських шкіл. Навчальний контент включає: відеоплатформи та інтерактивні вікторини (quizzes); використання освітніх ігор (educational games) та серйозних ігор (serious games); Hands-on Lab Exercises (Практичні лабораторні вправи). Вона акцентує увагу на активному навчанні, що є основою для побудови практичних завдань. 2 – Стаття базується на вичерпному дослідженні, проведеному у 2021–2023 роках, із залученням середніх шкіл (high schools) у ЄС. На основі цього дослідження була розроблена та узгоджена методологія та освітній контент для учнів середньої школи у двох сферах: кіберзахист (cyber-safety) та кібербезпека (cybersecurity). Описаний досвід включає аналіз рівня знань вчителів та студентів, а також визначення найбільш ефективних методів подачі контенту.	-	Так [8]
Integrating Biotechnology Virtual Labs into Online Education Platforms: Balancing Information Security and Enhanced Learning Experiences	-	1 – спрямовано на вищу освіту 2 – Основна тематика статті — інтеграція віртуальних лабораторій з біотехнології в онлайн-освіту, а не інформаційна безпека як предмет навчання.	Ні

Продовження табл. 1.3

1	2	3	4
Learning CyberSecurity with Story-Driven CTF Challenges: CyberTrials 2023	1 – Програма включає 9 практичних навчальних модулів, що складаються із серії CTF-завдань (Capture the Flag). CTF-змагання є класичним і детально структурованим прикладом практичних завдань з кібербезпеки (наприклад, криптографія, веб-вразливості, реверс-інжиніринг, форензика). Ці завдання організовані в інноваційній, ігровій наративній рамці (game-based narrative-driven framework). 2 – Програма розроблена для італійських школярок середньої школи (Italian high school female students). В описі чітко зазначено, що програма була успішно впроваджена (successfully engaged students), а досвід оцінювався через онлайн-опитування для вивчення зв'язку між залученістю та навчальними результатами. Дослідження підтверджує важливість hands-on, гейміфікованих активностей (тобто, практичних завдань) для освіти з кібербезпеки.	Доступ до повнотекстового матеріалу потребує аутентифікації через університет	Так [16]
Fostering Online Digital Literacy and Information Security Competencies Among Secondary School Students Through Game-Based Learning: A Formative Evaluation	-	1 – Матеріал спрямований на організації охорони здоров'я та їхній персонал (workforce awareness and training), що є корпоративним або професійним навчанням, а не середньою освітою. 2 – Хоча тематика стосується кібербезпеки, вона вузько сфокусована на охороні здоров'я (health care–specific) та організаційному рівні, а не на навчальних програмах для учнів.	Ні

Продовження табл. 1.3

1	2	3	4
What do high school students know about the field of cyber security? A survey of perception and experiences	1 – Немає відповідності, конкретні завдання не наведені. Стаття досліджує, які фактори впливають на зацікавленість учнів кар'єрою в кібербезпеці. Серед ключових факторів, що сприяють цій зацікавленості, виділено "early exposure to cyber-related activities" (раннє залучення до кібер-заходів) та "hands-on workshops" (практичні семінари). 2 – Хоча стаття сама по собі є опитуванням (survey) і не деталізує конкретні практичні завдання, вона підтверджує важливість і наявність таких практичних завдань у формі "cyber clubs" (кібер-клубів), "competitions" (змагань) та "hands-on workshops" як інструментів, що впливають на учнів. Дослідження було проведене серед учнів середньої школи (high school students). Основна мета статті — проаналізувати "perceptions and experiences" (сприйняття та досвід) учнів щодо кібербезпеки. Результати базуються на досвіді учнів, які брали участь у "cyber clubs, competitions, and hands-on workshops", що є описом впливу такого досвіду на їхнє сприйняття.	-	Так [20]
A comprehensive application architecture for unlocking the potential of student feedback	-	1 – Спрямовано на вищу освіту 2 – Основна тематика статті — архітектура програмного забезпечення для збору відгуків, а не викладання інформаційної безпеки.	Ні
280 characters to the White House: predicting 2020 U.S. presidential elections from twitter data	-	1 – Стаття не спрямована на освіту 2 – Тематика статті полягає у прогнозуванні політичних подій	Ні

Продовження табл. 1.3

1	2	3	4
Beyond Black-Boxes: Teaching Complex Machine Learning Ideas through Scaffolded Interactive Activities	-	2 – Матеріал є цікавим, проте він спрямований на вивчення систем машинного навчання через дослідження	Ні
A neuro-fuzzy model for predicting and analyzing student graduation performance in computing programs	1 – розглядається диференціація навчальної діяльності	1 – Вища освіта. 2 – Стаття присвячена розробці нейро-нечіткої моделі (neuro-fuzzy model) для прогнозування середнього балу (GPA) студентів на момент випуску з програм інформаційних технологій (IT programs). Стаття зосереджена на академічній успішності та прогностичних моделях, а не на навчанні інформаційної безпеки	Ні
An Effective Instructional Design to Enhance Learning Outcomes of Information Security Course in Online Mode	1 – Матеріал статті спрямований для студентів бакалаврату (undergraduate), приклади практичних завдань дуже детальні, ці матеріали можуть бути корисні як додатковий матеріал для кращих учнів ліцеїв у межах диференційованого підходу, зокрема для організації дослідницької діяльності. Стаття детально описує використання широкого спектру практичних інструментів та симуляторів з кібербезпеки: Wireshark, CISCO Packet Tracer, Metasploit, DVWA (Damn Vulnerable Web Application), OSSEC, Lophtcrack, Cryptool, OpenSSL, Virtual Labs. Також описується “Learning By Doing” (Навчання через дію), яке включає завдання на програмування криптографічних алгоритмів (Hill Cipher, AES, RSA) та симуляції атак (Man in the middle attack, SQL Injection).	1 – Матеріал статті спрямовано на вищу освіту, проте окремі завдання і підходи можуть бути корисними для побудови навчальних завдань високого рівня складності в межах диференційованого підходу	Так [10]
Core curriculum in pathology for future Irish medical students	-	1 – Цільова аудиторія – студенти, майбутні медики 2 – Не спрямовано безпосередньо на інформаційну безпеку	Ні

Продовження табл. 1.3

1	2	3	4
Narrative Integrated Career Exploration Platform	-	1 – Матеріал розроблено та застосовано для студентів бакалаврату (вищої освіти). 2 – Основна тематика статті — профорієнтація та кар'єрне дослідження у сфері STEM, а не навчання інформаційної безпеки.	Ні
Incorporating active learning activities to the design and development of an undergraduate software and web security course	1 – Не відповідає: Основний фокус — на загальних активних методах навчання, а не на специфіці завдань з ІБ. Стаття описує використання активних навчальних заходів (active learning activities) для просування технічних та нетехнічних навичок у кібербезпеці. До них належать: think-pair-share, buzz group та roleplay (рольові ігри).	1 – Матеріал розроблено та застосовано для студентів бакалаврату (вищої освіти).	Ні
Culturally-sensitive Cybersecurity Awareness Program Design for Iranian High-school Students	1 – Програма, хоча й фокусується на підвищенні кібергігієни (cyber hygiene) та обізнаності (awareness), була розроблена з використанням моделі ADDIE. Вона націлена на підвищення знань про: використання безпечних паролів, ризики використання неперевірених VPN, та інші практичні аспекти захисту. Хоча в описі згадується, що учні надають перевагу лекціям, програма є практичною і спрямована на збільшення обізнаності та, відповідно, на поведінкові зміни (наприклад, використання безпечного пароля). 2 – Програма розроблена спеціально для іранських школярів середньої школи (Iranian High-school Students) віком 16-18 років. Автори описують: аналіз поточного рівня обізнаності 616 учнів; пілотне впровадження курсу; оцінку ефективності за допомогою попереднього та підсумкового тестування (pre-and post-test results), які підтвердили позитивний вплив програми.	-	Так [11]

Продовження табл. 1.3

1	2	3	4
Is a Significant Demographic Left Out of the Equation? An Overview of Possible Inequitable Access to Cybersecurity Educational Programs in the United States	1 – Стаття прямо зазначає, що кібербезпекова освіта пропонується в K-12 через “camps” (табори), “clubs” (клуби), “competitions” (змагання) та “standalone coursework” (окремі курси). Ці заходи є класичними формами практичних завдань (особливо змагання та клуби, які часто проводять hands-on activities). Хоча стаття є оглядом і не деталізує самі завдання, вона описує контекст, де ці завдання застосовуються у середній освіті. 2 – Дослідження сфокусоване на учнях середньої та старшої школи (Middle and high school student populations). Автори аналізують доступність (access) та залученість (engage) учнів до кібербезпекових навчальних програм. Досвід застосування оцінюється через аналіз існуючих ініціатив (табори, змагання, клуби) та пропонується методологія для подальшого опитування вчителів щодо їхнього досвіду впровадження.	-	Так [7]
An Integrated Cybernetic Awareness Strategy to Assess Cybersecurity Attitudes and Behaviours in School Context	1 – Описано план уроків та інструменти самодіагностики, сфокусовані на кібербезпеці. Крім того, стратегія включає веб-застосунок для самодіагностики (”self-diagnosis web application”) для оцінки навичок кібербезпеки. 2 – Дослідження було проведено серед учнів молодшої середньої школи (junior high school population) (6-ті та 9-ті класи), що охоплює вікову групу середньої освіти.		Так [1]
Applied Orientation and Interdisciplinary Integration as a Factor in Increasing Student Learning Motivation	-	1 – Досвід застосування стосується вищої освіти. 2 – Основна тематика завдань — фізика та математика.	Ні

Продовження табл. 1.3

1	2	3	4
Educational modules and research surveys on critical cybersecurity topics	1 – Стаття описує розробку чотирьох навчальних модулів з критичних тем кібербезпеки та пов'язаних з ними практичних лабораторних робіт (hands-on labs). Лабораторні роботи розроблені для підвищення "hands-on experiences with real-world cyber activities".	1 – Матеріал орієнтований на студентів коледжів (college-level), які в Україні відносять до професійної освіти, проте вік студентів коледжів відповідає віку студентів ліцеїв. Отже критерій виключення не застосовуємо.	Так [19]
Using Terminal Histories to Monitor Student Progress on Hands-on Exercises	1 – Стаття присвячена практичним вправам (hands-on exercises), які часто використовуються в класах з кібербезпеки. Вправи виконуються на мережевому тестовому стенді (network testbed) і є добре структурованими завданнями з кібербезпеки (наприклад, атака "людина посередині", SYN-флуд, DNS-атака).	1 – Матеріал розроблено та застосовано для студентів коледжів. Проте окремі завдання можуть бути корисними для організації диференційованого навчання, зокрема як завдання високого рівня. Отже критерій виключення не застосовуємо.	Так [18]

Отже, релевантними за умовами включення до розгляду та виключення з розгляду виявились праці [1], [12], [6], [8], [7], [9], [10], [11], [18], [20]. Дидактичні матеріали авторів можна умовно розділити на три категорії: практичні завдання з кібергігієни та моделювання поведінки; лабораторні та технічні вправи; активне та ігрове навчання.

Практичні завдання з кібергігієни та моделювання поведінки мають на меті підвищити рівень обізнаності та кібергігієни (cyber hygiene) учнів (16–18 років). Увага акцентується на формуванні правильної поведінки та реакції у цифровому середовищі:

– управління автентифікацією – дослідники включають безпеку паролів (password security) як обов'язковий розділ у програмі для для старшокласників (16-18 років) [11] і як ключову тему навчання [1]. Завдання сфокусовані на практичній демонстрації створення та безпечного використання паролів для підвищення рівня знань у цій сфері;

– безпека в мережі та Wi-Fi – практичні завдання мають включати

обговорення загроз і ризиків підключення до незахищених та недовірених Wi-Fi мереж, а також питання, пов'язані з використанням VPN (Virtual Private Network). Необхідно навчати учнів, як забезпечити безпечне підключення до Інтернету (safe internet connection). Ці питання зазначені у праці [1] та рекомендовані до внесення до навчальної програми [11];

– соціальна інженерія – цей напрям передбачає завдання на ідентифікацію загроз. Ефективним методом є обговорення "живих кейсів кіберзагроз" (live cases of cyber threats) [9], з якими учні стикаються, використовуючи цифрові сервіси в Інтернеті. Фокус має бути на розпізнаванні фішингових атак (phishing) та інших видів маніпуляцій (manipulation) [1];

– конфіденційність даних – вправи мають охоплювати питання приватності (privacy) [1], зокрема, аналіз ризиків, пов'язаних із використанням соціальних мереж (Social Networks) [1]. Також необхідно сформувати навичку резервного копіювання (backup) даних [1]. Безпека соціальних мереж розглядається як обов'язковий компонент навчання [11];

– загальна кібергігієна – завдання на формування загальної безпечної поведінки в Інтернеті через практичне застосування принципів, таких як "Зупинись. Подумай. Підключись" (Stop. Think. Connect) [6]. Це загальний фреймворк для прийняття безпечних рішень у цифровому середовищі.

Лабораторні вправи передбачають використання практичних вправ (hands-on exercises) для підвищення залученості та формування навичок, необхідних для запобігання, виявлення та реагування на кібератаки:

– експериментальне навчання IoT – упровадження спільного (collaborative) та експериментального навчання (experiential learning) через використання "зламних іграшок Інтернету речей" (hackable Internet of Things (IoT) toys) [12]. Це слугує інноваційним педагогічним інструментом, що дозволяє учням практично освоювати концепції кібербезпеки та сприяє їхньому залученню до сфери;

– лабораторні роботи на мережевому полігоні – проведення добре структурованих практичних завдань (well-structured hands-on exercises) у спеціалізованому мережевому тестовому середовищі (network testbed) [18]. Такий підхід має на меті підвищити залученість студентів та забезпечити краще закріплення знань. Ці вправи повинні охоплювати такі теми, як "Безпека мереж" (Network Security та "Безпека операційних систем" (Operating System Security [6];

– забезпечення інформаційної безпеки (information assurance) – практичне вивчення процесів та інструментів, які необхідні для захисту конфіденційних цифрових даних від порушення, модифікації та знищення (processes and tools for protecting sensitive digital data from disruption, modification and destruction) [10]. Цей компонент є фундаментальною частиною курсу "Інформаційна безпека" і розглядається як один із розділів [6];

– вступ до криптографії – ознайомчі практичні завдання та сценарії, які вводять учнів у основи криптографії (cryptography). Для спрощення та візуалізації концепцій можуть бути використані класичні навчальні сценарії, наприклад, "Аліса та Боб" (Alice and Bob) [6];

– основи кіберрозвідки – вступні практичні заняття з кіберрозвідки (Cyber Intelligence), які формують розуміння збору та аналізу інформації, пов'язаної з кіберзагрозами, зокрема вивчення ключових протоколів та ідентифікаторів: IP, MAC та DNS; розгляд концепцій "Найслабша ланка" (weakest link) та "Концепція досягнення-пробою" (reach-breach concept), що є важливими для розуміння ризиків; ознайомлення з базовими елементами цифрового середовища: Кіберпростір (cyberspace) та Інтернет; вивчення питань чмарних обчислень та їхньої безпеки (cloud computing and its security), а також роботи маршрутизаторів та Wi-Fi (routers and WiFi) [6]. Ці питання стосуються професійної освіти, проте є доречними та кориснимми в межах вибіркового модуля "Інформаційна безпека" як матеріал підвищеної складності для зацікавлених учнів.

Організація практичних майстер-класів (hands-on workshops), розглядається як ефективний спосіб отримання практичного досвіду та

підвищення обізнаності учнів щодо кібербезпекових кар'єр [20].

Методики активного та ігрового навчання рекомендовані для підвищення залученості (engagement), набору (recruitment) та оцінки знань учнів. Вони також є одним із основних шляхів залучення (exposure) учнів до кібербезпекових активностей та професій:

– змагання "Захопи прапор" (Capture-the-Flag, CTF) – Це популярна форма змагань, яка використовується для залучення студентів до вивчення питань у сфері кібербезпеки [12]. Детально пропрацьовані активності у форматі CTF запропоновані у [9]. Змагання як такі розглядаються як один із елементів залучення учнів до діяльності в галузі кібербезпеки як навчальної так і професійної [20];

– використання освітніх ігор – дослідники стверджують, що ігри є ефективними для підвищення обізнаності та навчання безпеці в Інтернеті та рекомендують застосування освітніх ігор (educational games) та інтерактивних вікторин (quizzes) як інструментів активного навчання (active learning) [8], [9];

– аналіз реальних кейсів та дискусії – методика передбачає презентацію та обговорення "живих кейсів кіберзагроз" (live cases of cyber threats), з якими учні могли зіткнутися під час використання цифрових сервісів в Інтернеті. Це посилює взаємодію між учителями та учнями, демонструючи актуальність і застосовність навчального контенту [8], [9];

– позакласні та практичні заходи – до активного навчання також належать позакласні заходи, такі як участь у кіберклубах (cyber clubs), літніх таборах (camps) [7] та спеціалізованих практичних майстер-класах (hands-on workshops) [20]. Ці заходи забезпечують раннє залучення (early exposure) та практичний досвід, які є ключовими факторами для формування інтересу до кібербезпеки [20].

Отже, за результатами огляду визначено головні напрями тематичного наповнення навчальних курсів із інформаційної безпеки та знайдено приклади завдань і способи організації навчальної діяльності учнів у контексті побудови методичної системи вибіркового модуля "Інформаційна

безпека" для учнів ліцеїв. Залишається актуальною реалізація ідеї диференційованого навчання під час побудови такої методичної системи на підґрунті всесвітнього досвіду реалізації практично-орієнтованого підходу до навчання основам інформаційної безпеки.

Висновки до 1 розділу

Проведений у першому розділі теоретичний аналіз та систематизація наукових джерел дозволяють сформулювати наступні висновки.

Бібліографічний аналіз 585 публікацій з бази Scopus виявив п'ять основних тематичних кластерів досліджень у галузі навчання інформаційній безпеці. Встановлено, що активізація досліджень розпочалася у 2021-2022 роках у зв'язку з пандемією COVID-19 та зростанням кіберзагроз. Домінування термінів "cyber security" (195 поява) та "students" (190 поява) з найвищими показниками зв'язків підкреслює центральну роль учнівської аудиторії в дослідженнях кібербезпеки.

Сучасне розуміння диференційованого навчання базується на адаптації чотирьох основних елементів навчального процесу (зміст, процес, продукт, середовище) відповідно до трьох характеристик учнів (рівень готовності, інтереси, профіль навчання). Аналіз вітчизняних публікацій за 2021-2025 роки виявив недостатню розробленість практичних інструментів диференціації за інтересами учнів, що актуалізує необхідність створення відповідних методичних матеріалів.

Було ідентифіковано три основні категорії дидактичних матеріалів: практичні завдання з кібергігієни та моделювання поведінки; лабораторні та технічні вправи; методики активного та ігрового навчання. Встановлено домінування інноваційних підходів, таких як гейміфікація, CTF-змагання та симуляційне навчання, що свідчить про пошук ефективних педагогічних рішень для формування культури кібербезпеки.

Незважаючи на значний інтерес до диференційованого навчання, практичні розробки обмежуються переважно диференціацією за рівнем складності завдань. Бракує теоретичного обґрунтування та практичних прикладів диференціації за професійними інтересами учнів, що створює передумови для розробки авторської методичної системи.

Проведений аналіз довів, що існує об'єктивна потреба в ство-

ренні методичної системи, яка б поєднувала світовий досвід практично-орієнтованого навчання основам інформаційної безпеки з принципами диференціації за професійними інтересами та рівнем підготовки учнів ліцеїв.

Таким чином, результати теоретичного дослідження створюють наукове підґрунтя для розробки методичної системи диференційованого навчання вибіркового модуля "Інформаційна безпека" учнів ліцеїв, що буде представлено в наступному розділі роботи.

РОЗДІЛ 2
МЕТОДИЧНА СИСТЕМА ДИФЕРЕНЦІЙОВАНОГО НАВЧАННЯ ВИБІРКОВОГО МОДУЛЯ “ІНФОРМАЦІЙНА БЕЗПЕКА” УЧНІВ ЛІЦЕЇВ

2.1. Обґрунтування змістовного наповнення вибіркового модуля “Інформаційна безпека” учнів ліцею

2.1.1. Порівняльний аналіз програми навчання учнів інформаційної безпеки

Інформаційна безпека не є ізольованим модулем, а є наскрізною вимогою курсу інформатики, яка формується через декілька міжпредметних компетентностей, що відображає сучасні педагогічні підходи до формування відповідального цифрового громадянства. Проаналізуємо Державний стандарт базової середньої освіти [28], зокрема інформатичну освітню галузь. У таблиці 2.1 подані вимоги до кібербезпеки, цифрової етики та захисту даних, які інтегровані в структуру ключових компетентностей.

Як видно з таблиці компетентність “Екологічна грамотність і здорове життя” містить важливий блок вимог, що стосуються фізичної та технічної безпеки. Зокрема, стандарт вимагає від здобувачів освіти дотримання правил безпечного поводження з комп’ютерними пристроями (апаратними, мережевими та програмними засобами). Критично важливим є вміння обирати безпечні паролі та інші методи автентифікації, що є базовим елементом захисту персональних облікових записів.

Соціальний вимір кібербезпеки є фундаментальною складовою компетентності “Громадянська та соціальна компетентності”. Основний аспект цієї компетентності зміщується з “як захистити себе” на “як діяти відповідально та законно”. Учні повинні не просто знати, а й поясню-

Таблиця 2.1

Вимоги до учнів щодо формування навичок безпечного та відповідального поводження у цифровому середовищі згідно з Державним стандартом базової середньої освіти [28].

№	Ключова компетентність	Уміння та ставлення
1	**Екологічна грамотність і здорове життя**	• Уміння: дотримуватися правил безпечного поводження з комп'ютерними пристроями (апаратними, мережевими та програмними засобами). • Уміння: обирати безпечні паролі та інші методи автентифікації.
2	**Громадянська та соціальна компетентності**	• Уміння: пояснювати співвідношення між правилами, потребами і правом та законами в галузі цифрових технологій. • Уміння: дотримуватися у власній інформаційній діяльності законів щодо захисту даних, інтелектуальної і приватної власності, пояснювати відповідальність за їх порушення. • Уміння: наводити приклади наслідків порушення прав інтелектуальної власності, розрізняти різновиди і серйозність порушень. • Ставлення: повага до інтелектуальної власності та нетерпимість до порушень правових норм.

вати співвідношення між правилами, потребами і правом та законами в галузі цифрових технологій. Центральною вимогою є дотримання законів щодо захисту даних, інтелектуальної і приватної власності у власній інформаційній діяльності. Стандарт вимагає від учнів здатності пояснювати відповідальність за їх порушення, включно з умінням наводити при-

клади наслідків порушення прав інтелектуальної власності та розрізняти серйозність цих порушень [28]. Це формує повагу до інтелектуальної власності та нетерпимість до порушень правових норм.

Ядро практичного кіберзахисту зосереджено в компетентності "Інформаційно-комунікаційна компетентність (ІКТ)". Тут формуються навички активного управління власним цифровим слідом та захистом. Це охоплює здатність розрізняти особисту, приватну і конфіденційну інформацію, що є необхідною передумовою для усвідомленого захисту. Технічний захист передбачає використання цифрових інструментів для захисту даних, включаючи освоєння шифрування та двофакторної автентифікації. Не менш важливим є превентивний захист: учні мають вміти розпізнавати та уникати фішингових посилань, спаму та іншого небезпечного контенту. Нарешті, Стандарт вимагає знання протоколів поведінки: дотримання етикету (нетикету) в мережевій комунікації та знання алгоритму дій у разі виявлення кіберзагрози чи витоку даних [28].

Вимоги, що стосуються безпеки, пронизують і наскрізні компетентності. У межах "Навчання впродовж життя" учні мають набути навичок динамічної безпеки: оцінювати ризики для приватності та безпеки при освоєнні нових технологій [28]. Це також включає практичне вміння використовувати антивірусні та інші захисні програми та розуміння наслідків використання неліцензійного програмного забезпечення.

Компетентність "Уміння вчитися" формує основу для інформаційної безпеки, вимагаючи від учнів розрізняти надійні та ненадійні джерела інформації в Інтернеті [28]. Це є критично важливим для протидії дезінформації та соціальній інженерії.

Державний стандарт України визначає компетентнісний потенціал Інформатичної освітньої галузі, виділяючи ключові вміння та ставлення, які мають бути сформовані у здобувачів освіти. Проте, стандарт не є переліком тем; він є нормативним каркасом і філософською основою. Завдання навчальної програми полягає у трансформації цих загальних вимог у конкретний, структурований і послідовний навчальний зміст.

З інформаційною безпекою учні знайомляться ще у базовій школі. Проаналізуємо більш детально модельні навчальні програми "Інформатика. 5-6 клас" [29] та "Інформатика. 7-9 клас" [30] для за-

кладів загальної середньої освіти (авторів Ривкінд Й. Я., Лисенко Т. І., Чернікова Л. А., Шакотько В. В.), які побудовані на концепції Нової української школи [15].

Модельна навчальна програма "Інформатика. 5-6 класи" [29] вже на етапі пояснювальної записки визначає безпеку як ключовий елемент, де у меті навчання зазначається: " *...розвиток особистості учня, здатного... безпечно та відповідально діяти в інформаційному суспільстві.*"

Модельна навчальна програма "Інформатика" для 5–6 класів формує базову цифрову культуру, концентруючись на етичних, правових та гігієнічних аспектах безпеки. На цьому етапі навчання спрямоване на виховання відповідального користувача, здатного безпечно взаємодіяти з початковими цифровими інструментами. Мережевий етикет є наріжним каменем програми 5–6 класів. Учні не просто знайомляться з нетікетом, а засвоюють правила культурної та поважної взаємодії в онлайн-середовищах. Це включає розуміння тону спілкування, уникнення конфліктів та формування позитивної цифрової репутації. Ця складова є фундаментальною для запобігання соціальним загрозам (наприклад, кібербулінгу). З моменту створення перших інформаційних продуктів (презентацій, текстових документів), від учнів вимагається розуміння інтелектуальної власності. Вони мають розрізняти різні типи дозволів на використання контенту та обов'язково зазначати джерела використаних матеріалів. Це не лише правова вимога, а й перший практичний крок до забезпечення цілісності даних (використання перевіреної інформації) та академічної чесності. Під вимогою "Дотримується правил кібербезпеки" мається на увазі опанування набору критично важливих поведінкових правил. Це стосується використання надійних, унікальних паролів, обережного ставлення до невідомих електронних листів і посилань (первинна профілактика фішингу), а також розуміння, коли та яку особисту інформацію можна розголошувати. Хоча навчальна програма не вивчає резервне копіювання, тема "Інформаційні процеси та системи" формує розуміння цінності даних через їх організацію, збереження та управління файловою структурою. Це є непрямою, але необхідною передумовою для подальшого вивчення системного захисту. Отже, у 5-6 класах за модельною навчальною програмою закладається фундамент комп'ютерної безпеки концентруючись на формуванні відповідальної

та етичної цифрової поведінки, але не торкається технічної складової захисту.

Модельна навчальна програма "Інформатика" для 7–9 класів [30] значно поглиблює знання, які були закладені раніше, особливо в частині захисту персональних даних та приватності. Крім того відображає зростання соціальної та інформаційної складності, посилюючи фокус на критичному мисленні та відповідальності в мережевих середовищах. У темі "Інформаційні процеси та системи. Інформація" (7 клас), учні переходять від простого пошуку інформації до її оцінювання. Вони вчаться виявляти, аналізувати та спростовувати фейки, маніпулятивну та недостовірну інформацію. Це є життєво важливою оборонною стратегією інформаційної безпеки, спрямованою на захист від інформаційних атак. При вивченні комунікації у 7 класі, учні вже вчаться захищати паролі та персональні дані. Тема "Комп'ютерні мережі. Мережеві технології" (8 клас) виводить загальні правила кібербезпеки (з 5-6 класів) на більш високий рівень. Учні вчаться аналізувати небезпеки під час використання конкретних мережевих сервісів та усвідомлювати наслідки своїх дій у більших мережевих спільнотах. В рамках опрацювання інформації, виникає потреба захищати персональні дані від несанкціонованого доступу та розуміти основи шифрування. Це включає непряме розуміння важливості аутентифікації та захисту своїх облікових записів. Теми авторського права та етичних норм під час спілкування (8 клас) повторюються, підтверджуючи їхню незмінну важливість у будь-якому віці, особливо в контексті збільшення обсягу створюваного та споживаного контенту. У 9 класі, при вивченні "Інформаційних систем", учні активно використовують хмарні сервіси для колективної роботи. Це вимагає від них дотримання правил безпеки в спільних та віддалених середовищах. На рівні проєктної діяльності (9 клас) поглиблюється ціннісна складова щодо дотримання правил безпеки та запобігання конфліктам. Таким чином, у 7-9 класах програма виводить поняття безпеки за межі персонального пристрою, підводячи до концепцій мережевої взаємодії та захисту даних, що зберігаються поза контролем користувача.

У навчальній програмі з інформатики для учнів 10-11 класів [27] закладаються основи, які орієнтуються на поведінкові аспекти та широку

інформаційну грамотність. Базовий модуль переважно зосереджений на поведінковій безпеці та концепції цифрового громадянства, навчаючи учнів загальним правилам безпечної роботи та етиці в мережі Інтернет. Його основна мета полягає у формуванні знань про те, "як безпечно користуватися" інформаційними технологіями, а також охоплює широкий спектр тем: від штучного інтелекту та Інтернету речей до фінансових розрахунків і СУБД. Безпека тут є лише одним із елементів, що підтримує загальну компетентність. У питаннях загроз програма базового модулю обмежується лише загальними "проблемами та загрозами в Інтернеті", що є лише поверхневим знайомством. Учні дізнаються про ризики, але не про механізми їхньої реалізації. Щодо засобів захисту, то базовий модуль програми вимагає від учнів лише дотримання правил безпечної поведінки.

Питання основних понять інформаційної безпеки та загроз представлені на рівні знаннєвої складової цієї лінії. Тут вводиться необхідна термінологія, яка дозволяє учням визначити загальну проблематику інформаційної безпеки і сформувати уявлення про роль інформаційної системи та потенційні небезпеки. Учні дізнаються про основи інформаційної безпеки та проблеми інформаційної безпеки, що є відправною точкою для поглибленого вивчення.

Критично важливим є питання дотримання правил безпечної роботи. Програма базового модулю, у своїй діяльнісній складовій, чітко вимагає, щоб учень дотримувався правил безпечної поведінки в Інтернеті та використовував технології цифрового громадянства. Це забезпечує акцент на етиці, особистій відповідальності, мережевому етикету та усвідомленій поведінці в мережі. Це є непрямим охопленням захисту від шкідливого програмного забезпечення, оскільки безпечна поведінка є першим і найважливішим кроком у запобіганні завантаженню вірусів, хоча й без вивчення технічних засобів їхнього усунення. Обов'язкове вивчення цих правил спрямоване на мінімізацію ризиків, пов'язаних із соціальною інженерією та фішингом.

Крім того слід зауважити, що при вивченні змістової лінії "Мультимедійні та гіпертекстові документи", тема створення веб-сайтів за допомогою систем керування вмістом включає вимогу дотримання правил ергономічного розміщення матеріалів. Хоча це безпосередньо стосується

використання та зручності для користувача, всеж таки це є елементом забезпечення надійності та цілісності ресурсу, що опосередковано стосується безпеки, оскільки добре структурований і ергономічний сайт менш схильний до помилок, які можуть створити вразливості, але, знову ж таки, технічний захист сервера чи коду від злому тут не розглядається.

Обов'язкова частина, представлена базовим модулем, охоплює лише загальні основи інформаційної безпеки та її проблеми у широкому соціальному контексті. Вона повністю фокусується на етичній поведінці та цифровому громадянстві як головних інструментах захисту, що включає усвідомлення загроз в Інтернеті. Навички базового модуля охоплюють загальну комп'ютерну грамотність та планування діяльності, тоді як технічна безпека залишається виключно на рівні правил поведінки. У цій частині повністю відсутні теми мережевого захисту та збереження даних на системному рівні, оскільки вони виходять за рамки мінімальних вимог.

Базовий модуль ефективно інтегрує деякі основи безпеки, закладаючи необхідний фундамент для вибіркового модулю "Інформаційна безпека".

2.1.2. Аналіз вибіркового модуля "Інформаційна безпека"

Програма вибіркового модулю "Інформаційна безпека" рекомендована Міністерством освіти і науки України [27]. Вона рекомендована для учнів профільної школи і розрахована на 17 годин. Програма охоплює три розділи.

Розділ 1 "Основи безпеки інформаційних технологій" присвячений формуванню ціннісної основи кібербезпеки, а також правової та аналітичної свідомості. Під час вивчення розділу учні опановують основні поняття інформаційної безпеки, зрозуміють місце та роль автоматизованих систем, а також причини загострення проблеми безпеки. Детально вивчають інформаційні відносини, суб'єктів, їхні інтереси та шляхи нанесення шкоди. Аналізують загрози безпеці, джерела та канали несанкціонованого доступу, включаючи комп'ютерні віруси та програми-зломщики. Основний акцент зміщується з базових навичок (які учні вже мають після базового модулю курсу інформатики) на правове обґрунтування, систематизацію загроз та аналіз ризиків. Учні осмислюють важливість і місце інформаційної безпеки в сучасному суспільстві. Учні повинні навчитися не лише дотри-

муватись правил кібергігієни, але й аналізувати вразливості, створювати базові матриці ризиків для інформаційних систем, а також розуміти правове поле інформаційних відносин та відповідальності в Україні. Наприкінці вивчення цього розділу учні зможуть не лише ідентифікувати базові загрози, але й сформує правове та етичне підґрунтя для подальшої практичної роботи з безпекою, усвідомлюючи власну відповідальність у цифровому середовищі.

Розділ 2 "Забезпечення безпеки інформаційних технологій" є фундаментальним і присвячений системному захисту окремого комп'ютера та даних. Його зміст є найбільш насиченим з погляду нових, складних тем, які не розглядалися на базовому рівні, зокрема криптографія та моделі розмежування доступу. Це закладає основи інженерного підходу до захисту інформації. Під час вивчення розділу учні детально опанують керування доступом: моделі ІАА (ідентифікація, автентифікація, авторизація), дискреційну та мандатну моделі. Проведуть детальне вивчення криптографічних методів (шифрування та хешування), їх класифікації. Ознайомляться з електронним цифровим підписом (ЕЦП) та його інфраструктурою (центри сертифікації). Розглянуть засоби контролю цілісності програмного забезпечення та даних, а також навчаться створювати і відновлювати резервні копії операційних систем і даних, забезпечуючи цілісність та конфіденційність інформації. Результати цього розділу забезпечують глибоке розуміння та практичне володіння фундаментальними інструментами захисту даних і систем, зокрема криптографічними механізмами, що є наріжним каменем будь-якої інформаційної безпеки.

Розділ 3 "Забезпечення безпеки комп'ютерних систем і мереж" найбільш практико-орієнтований. Він повністю присвячений мережевому захисту та конфігуруванню інфраструктури. Опанування матеріалом роздулу сприятиме підготовці учнів до роботи з корпоративними мережами. Учні навчаться аналізувати типову корпоративну мережу, рівні інфраструктури, мережеві загрози (DDoS, MITM) та атаки. Опанують віртуальні приватні мережі (VPN), їх призначення та тунелювання. Вивчать призначення та захисні механізми міжмережевих екранів (брандмауерів), а також політику безпеки. Розглянуть системи аналізу вмісту трафіку (пошта, веб) та сценарії реагування. Теми міжмережеві екрани

(брандмауери), VPN-мережі та аналіз трафіку є абсолютно новими для учнів. При вивченні розділу учні повинні набути діяльнісної складової у сфері захисту мереж. Вони мають вміти аналізувати мережеві загрози (DDoS, MITM), розуміти принципи роботи брандмауерів та конфігурувати правила фільтрації (на рівні симуляції чи ОС). Крім того, вони повинні вміти налаштовувати VPN-клієнтів та розуміти, як працюють системи аналізу вмісту трафіку. Результатом є практичні навички захисту мережевої інфраструктури. Після завершення розділу учні мають пояснити типи корпоративних мереж, класифікувати загрози, описувати принципи роботи брандмауерів та VPN. Виконувати конфігурування міжмережевого екрану, розуміючи принципи функціонування корпоративних мереж та вміючи конфігурувати критичні елементи захисту, такі як брандмауери та VPN. Також використовувати засоби моніторингу мережного трафіку, виконувати конфігурування простих маршрутизаторів. Набути практичні навички роботи з периметровим захистом, усвідомлювати необхідність та виконувати резервне збереження даних, дотримуватись правил безпечної роботи в Інтернеті, враховувати наслідки несанкціонованого доступу,

Аналіз програми дозволив запропонувати такий календарний план (таблиця 2.2).

Таблиця 2.2

Календарно-тематичне планування для вибіркового модуля “Інформаційна безпека”.

№	Тема уроку	Мета уроку	Зміст навчання
Розділ І: Основи безпеки ІТ (систематизація) (3 год.)			
1	Систематизація загроз. Правове поле ІБ в Україні.	Систематизувати знання про загрози та вразливості; засвоїти правові основи ІБ (кейс-стаді).	Теоретичні основи. Правове поле ІБ в Україні.
2	Інформаційні відносини та аналіз вразливостей. Оцінка ризиків.	Опанувати методологію оцінки ризиків; практично створити матрицю ризиків.	Інформаційні відносини. Аналіз вразливостей. Практикум: Створення матриці ризиків.

3	Політика кібергігієни (переосмислення) та контроль цілісності (вступ).	Навчитися використовувати хеш-суми для контролю цілісності; переосмислити правила кібергігієни.	Політика кібергігієни. Практикум: використання хеш-сум.
Розділ II: Системний захист (криптографія) (7 год.)			
4	Керування доступом: ІАА. Дискреційна/мандатна моделі.	Засвоїти ключові моделі керування доступом (ІАА); відпрацювати застосування через рольову гру.	Керування доступом: ідентифікація, автентифікація, авторизація (ІАА). Моделі доступу.
5	Криптографічні методи: Шифрування та хешування (теорія).	Зрозуміти принципи та класифікацію криптографічних методів; проаналізувати алгоритми.	Криптографічні методи: шифрування (симетричне/асиметричне) та хешування.
6	Лабораторна робота 1: Практичне застосування шифрування (2 год.)	Набути практичних навичок шифрування та дешифрування із застосуванням GPG / аналогів.	Діяльнісна складова: робота з GPG / аналогами (симетричне та асиметричне шифрування).
7	Електронний цифровий підпис (ЕЦП). Центри сертифікації.	Вивчити принципи ЕЦП та інфраструктуру відкритих ключів; проаналізувати приклади використання.	ЕЦП та інфраструктура відкритих ключів. Кейс: Використання ЕЦП в Україні.
8	Засоби контролю цілісності ПЗ та даних.	Ознайомитися з інструментами контролю цілісності; практично перевірити цілісність ПЗ.	Засоби контролю цілісності ПЗ та даних. Практикум: Перевірка цілісності ПЗ.
9	Резервне копіювання ОС та даних. Політика відновлення.	Розробити політику резервного копіювання та відновлення; практично створити образ ОС (віртуальне середовище).	Резервне копіювання ОС та даних. Практикум: Створення образу ОС.
Розділ III: Мережевий захист (конфігурування) (7 год.)			
11	Корпоративна мережа. Рівні інфраструктури. Мережеві загрози.	Вивчити структуру корпоративної мережі та проаналізувати основні мережеві загрози (DDoS, MITM).	Корпоративна мережа, її інфраструктура. Мережеві загрози (DDoS, MITM).

12	Міжмережеві екрани (брандмауери): принципи роботи.	Засвоїти принципи функціонування брандмауерів; зрозуміти їхню роль у периметровому захисті.	Міжмережеві екрани (брандмауери): принципи роботи та захисні механізми.
13	Лабораторна робота 2: Конфігурування міжмережевого екрану (2 год.)	Набути практичних навичок конфігурування брандмауера та налаштування правил фільтрації.	Діяльнісна складова: налаштування правил фільтрації (ОС/симулятор).
14	Віртуальні приватні мережі (VPN): призначення та тунелювання.	Вивчити призначення та архітектуру VPN; зрозуміти механізми тунелювання.	Віртуальні приватні мережі (VPN): призначення та тунелювання.
15	Лабораторна робота 3: Налаштування VPN-клієнта.	Практично налаштувати та використовувати VPN-клієнт для безпечного віддаленого доступу.	Діяльнісна складова: робота з VPN-клієнтом.
16	Системи аналізу вмісту трафіку (пошта, веб).	Ознайомитися з принципами роботи систем DLP/IDS/IPS та їхньою роллю у фільтрації контенту.	Системи аналізу вмісту трафіку (пошта, веб).
17	Підсумкове заняття / Захист проєкту.	Систематизувати набуті знання та вміння; здійснити презентацію та захист фінального проєкту.	Систематизація знань, оцінювання, захист проєкту.

2.2. Розробка завдань для диференційованого навчання вибіркового модуля “Інформаційна безпека” учнів ліцею

2.2.1. Практична робота №1 “Систематизація загроз та правове поле інформаційної безпеки”

Розроблена практична робота демонструє реалізацію диференційованого підходу при вивченні першої теми курсу. Структурно робота організована таким чином, що забезпечує гнучкість у виборі траєкторії виконання завдань при збереженні єдиних навчальних цілей.

Практична робота виконується протягом двох уроків з додатковою самостійною роботою вдома. Перший урок (45 хвилин) присвячений виконанню завдання середнього рівня для кожного спрямування в класі під керівництвом учителя. Це забезпечує формування фундаментальних знань та вмінь, необхідних для подальшої самостійної роботи. Завдання достатнього та високого рівнів виконується як домашня робота за вибором учня, що дозволяє індивідуалізувати темп та глибину опрацювання матеріалу. Презентація результатів (15 хвилин на наступному уроці) створює умови для обміну досвідом та взаємонавчання учнів.

Академічний напрямок "Дослідник безпеки" спрямований на формування аналітичних та дослідницьких компетентностей у галузі інформаційної безпеки. Завдання цього напрямку (табл. 2.3) акцентують увагу на систематизації знань, критичному аналізі джерел та створенні інформаційних продуктів .

На середньому рівні учні створюють структуровану класифікацію загроз інформаційній безпеці, використовуючи критерії джерела походження (внутрішні/зовнішні), наміру (навмисні/випадкові) та об'єкта атаки. Обов'язковим компонентом є пошук та аналіз двох реальних прикладів кіберінцидентів в Україні за останні роки. Це формує навички роботи з актуальною інформацією та розуміння реальних загроз у національному контексті.

Достатній рівень передбачає побудову схеми взаємозв'язків між типами загроз, що розвиває системне мислення учнів. Порівняльний аналіз класифікацій загроз за українським законодавством та міжнародним стандартом ISO 27001 формує розуміння різних підходів до систематизації загроз. Аналіз тенденцій змін загроз за останні три роки розвиває навички прогнозування та стратегічного мислення.

На високому рівні учні створюють комплексні інформаційні продукти – інфографіку ландшафту загроз для освітніх закладів України та презентацію про трансформацію загроз після початку повномасштабної війни. Розробка практичних рекомендацій для закладу освіти демонструє здатність застосовувати теоретичні знання для вирішення реальних проблем.

Технічний напрямок "Етичний хакер" орієнтований на формування практичних навичок виявлення та усунення вразливостей інформаційних

Таблиця 2.3

Завдання для “Дослідників безпеки”.

РІВЕНЬ	ЗАВДАННЯ
Середній	**Базове дослідження:** 1. Створити таблицю-класифікацію з 8+ загроз ІБ за категоріями: джерело (внутрішні/зовнішні), намір (навмисні/випадкові), об’єкт атаки 2. Знайти 2 реальні приклади кіберінцидентів в Україні (2023-2024 рр.) 3. Оформити у вигляді документа з посиланнями на джерела
Достатній	**Поглиблений аналіз (додатково до середнього рівня):** 1. Побудувати схему взаємозв’язків між типами загроз 2. Порівняти класифікації загроз: Закон України “Про основні засади забезпечення кібербезпеки” vs ISO 27001 3. Проаналізувати тенденції змін загроз за останні 3 роки
Високий	**Експертний рівень (додатково до достатнього рівня):** 1. Створити інфографіку “Ландшафт загроз ІБ для освітніх закладів України” 2. Підготувати презентацію до виступу на тему “Як змінилися загрози ІБ в Україні після 24.02.2022” 3. Розробити 3 рекомендації для ліцею щодо протидії актуальним загрозам

систем. Завдання (табл. 2.4) побудовані за принципом поступового ускладнення від базової діагностики до симуляції пентесту.

Базовий рівень включає проведення сканування безпеки персонального комп’ютера з використанням онлайн-інструментів, зокрема Shields Up! від GRC.com. Учні опановують базові навички технічного аудиту через заповнення чек-листа, що включає перевірку антивірусного захисту, актуальності оновлень операційної системи, складності паролів та налаштувань фаєрволу. Документування результатів у вигляді скріншот-звіту з поясне-

Таблиця 2.4

Завдання для “Етичного хакера”.

РІВЕНЬ	ЗАВДАННЯ
Рівень I (6 балів)	**Базова практика:** 1. Провести сканування безпеки ПК (Shields Up! від GRC.com) 2. Заповнити чек-лист: антивірус, оновлення ОС, складність паролів, фаєрвол 3. Створити скріншот-звіт з поясненнями знайдених проблем
Рівень II (9 балів)	**Технічне дослідження (додатково до рівня I):** 1. Дослідити одну CVE вразливість: опис, механізм, патч 2. Створити демонстрацію загрози: фішинг (макет), слабкий пароль, або SQL-ін’єкція (DVWA) 3. Протестувати з онлайн-сервіси на HaveIBeenPwned
Рівень III (11-12 балів)	**Пентест-симуляція (додатково до рівнів I-II):** 1. Провести міні-аудит за OWASP Top 10 2. Написати Python-скрипт для перевірки складності паролів 3. Записати відео-демонстрацію (3-5 хв) атаки та захисту

ннями формує навички технічної документації.

На технічному рівні дослідження учні поглиблюють розуміння механізмів вразливостей через дослідження конкретної CVE-вразливості, включаючи її опис, механізм експлуатації та методи усунення. Створення демонстрації загрози (макет фішингової атаки, демонстрація атаки на слабкий пароль або SQL-ін’єкція в навчальному середовищі DVWA) забезпечує практичне розуміння методів атак. Використання сервісу HaveIBeenPwned для перевірки витоків даних формує навички персональної кібергігієни.

Рівень пентест-симуляції передбачає проведення міні-аудиту за методологією OWASP Top 10, що є професійним стандартом у галузі веббезпеки. Написання Python-скрипту для перевірки складності паролів розвиває навички програмування для вирішення задач безпеки. Створення відео-демонстрації атаки та захисту (3-5 хвилин) формує вміння

візуалізувати та пояснювати складні технічні процеси.

Управлінський напрямок “Менеджер безпеки” спрямований на формування компетентностей з управління інформаційною безпекою на організаційному рівні. Завдання (табл. 2.5) акцентують увагу на правових, економічних та організаційних аспектах забезпечення інформаційної безпеки.

Таблиця 2.5

Завдання для “Менеджера безпеки”.

РІВЕНЬ	ЗАВДАННЯ
Рівень I (6 балів)	**Базове планування:** 1. Проаналізувати Закон України “Про захист персональних даних” 2. Розробити чек-лист compliance для інтернет-магазину 3. Створити шаблон “Згоди на обробку персональних даних”
Рівень II (9 балів)	**Управлінське рішення (додатково до Рівня I):** 1. Розробити матрицю ризиків 5x5 для стартапу (10 загроз) 2. Розрахувати базовий бюджет ІБ для компанії з 10 співробітників 3. Створити план реагування на інцидент (1 сторінка)
Рівень III (11-12 балів)	**Стратегічний рівень (додатково до Рівнів I-II):** 1. Розробити презентацію для керівництва (7-10 слайдів) з ROI 2. Створити проект “Положення про інформаційну безпеку” (2-3 сторінки) 3. Розробити 5 KPI для оцінки ефективності ІБ

Базовий рівень планування включає аналіз Закону України “Про захист персональних даних” та розробку практичних документів для забезпечення відповідності вимогам законодавства. Створення чек-листа compliance для інтернет-магазину та шаблону згоди на обробку персональних даних формує розуміння правових вимог та навички розробки корпоративної документації.

Управлінське рішення передбачає розробку матриці ризиків розміром 5×5 для стартапу з ідентифікацією та оцінкою 10 загроз. Розрахунок базового бюджету інформаційної безпеки для малого підприємства розвиває навички фінансового планування в галузі безпеки. Створення плану реагування на інцидент формує розуміння процесів управління інцидентами.

На стратегічному рівні учні розробляють презентацію для керівництва з обґрунтуванням повернення інвестицій (ROI) в інформаційну безпеку. Створення проекту "Положення про інформаційну безпеку" демонструє здатність розробляти нормативні документи організації. Розробка ключових показників ефективності (KPI) для оцінки стану інформаційної безпеки формує навички стратегічного управління.

2.2.2. Урок №4 "Керування доступом: IAA. Дискреційна/Мандатна моделі"

Тема керування доступом є фундаментальною у вивченні інформаційної безпеки, оскільки формує розуміння базових механізмів захисту інформаційних ресурсів. Розроблена система диференційованих завдань для уроку №4 реалізує комплексний підхід до вивчення концепції IAA (Ідентифікація, Автентифікація, Авторизація) та моделей керування доступом через призму професійних інтересів та майбутньої спеціалізації учнів.

Структура уроку побудована за принципом поступового занурення у предметну область: від загального розуміння процесів ідентифікації користувачів до практичної реалізації різних моделей керування доступом. Особливістю методичного підходу є використання спільної стартової активності, що забезпечує формування єдиного понятійного апарату перед диференційованою роботою.

Мозковий штурм "Як система впізнає користувача?" створює когнітивну основу для подальшої диференційованої роботи. Через перегляд демонстраційного відео процесу входу в систему (2 хвилини) та інтерактивне заповнення схеми (рис. 2.1) на дошці учні формують розуміння триєдиної концепції IAA. Схема візуалізує логічний ланцюжок: "Хто я?" відповідає процесу ідентифікації через логін, "Доведи це!" розкриває сутність автентифікації через паролі чи біометрію, "Що можу?" демон-

струє механізм авторизації через права доступу.

Рис. 2.1. Концепція IAA (ідентифікація, автентифікація, авторизація).

Така структурована візуалізація забезпечує формування ментальної моделі, яка стає опорою для виконання диференційованих завдань незалежно від обраного напрямку. Важливо, що всі учні отримують однакову базову інформацію, але далі інтерпретують та застосовують її відповідно до специфіки свого профілю.

Академічний напрямок "Аналітик систем безпеки" (табл. 2.6) орієнтований на формування аналітичних компетентностей у сфері керування доступом. На середньому рівні учні опановують базові концепції IAA та порівнюють основні моделі керування доступом на прикладах реальних систем. Достатній рівень передбачає поглиблений аналіз механізмів автентифікації та авторизації, включаючи сучасні підходи RBAC. На високому рівні учні демонструють здатність синтезувати знання для проєктування систем керування доступом та презентації результатів дослідження.

2.3. Методичні рекомендації щодо здійснення диференційованого навчання вибіркового модуля "Інформаційна безпека" учнів ліцею

2.3.1. Загальні рекомендації щодо проведення практичних робіт

При проведені практичних робіт бажано враховувати індивідуальні особливості учнів. На рис. 2.2 запропонована модель побудови

Таблиця 2.6

Завдання для академічного напрямку “Аналітик систем безпеки”.

РІВЕНЬ	ЗАВДАННЯ
Середній	**Базове дослідження:** 1. Заповніть порівняльну таблицю Дискреційної (DAC) і Мандатної (MAC) моделей керування доступом за критеріями: принцип роботи, переваги, недоліки, приклади застосування 2. Знайдіть 2 реальні приклади використання IAA в українських онлайн-сервісах (Дія, банкінг тощо) 3. Оформити у вигляді аналітичної записки з посиланнями на джерела
Достатній	**Поглиблений аналіз (додатково до середнього рівня):** 1. Порівняти реалізацію автентифікації: однофакторна vs багатофакторна (MFA) 2. Проаналізувати модель RBAC (Role-Based Access Control) та її застосування в освітніх закладах 3. Створити схему взаємозв’язків між компонентами IAA
Високий	**Експертний рівень (додатково до достатнього рівня):** 1. Підготувати порівняльний аналіз моделей керування доступом (DAC, MAC, RBAC, ABAC) з рекомендаціями щодо застосування 2. Розробити проєкт системи керування доступом для шкільної мережі 3. Створити презентацію “Сучасні методи автентифікації: від паролів до біометрії”

індивідуальної освітньої траєкторії кожного учня. Представлена схема відображає повний цикл диференційованого навчання, починаючи від діагностики індивідуальних особливостей учня і завершуючи оцінюванням результатів. Центральною ідеєю моделі є трикомпонентна діагностика учня, що враховує його інтереси, рівень підготовки та стиль навчання. Ці

три параметри формують основу для подальшої індивідуалізації освітньої траєкторії. Система передбачає двоетапний вибір: спочатку визначається напрямок (академічний для майбутніх дослідників, технічний для практиків-інженерів, управлінський для менеджерів), а потім рівень складності завдань – від середнього до високого. Така архітектура забезпечує гнучкість методичної системи та дає змогу адаптувати навчальний процес під індивідуальні потреби кожного учня, що цілком узгоджується з сучасними принципами диференційованого навчання.

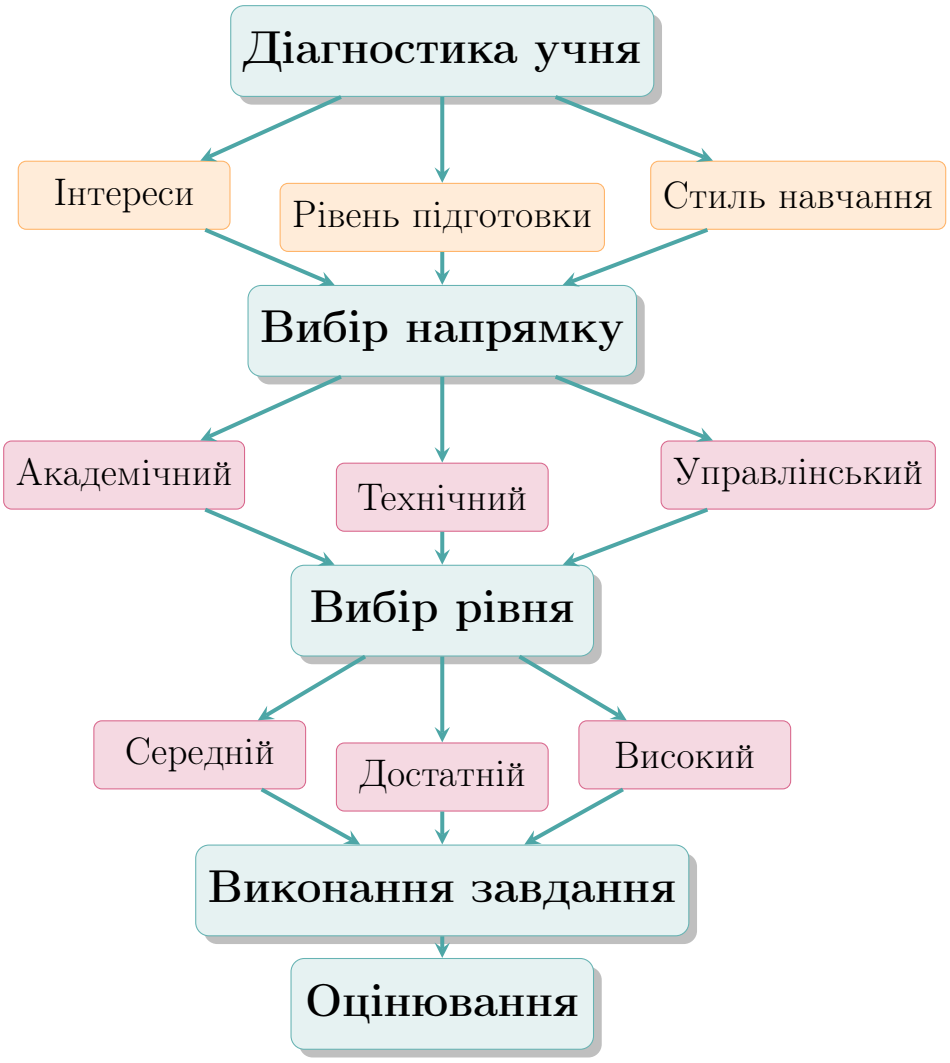

Рис. 2.2. Модель побудови індивідуальної освітньої траєкторії учня.

Ефективна реалізація диференційованого підходу в навчанні інформаційної безпеки потребує створення системи різнорівневих завдань, що враховують не лише рівень підготовки учнів, але й їхні професійні інтереси та майбутню спеціалізацію. Розроблена система диференційованих завдань базується на принципах, визначених у теоретичному розділі робо-

ти, та реалізує багатовимірну модель диференціації навчання.

У процесі розробки системи завдань було реалізовано комплексний підхід до диференціації, що базується на двох ключових вимірах: диференціація за інтересами та рівнева диференціація (табл. 2.7).

Таблиця 2.7

Структура диференціації завдань вибіркового модуля “Інформаційна безпека”.

Вимір диференціації	**Характеристика**	**Реалізація в практичних роботах**
Диференціація за інтересами	Врахування майбутньої спеціалізації учнів та варіативність тематичного наповнення	3 напрямки з урахуванням різних аспектів теми: академічний, технічний, управлінський
Рівнева диференціація	Врахування рівня підготовки та здібностей	3 рівні складності: середній, достатній, високий

Диференціація за інтересами реалізована через створення трьох напрямків завдань, кожен з яких корелює з певною групою майбутніх спеціальностей та професійних інтересів учнів (табл. 2.8). Академічний напрямок “Дослідник безпеки” орієнтований на учнів, які планують обрати гуманітарні та соціальні спеціальності – право, журналістику, соціологію, міжнародні відносини. Технічний напрямок “Етичний хакер” розрахований на майбутніх фахівців у галузі програмування, кібербезпеки та системного адміністрування. Управлінський напрямок “Менеджер безпеки” спрямований на учнів, які цікавляться менеджментом, економікою, бізнесом та державним управлінням. Диференціація за інтересами проявляється у варіативності тематичного наповнення завдань у межах теми. Кожен напрямок акцентує увагу на специфічних аспектах теми, релевантних для майбутньої професійної діяльності учнів.

Рівнева диференціація забезпечує поступове ускладнення завдань від середнього до високого рівня в межах кожного профільного напрямку (табл. 2.9). Така структура дозволяє кожному учневі працювати в зоні най-

Таблиця 2.8

Порівняльна характеристика профільних напрямків.

Критерій	**Академічний напрямок**	**Технічний напрямок**	**Управлінський напрямок**
Цільова аудиторія	Майбутні юристи, журналісти, соціологи	Майбутні програмісти, системні адміністратори	Майбутні менеджери, економісти
Основний фокус	Аналіз, систематизація, дослідження	Практичні навички, тестування, програмування	Планування, бюджетування, управління ризиками
Ключові компетентності	Критичне мислення, аналіз джерел, створення інфопродуктів	Технічні навички, програмування, пентестинг	Стратегічне планування, комплаєнс, управління проектами
Типи завдань	Класифікації, порівняльний аналіз, інфографіка	Сканування, написання скриптів, демонстрації	Матриці ризиків, бюджети, показники ефективності
Кінцевий продукт	Аналітичні звіти, презентації, інфографіка	Технічні звіти, скрипти, відео-демонстрації	Управлінські документи, плани, положення

ближчого розвитку, поступово нарощуючи складність виконуваних завдань відповідно до власного прогресу.

Система оцінювання диференційованих завдань (табл. 2.10) Розроблена чотирирівнева система оцінювання враховує три критерії: повноту виконання завдань, якість аналізу та оформлення результатів.

Високий рівень (10-12 балів) передбачає виконання всіх завдань обраного рівня, глибокий аналіз з власними висновками та структуроване оформлення з візуалізацією. Достатній рівень (7-9 балів) вимагає виконан-

Таблиця 2.9

Прогресія складності завдань за рівнями.

Рівень	**Когнітивні процеси (за таксономією Блума)**	**Характер діяльності**	**Ступінь самостійності**
Середній	Знання, розуміння, застосування	Репродуктивна з елементами продуктивної	Виконання за зразком з детальними інструкціями
Достатній	Аналіз, синтез	Продуктивна з елементами творчої	Часткова самостійність з опорними схемами
Високий	Оцінка, створення	Творча, дослідницька	Повна самостійність, власні рішення

Таблиця 2.10

Критерії оцінювання диференційованих завдань.

Бали	**Повнота виконання**	**Якість аналізу**	**Оформлення результатів**	**Додаткові критерії**
10-12	100% завдань	Глибокий аналіз, власні висновки, критичне мислення	Структуровано, візуалізація, дотримання вимог	Креативність, наднормові елементи
7-9	70-90% завдань	Достатній аналіз, є висновки, логічність	Структуровано, незначні недоліки	Виконано в термін
4-6	50-70% завдань	Поверхневий аналіз, описовий характер	Неструктуровано, без візуалізації	Потребує доопрацювання
1-3	<50% завдань	Відсутній аналіз, фрагментарність	Не відповідає вимогам	Несамостійне виконання

ня 70-90% завдань з достатнім аналізом та структурованим оформленням, хоча можуть бути незначні недоліки. Середній рівень (4-6 балів) характеризується виконанням 50-70% завдань з поверхневим аналізом та неструктурованим оформленням. Початковий рівень (1-3 бали) відповідає виконанню менше 50% завдань без аналізу та з оформленням, що не відповідає вимогам.

Представлені таблиці та схеми ілюструють комплексний підхід до організації диференційованого навчання вибіркового модуля "Інформаційна безпека". Система забезпечує:

- гнучкість вибору – учні можуть обрати напрямок та рівень складності відповідно до власних потреб;
- ррогресивність навчання – поступове ускладнення завдань забезпечує розвиток компетентностей;
- ррактичну спрямованість – завдання орієнтовані на реальні професійні ситуації;
- об'єктивність оцінювання – чіткі критерії забезпечують прозорість та справедливість оцінки;

Важливим аспектом диференційованого навчання є варіативність форм представлення результатів виконання завдань. Кожен профільний напрямок передбачає специфічні формати, що відповідають характеру майбутньої професійної діяльності та розвивають відповідні компетентності (табл. 2.11).

Академічний напрямок акцентує увагу на аналітичних та дослідницьких форматах: письмові роботи формують навички структурованого викладу думок, візуалізація даних розвиває вміння систематизувати інформацію, а підготовка презентацій сприяє формуванню комунікативних компетентностей.

Технічний напрямок орієнтований на практичні результати: технічна документація та програмний код демонструють рівень володіння фаховими інструментами, візуальні матеріали фіксують процес виконання завдань, а використання платформ на кшталт GitHub формує навички командної роботи та версіонування.

Управлінський напрямок зосереджений на документах організаційного характеру: розробка політик та планів розвиває стратегічне мислення, створення дашбордів та матриць ризиків формує аналітичні компетентності, а інтерактивні інструменти демонструють здатність автоматизувати управлінські процеси.

Таблиця 2.11

Форми представлення результатів диференційованих завдань.

Напрямок	**Текстові формати**	**Візуальні формати**	**Інтерактивні формати**
Академічний	Аналітичні звіти, есе, огляди	Інфографіка, діаграми, схеми	Презентації, вебсайти
Технічний	Технічна документація, код	Скріншоти, блок-схеми	Відеодемонстрації, GitHub
Управлінський	Політики, плани, звіти	Дашборди, матриці ризиків	Інтерактивні калькулятори

Така варіативність форм представлення результатів дозволяє учням обирати оптимальний спосіб демонстрації набутих компетентностей відповідно до власних сильних сторін та професійних інтересів, водночас забезпечуючи об'єктивність оцінювання через чіткі критерії для кожного формату.

Запропонована модель може бути адаптована для інших тем курсу зі збереженням основних принципів диференціації.

2.3.2. Методичні рекомендації до Практичної роботи №1

Практична робота №1 "Систематизація загроз та правове поле інформаційної безпеки" є вступною до курсу і закладає фундамент для подальшого вивчення модуля. При її проведенні рекомендується дотримуватися наступних методичних принципів.

Організація навчального простору. На початку заняття вчитель проводить коротке опитування для визначення початкового рівня

обізнаності учнів з питань інформаційної безпеки. Це дозволяє скоригувати темп роботи та обсяг консультативної підтримки для кожної групи. Як зазначають автори [14], включення активних методів навчання до курсів з безпеки програмного забезпечення суттєво підвищує залученість студентів та якість засвоєння матеріалу.

Формування груп. Учні об'єднуються у групи по 3-4 особи відповідно до обраного напрямку (академічний, технічний, управлінський). Важливо забезпечити можливість зміни напрямку протягом перших двох занять, якщо учень усвідомлює, що інший профіль краще відповідає його інтересам. Дослідження авторів [2] підтверджують, що прикладна орієнтація завдань та міждисциплінарна інтеграція є ключовими факторами підвищення мотивації учнів до навчання.

Робота із джерелами інформації. Для виконання завдань середнього рівня учні використовують рекомендовані вчителем джерела: офіційні звіти CERT-UA, матеріали Державної служби спеціального зв'язку та захисту інформації України, новинні публікації про кіберінциденти. Для достатнього та високого рівнів учні самостійно здійснюють пошук додаткових джерел, що розвиває навички критичного аналізу інформації та верифікації даних.

Диференціація консультативної підтримки. Учні середнього рівня отримують покрокові інструкції та шаблони для заповнення. Учні достатнього рівня працюють з частково структурованими матеріалами. Учні високого рівня отримують лише загальні рекомендації, що стимулює самостійність та креативність. Такий підхід узгоджується з результатами дослідження авторів [16], які продемонстрували ефективність поєднання теоретичних занять з практичними hands-on активностями у навчанні кібербезпеки.

Презентація результатів. На другому уроці кожна група представляє результати своєї роботи (3-5 хвилин на групу). Решта учнів заповнюють аркуші взаємооцінювання, що сприяє розвитку критичного мислення та комунікативних навичок. Автори [4] наголошують на важливості інтерактивних scaffolded активностей для ефективного засвоєння складних концепцій.

Оцінювання. Рекомендується використовувати комбіноване

оцінювання: 60% – якість виконання завдання (відповідність критеріям, повнота, коректність), 20% – презентація результатів, 20% – робота в команді та участь в обговоренні. Критерії оцінювання повідомляються учням на початку роботи.

Рефлексія. Наприкінці заняття учні заповнюють коротку анкету самооцінювання, що дозволяє вчителю відстежувати динаміку розвитку компетентностей та коригувати подальшу роботу. Особливу увагу слід приділити зворотному зв'язку щодо складності завдань та зрозумілості інструкцій.

Висновки до 2 розділу

У другому розділі розроблено методичну систему диференційованого навчання вибіркового модуля "Інформаційна безпека" для учнів ліцеїв. Основні результати включають:

1. Здійснено порівняльний аналіз програм навчання інформаційної безпеки для учнів 5-11 класів та обґрунтовано змістовне наповнення вибіркового модуля. Визначено, що модуль охоплює ключові теми: систематизацію загроз, правове поле інформаційної безпеки, керування доступом, криптографічний захист та безпеку в мережі Інтернет.

2. Розроблено календарно-тематичне планування модуля, що включає 8 годин аудиторної роботи та передбачає проведення 2 практичних робіт. Планування враховує принципи поступового ускладнення матеріалу та забезпечує наступність із базовим курсом інформатики.

3. Створено систему диференційованих завдань для трьох профільних напрямків: академічного ("Дослідник безпеки", "Аналітик систем безпеки"), технічного ("Етичний хакер") та управлінського ("Менеджер безпеки"). Кожен напрямок передбачає три рівні складності: середній, достатній та високий.

4. Розроблено детальні завдання для Практичної роботи №1 "Систематизація загроз та правове поле інформаційної безпеки" та Уроку №4 "Керування доступом: ІАА. Дискреційна/Мандатна моделі" з урахуванням специфіки кожного напрямку та рівня складності.

5. Запропоновано модель побудови індивідуальної освітньої траєкторії учня, що базується на трикомпонентній діагностиці (інтереси, рівень підготовки, стиль навчання) та забезпечує гнучкість у виборі напрямку і рівня складності завдань.

6. Визначено форми представлення результатів диференційованих завдань для кожного напрямку: текстові формати (аналітичні звіти, технічна документація, політики), візуальні формати (інфографіка, блок-схеми, дашборди) та інтерактивні формати (презентації, відеодемонстрації, веб-ресурси).

7. Сформульовано методичні рекомендації щодо проведення практичних робіт, включаючи організацію навчального простору, формування груп, диференціацію консультативної підтримки, критерії оцінювання та організацію рефлексії.

Розроблена методична система забезпечує реалізацію принципів диференційованого навчання згідно з моделлю К. Томлінсон та враховує сучасні тенденції у галузі навчання кібербезпеки.

ВИСНОВКИ

У кваліфікаційній роботі досліджено проблему диференційованого навчання інформаційної безпеки учнів ліцеїв та розроблено методичну систему для вибіркового модуля “Інформаційна безпека”. Основні результати дослідження:

1. Проаналізовано сучасний стан навчання інформаційної безпеки у закладах загальної середньої освіти. Встановлено, що попри наявність окремих тем у курсі інформатики, системне вивчення питань кібербезпеки потребує розробки спеціалізованих модулів із урахуванням індивідуальних особливостей учнів.

2. Досліджено теоретичні засади диференційованого навчання на основі аналізу вітчизняних та зарубіжних наукових джерел. Визначено, що модель К. Томлінсон, яка передбачає диференціацію за змістом, процесом, продуктом та середовищем на основі готовності, інтересів та профілю навчання учнів, є оптимальною для застосування у навчанні інформаційної безпеки.

3. Здійснено аналіз міжнародного досвіду навчання кібербезпеки учнів шкіл. Виявлено тенденції до використання практико-орієнтованих методів (CTF-змагання, симуляції, hands-on активності), гейміфікації та диференціації навчального матеріалу відповідно до майбутніх професійних інтересів учнів.

4. Обґрунтовано змістовне наповнення вибіркового модуля «Інформаційна безпека» для учнів ліцеїв на основі аналізу чинних навчальних програм з інформатики та сучасних вимог до компетентностей у сфері кібербезпеки. Розроблено календарно-тематичне планування модуля обсягом 8 годин.

5. Розроблено систему диференційованих завдань для трьох профільних напрямків (академічний, технічний, управлінський) та трьох рівнів складності (середній, достатній, високий). Система забезпечує варіативність освітніх траєкторій та враховує різноманітність професійних інтересів учнів.

6. Запропоновано модель побудови індивідуальної освітньої траєкторії, що включає діагностику індивідуальних особливостей учня, вибір напрямку та рівня складності, виконання завдань та оцінювання результатів. Модель забезпечує гнучкість методичної системи та можливість адаптації до потреб кожного учня.

7. Сформульовано методичні рекомендації щодо здійснення диференційованого навчання вибіркового модуля, включаючи організацію практичних робіт, формування груп, диференціацію консультативної підтримки та критерії оцінювання.

Практичне значення отриманих результатів полягає у можливості використання розробленої методичної системи вчителями інформатики для проведення занять з вибіркового модуля «Інформаційна безпека» в закладах загальної середньої та профільної освіти.

Перспективи подальших досліджень пов'язані з експериментальною перевіркою ефективності розробленої методичної системи, розширенням змісту модуля, створенням електронних освітніх ресурсів для підтримки диференційованого навчання та розробкою системи автоматизованого оцінювання результатів виконання завдань.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Antunes M. J. G.*, *Silva C. S.*, *Marques F.* An integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviours in school context // Applied Sciences. — 2021. — Т. 11, № 23. — С. 11269. — DOI: 10.3390/app112311269.
2. Applied orientation and interdisciplinary integration as a factor in increasing student learning motivation / P. V. Nikitin [та ін.] // Universal Journal of Educational Research. — 2020. — Т. 8, № 10. — С. 4931—4938. — DOI: 10.13189/ujer.2020.081065.
3. *Bilousova L.*, *Kolgatina L.*, *Kolgatin O.* How can we encourage students to manage their own learning? // Ukrainian Journal of Educational Studies and Information Technology. — 2023. — Т. 11, № 1. — С. 55—65. — DOI: 10.32919/uesit.2023.01.05.
4. *Broll B.*, *Grover S.* Beyond Black-Boxes: Teaching Complex Machine Learning Ideas through Scaffolded Interactive Activities // Proceedings of the AAAI Conference on Artificial Intelligence. — 2023. — Т. 37, № 13. — С. 15990—15998. — DOI: 10.1609/aaai.v37i13.26898.
5. Clip thinking of modern pupils / students: observations of teachers of Ukraine / S. Skvortsova [та ін.] // ICERI2021 Proceedings. — Online Conference : IATED, 2021. — С. 2223—2230. — (14th annual International Conference of Education, Research and Innovation). — ISBN 978-84-09-34549-6. — DOI: 10.21125/iceri.2021.0562.
6. Cybersecurity activities for education and curriculum design: A survey / M. Ismail [та ін.] // Computers in Human Behavior Reports. — 2024. — Т. 16. — С. 100501. — DOI: 10.1016/j.chbr.2024.100501.
7. *Jacob J.*, *White G. B.* Is a Significant Demographic Left Out of the Equation? An Overview of Possible Inequitable Access to Cybersecurity Educational Programs in the United States // Proceedings of the Annual Hawaii International Conference on System Sciences. — 2022. — С. 2248—2259. — DOI: 10.24251/hicss.2022.282.

8. *Jerman-Blažič A.*, *Blažić B. J.* Toward effective learning of cybersecurity: new curriculum agenda and learning methods // Journal of Cybersecurity. — 2024. — Т. 10, № 1. — tyae018. — DOI: 10.1093/cybsec/tyae018.

9. *Jerman-Blažič A.*, *Blažić B. J.* Teaching and learning cybersecurity for European youth by applying interactive technology and smart education // Education and Information Technologies. — 2025. — Т. 30, № 7. — С. 9093—9120. — DOI: 10.1007/s10639-024-13155-3.

10. *Jeyamala C.*, *Moorthy A. D.*, *Uma K. V.* An Effective Instructional Design to Enhance Learning Outcomes of Information Security Course in Online Mode // Journal of Engineering Education Transformations. — 2023. — Т. 36, Special Issue 2. — С. 319—325. — DOI: 10.16920/jeet/2023/v36is2/23047.

11. *Karimnia R.*, *Maennel K.*, *Shahin M.* Culturally-sensitive Cybersecurity Awareness Program Design for Iranian High-school Students // Proceedings of the 8th International Conference on Information Systems Security and Privacy - ICISSP. — INSTICC. SciTePress, 2022. — С. 121—132. — ISBN 978-989-758-553-1. — DOI: 10.5220/0010824800003120.

12. Remote Controlled Cyber: Toward Engaging and Educating a Diverse Cybersecurity Workforce / C. Gough [та ін.] // Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1. — Portland, OR, USA : Association for Computing Machinery, 2024. — С. 394—400. — (SIGCSE 2024). — ISBN 9798400704239. — DOI: 10.1145/3626252.3630917.

13. *Spirin O. M.*, *Kovalchuk V. N.* Methodic of the on-line safety of the senior pupils in the teaching and educational process at school // Information Technologies and Learning Tools. — 2011. — Т. 21, № 1. — DOI: 10.33407/itlt.v21i1.411.

14. *Srivatanakul T.*, *Annansingh F.* Incorporating active learning activities to the design and development of an undergraduate software and web security course // Journal of Computers in Education. — 2022. — Т. 9, № 1. — С. 25—50. — DOI: 10.1007/s40692-021-00194-9.

15. The New Ukrainian School: conceptual principles of secondry school reform / O. Elkin [та ін.]. — Kyiv, 2017. — URL: https://mon.gov.ua/storage/app/media/zagalna%20serednya/Book-ENG.pdf.

16. *Toccafondi N.*, *Bilancini E.*, *Boncinelli L.* Learning CyberSecurity with Story-Driven CTF Challenges: CyberTrials 2023 // Higher Education Learning Methodologies and Technologies Online / за ред. G. Casalino [та ін.]. — Cham : Springer Nature Switzerland, 2024. — С. 307—322. — ISBN 978-3-031-67351-1. — DOI: 10.1007/978-3-031-67351-1_21.

17. *Tomlinson C. A.* How to Differentiate Instruction in Mixed-Ability Classrooms. — 2-е вид. — Alexandria, USA : ASCD, 2001. — URL: https://books.google.com.ua/books?id=ivlQBAAAQBAJ&printsec=frontcover&authuser=1#v=onepage&q&f=false.

18. Using Terminal Histories to Monitor Student Progress on Hands-on Exercises / J. Mirkovic [та ін.] // Proceedings of the 51st ACM Technical Symposium on Computer Science Education. — Portland, OR, USA : Association for Computing Machinery, 2020. — С. 866—872. — (SIGCSE '20). — ISBN 9781450367936. — DOI: 10.1145/3328778.3366935.

19. *Wang L.*, *Yang J.*, *Wan P.* Educational modules and research surveys on critical cybersecurity topics // International Journal of Distributed Sensor Networks. — 2020. — Т. 16, № 9. — DOI: 10.1177/1550147720954678.

20. What do high school students know about the field of cyber security? A survey of perception and experiences / S. Mishra [та ін.] // Issues in Information Systems. — 2024. — Т. 25, № 3. — С. 36—46. — DOI: 10.48009/3_iis_2024_104.

21. *Білик Р. М.*, *Ніколаєв О. М.* Реалізація диференційованого навчання у компетентнісній освіті // Збірник наукових праць Кам'янець-Подільського національного університету імені Івана Огієнка. Серія педагогічна. — 2017. — № 23. — С. 121—124. — URL: http://ped-series.kpnu.edu.ua/article/view/125434/119888.

22. *Білоусова Л. І.*, *Колгатіна Л. С.*, *Колгатін О. Г.* ІКТ-орієнтоване управління самостійною роботою майбутніх учителів // Збірник наукових праць «Актуальні питання природничо-математичної

освіти». — 2019. — 2(14). — С. 75—81. — DOI: 10.5281/zenodo.3669035.

23. *Британ Ю.* Англомовні комунікативні ситуації безпечного поводження в Інтернет-просторі та запобігання кібербулінгу (за ресурсами Британської Ради) // Вісник Національного університету "Чернігівський колегіум" імені Т. Г. Шевченка. — 2023. — № 21. — С. 73—77. — DOI: 10.58407/visnik.232112.

24. Віртуальний кабінет інформатики. Інформаційна безпека. — 2023. — URL: https://sites.google.com/view/infbez406/.

25. *Гайдаєнко Н. С., Рашидов С. Ф.* Проблеми та перспективи розвитку інклюзивної освіти в умовах реформування освітньої галузі України // Духовність особистості: методологія, теорія і практика : збірник наукових праць. — 2021. — 3(102). — С. 85—94. — URL: https://journals.snu.edu.ua/index.php/DOMTP_SNU/article/view/62/52.

26. *Засєкіна Т. М.* Розроблення пропедевтичного інтегрованого курсу як складника цілісної природничої освіти // Педагогічна освіта: теорія і практика. — 2020. — 2(29). — С. 171—186. — DOI: 10.32626/2309-9763.2020-29-171-186.

27. Інформатика. Навчальна програма вибірково-обов'язкового предмету для учнів 10-11 класів загальноосвітніх навчальних закладів (Рівень стандарту). — Міністерство освіти і науки України, 2017. — URL: https://mon.gov.ua/storage/app/media/zagalna%20serednya/programy-10-11-klas/2018-2019/informatika-standart-10-11.docx.

28. *Кабінет Міністрів України.* Про деякі питання державних стандартів повної загальної середньої освіти. — Київ, 30.09.2020. — URL: https://zakon.rada.gov.ua/laws/show/898-2020-%D0%BF#Text.

29. Модельна навчальна програма «Інформатика. 5-6 класи» для закладів загальної середньої освіти / Й. Я. Ривкінд [та ін.]. — Міністерство освіти і науки України, 2021. — URL: https://mon.gov.ua/static-objects/mon/sites/1/zagalna%20serednya/Navchalni.prohramy/2021/14.07/Model.navch.prohr.5-9.klas.NUSH-poetap.z.2022/

Inform.osv.haluz.5-6-kl/Inform.5-6-kl.Ryvkind.ta.in.14.07.pdf.

30. Модельна навчальна програма «Інформатика. 7-9 класи» для закладів загальної середньої освіти / Й. Я. Ривкінд [та ін.]. — Міністерство освіти і науки України, 2023. — URL: https://mon.gov.ua/static-objects/mon/sites/1/zagalna%20serednya/Navchalni.prohramy/2023/Model.navch.prohr.5-9.klas/Inform.osv.haluz.2023/16.08.2023/Informatyka.7-9%20kl.Ryvkind.ta.in.16.08.2023.pdf.

31. *Скворцова С.*, *Нєдялкова К.* Методичні підходи, реалізовані у підручнику з математики для учнів 6 класів (за підручником «Математика. 6 клас» Світлани Скворцової та Катерини Нєдялкової) // Український Педагогічний журнал. — 2023. — № 3. — С. 217—226. — DOI: 10.32405/2411-1317-2023-3-217-226.

32. *Трубачева С.*, *Мішеніна Т.*, *Коник О.* Роль електронного портфоліо вчителя як освітнього ресурсу в навчально-методичному забезпеченні процесу подолання освітніх втрат учнів // Проблеми сучасного підручника. — 2024. — № 32. — С. 299—305. — DOI: 10.32405/2411-1309-2024-32-299-305.

33. *У Ю.*, *Пісоцька М. Е.* Підходи науковців України до визначення поняття «диференціація навчання» // Матеріали І Всеукраїнських Прокопенківських читань. — Харків : Харків. нац. пед. ун-т ім. Г. С. Сковороди, 2022. — С. 344—348. — URL: https://dspace.hnpu.edu.ua/server/api/core/bitstreams/82296d03-8b6c-4405-94aa-cf7ff91ccecb/content.

34. *Шаров С.*, *Гладких Г.* Диференціація освітнього процесу як педагогічна проблема // Актуальні питання гуманітарних наук. — 2021. — Т. 3, № 36. — С. 285—289. — DOI: 10.24919/2308-4863/36-3-47. — URL: https://doi.org/10.24919/2308-4863/36-3-47.

35. *Шевчук Л.* Сутність та специфіка поняття «диференціація навчання»: інформація для ознайомлення педагогів // Проблеми сучасного підручника. — 2020. — № 25. — С. 219—227. — DOI: 10.32405/2411-1309-2020-25-219-227. — URL: https://ipvid.org.ua/index.php/psp/article/view/68.

Додаток А.
Детальний аналіз тематичних кластерів досліджень з навчання інформаційній безпеці

Характеристика тематичних кластерів за результатами аналізу VOSviewer.

№	Назва кластера	Ключові терміни	Характеристики	Новітні тренди	Наукові імплікації
1	**Інформаційні технології та їхній вплив на суспільство**	• artificial intelligence (85 зв'язків, 18 появ) • machine learning (середній рік 2022.1) • e-learning (233 зв'язки, 52 появи) • data privacy • virtual reality • social media • covid-19 (середній рік 2022.5)	• Найбільш загальний кластер • Охоплює сучасні технології • Високий середній рік публікацій (2021-2022) • Висока нормалізована цитованість	• Інтеграція ШІ в онлайн-освіту • AI-асистенти для навчання • Адаптивне персоналізоване навчання • VR/AR технології в освіті • Відповідь на виклики пандемії	• Розробка цифрових освітніх систем • Оцінка ефективності AI-платформ • Дослідження впливу технологій на навчання • Етичні питання використання ШІ в освіті
2	**Освіта та обізнаність у сфері інформаційної безпеки**	• education (356 зв'язків, 72 появи) • information security education (45 зв'язків, 12 появ) • security of data (425 зв'язків, 99 появ) • authentication • security awareness • information systems	• Фокус на формальній освіті • Високі показники зв'язків • Фундаментальні теми • Середній рік публікацій 2017-2018	• Розвиток цифрової грамотності • Стандарти кібергігієни • Інтеграція безпеки в навчальні програми • Формування культури безпеки	• Підготовка викладачів • Розробка курсів з ІБ • Політика безпечного навчання • Методики оцінки обізнаності

Табл. .12 – *Продовження*

№	Назва кластера	Ключові терміни	Характеристики	Новітні тренди	Наукові імплікації
3	**Навчання кібербезпеці в освітніх закладах**	• cyber security (1008 зв'язків, 195 появ) • cybersecurity education (209 зв'язків, 49 появ) • capture the flag (CTF) • game-based learning • adversarial machine learning (середній рік 2024.3) • k-12 education	• Найпотужніший кластер за зв'язками • Активні сучасні дослідження • Інноваційні методи навчання • Орієнтація на школярів	• CTF-змагання як метод навчання • Симуляції кібератак • Практична hands-on підготовка • Включення ML/AI в безпеку • Геймифіковане навчання	• Методики практичного навчання • Розробка навчальних симуляторів • Адаптація для різних вікових груп • Оцінка ефективності ігрових методів
4	**Тренування персоналу в галузі кібербезпеки**	• cybersecurity (862 зв'язки, 195 появ) • computer crime (182 зв'язки, 29 появ) • network security (281 зв'язок, 52 появи) • personnel training • serious games • gamification	• Фокус на професійній підготовці • Висока цитованість (14.3 для computer crime) • Практична спрямованість • Використання серйозних ігор	• Інцидент-менеджмент у школах • Викладання через симулятори • Серйозні ігри для тренування • Сценарії реагування на загрози	• Інтеграція кіберзахисту в лабораторії • STEM-курси з кібербезпеки • Підвищення кваліфікації вчителів • Розробка тренінгових програм
5	**Освіта в комп'ютерних науках та інженерії**	• students (1008 зв'язків, 190 появ) • computer science education • curricula (433 зв'язки, 76 появ) • engineering education (402 зв'язки, 73 появи) • teaching • k-12, middle school	• Студенто-центрований підхід • Академічна спрямованість • Фокус на навчальних програмах • Охоплення різних освітніх рівнів	• Розвиток інформатики в школах • STEAM-підходи • Інтеграція з математикою та науками • Проектне навчання	• Впровадження інформатики в програми • Оцінка ефективності навчання • Розробка стандартів освіти • Підготовка навчальних матеріалів

Основні висновки з кластерного аналізу:

1. **Домінуючі теми:** кібербезпека (“cyber security”, “cybersecurity”) є центральною темою дослідження з найвищими показниками зв’язків (1008) та кількості поява (195) у кількох кластерах.

2. **Взаємозв’язок тематик:** існує сильний зв’язок між темами кібербезпеки та освітою, що видно з багатьох термінів-мостів між кластерами (“cyber-security educations”, “cybersecurity education”, “information security education”).

3. **Часова актуальність:** дослідження в галузі кібербезпеки, штучного інтелекту та машинного навчання є найбільш актуальними (середні роки публікації 2021-2024), що свідчить про активний розвиток цих напрямів.

4. **Інновації в навчанні:** використання “gamification”, “serious games”, “capture the flag” та “game-based learning” вказує на пошук нових, інтерактивних підходів до навчання кібербезпеці.

5. **Фокус на аудиторії:** значна увага приділяється різним групам учнів: “students” (190 появ), “high school students”, “k-12 education”, “middle school”, “primary schools”, “secondary schools”, “teachers”, “personnel”, що свідчить про диференційований підхід до навчання.

6. **Міждисциплінарність:** перетин технічних (cybersecurity, network security), педагогічних (education, teaching) та соціальних (awareness, privacy) аспектів демонструє комплексний характер проблеми.