Міністерство освіти і науки України
Криворізький національний університет
Факультет інформаційних технологій
Кафедра професійної та соціально-гуманітарної освіти

ЛОГВИНЕНКО Віолетта Валеріївна

Магістерська робота

ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ ДЛЯ ФОРМУВАННЯ НАВИЧОК З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗДОБУВАЧІВ ФАХОВОЇ ПЕРЕДВИЩОЇ ОСВІТИ

за спеціальністю 015 «Професійна освіта (цифрові технології)»

Науковий керівник:
кандидат педагогічних наук,
доцент
Єчкало Юлія Володимирівна

Допущено до захисту
«___»_____ 2025 р.
Завкафедри ПСГО _____ С. М. Хоцкіна

Робота захищена «___»_____ 2025 р. з оцінкою _____
Голова ЕК_____ _____

КРИВИЙ РІГ – 2025

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ІБ – інформаційна безпека

ІКТ – інформаційно-комунікаційні технології

ФПО – фахова передвища освіта

ЦТ – цифрові технології

ЗМІСТ

ВСТУП

Актуальність дослідження. Сучасний етап розвитку суспільства характеризується інтенсивною цифровізацією, яка впливає на всі аспекти життя, зокрема й освіту. Використання цифрових технологій у закладах фахової передвищої освіти стає не лише засобом підвищення якості навчання, а й необхідною умовою формування у здобувачів ключових компетентностей для життя і професійної діяльності.

Особливої ваги набуває питання формування навичок інформаційної безпеки, оскільки цифрове середовище, поряд із широкими можливостями для навчання, комунікації та розвитку, створює і низку ризиків: кіберзагрози, поширення недостовірної інформації, витік персональних даних, маніпулятивний інформаційний вплив. Це актуалізує потребу у підготовці здобувачів освіти до безпечного та відповідального користування цифровими ресурсами, розвитку їх критичного мислення та інформаційної культури.

Важливим завданням закладів фахової передвищої освіти є створення освітнього середовища, яке забезпечить не лише засвоєння теоретичних знань, а й практичне формування навичок безпечної роботи з інформацією та цифровими інструментами. Це вимагає від педагогів упровадження сучасних методик та інноваційних освітніх технологій, здатних інтегрувати знання з інформаційної безпеки у навчальний процес.

Науково-методичні та психолого-педагогічні аспекти цифровізації освіти розглядалися у працях В. Бикова, І. Дичківської, Л. Лупаренко, С. Семерікова, О. Спіріна, В. Ткачук, А. Яцишин та інших науковців. Різні аспекти формування інформаційної культури та безпечної поведінки в цифровому середовищі досліджували А. Гедзик, Г. Дей, В. Дубинський, В. Ігнатенко, А. Литвинчук, Ю. Мирошниченко, І. Радомський, А. Чорномидз.

Однак проблема цілеспрямованого використання цифрових технологій саме для формування навичок інформаційної безпеки здобувачів фахової передвищої освіти ще не отримала належного висвітлення. Виходячи з актуальності зазначеної проблеми обрано тему дослідження: **«Використання цифрових технологій для формування навичок з інформаційної безпеки здобувачів фахової передвищої освіти»**.

Об'єкт дослідження – освітній процес у закладах фахової передвищої освіти.

Предмет дослідження – використання цифрових технологій з метою формування навичок з інформаційної безпеки у здобувачів фахової передвищої освіти.

Мета дослідження: обґрунтування і розробка методики використання цифрових технологій для формування навичок з інформаційної безпеки здобувачів фахової передвищої освіти.

Теоретичний аналіз проблеми, вивчення педагогічного досвіду дозволили висунути **гіпотезу**: використання цифрових технологій для формування навичок з інформаційної безпеки здобувачів фахової передвищої освіти буде ефективним за таких організаційно-педагогічних умов:

– реалізація мобільного навчання як форми організації навчальної діяльності з формування навичок інформаційної безпеки здобувачів фахової передвищої освіти;

– впровадження технології гейміфікації як інноваційного засобу організації навчальної діяльності з формування навичок інформаційної безпеки здобувачів фахової передвищої освіти.

Відповідно до мети, об'єкта, предмета й гіпотези дослідження були поставлені такі **завдання**:

1) проаналізувати науково-методичну, психолого-педагогічну та навчальну літературу з проблеми дослідження;

2) визначити та теоретично обґрунтувати організаційно-педагогічні умови використання цифрових технологій у формуванні навичок інформаційної безпеки;

3) розробити модель використання цифрових технологій для формування навичок з інформаційної безпеки у здобувачів фахової передвищої освіти;

4) упровадити елементи методики використання цифрових технологій для формування навичок з інформаційної безпеки здобувачів фахової передвищої освіти;

5) експериментально перевірити методику використання цифрових технологій для формування навичок з інформаційної безпеки здобувачів фахової передвищої освіти.

У дослідженні для розв'язання поставлених завдань використовувалися такі **методи дослідження**:

– теоретичні (вивчення, аналіз і узагальнення науково-педагогічних, психолого-педагогічних, методичних джерел, а також нормативно-правових документів з проблеми формування навичок з інформаційної безпеки; порівняння, систематизація та класифікація наукових підходів до використання цифрових технологій у процесі підготовки здобувачів освіти);

– емпіричні (педагогічне спостереження за освітнім процесом, анкетування й опитування здобувачів фахової передвищої освіти з метою виявлення рівня сформованості навичок з інформаційної безпеки; проведення педагогічного експерименту для перевірки ефективності застосування цифрових технологій у навчальному процесі; тестування для визначення динаміки розвитку зазначених навичок);

– математичні (кількісний та якісний аналіз результатів педагогічного експерименту із застосуванням методів статистичної обробки даних з метою обґрунтування достовірності отриманих результатів).

Теоретичне значення дослідження полягає у визначенні та

обґрунтуванні організаційно-педагогічних умов ефективного використання цифрових технологій для формування навичок з інформаційної безпеки у здобувачів фахової передвищої освіти.

Практичне значення отриманих результатів полягає у розробленні методичних рекомендацій щодо використання цифрових технологій для формування навичок з інформаційної безпеки здобувачів фахової передвищої освіти.

Дослідно-експериментальна робота проводилася на базі закладу фахової передвищої освіти ВСП «Гірничо-електромеханічний фаховий коледж» Криворізького національного університету.

Структура дослідження: науково-дослідна робота складається зі вступу, трьох розділів, висновків до розділів, висновків, списку використаних джерел, додатків.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ОСНОВИ ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ ДЛЯ ФОРМУВАННЯ НАВИЧОК З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗДОБУВАЧІВ ФАХОВОЇ ПЕРЕДВИЩОЇ ОСВІТИ

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ ДЛЯ ФОРМУВАННЯ НАВИЧОК З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗДОБУВАЧІВ ФАХОВОЇ ПЕРЕДВИЩОЇ ОСВІТИ

1.1 Стан дослідження проблеми формування навичок з інформаційної безпеки здобувачів фахової передвищої освіти

Трансформація освітнього простору під впливом цифрових технологій створює принципово нові умови функціонування системи освіти. Інтенсивна інтеграція інформаційно-комунікаційних технологій (ІКТ) у навчальний процес, перехід на змішані та дистанційні форми навчання, широке використання освітніх платформ формують цифрове освітнє середовище, яке, поряд з новими можливостями, породжує серйозні виклики у сфері інформаційної безпеки (ІБ).

Правове регулювання питань ІБ в системі освіти України базується на низці законодавчих актів. Закон України «Про освіту» [15] визначає цифрову компетентність як одну з ключових компетентностей, необхідних для успішної життєдіяльності. Закон України «Про фахову передвищу освіту» [16] встановлює вимоги до формування професійних компетентностей, які включають здатність до використання інформаційних технологій у професійній діяльності.

Освітні стандарти фахової передвищої освіти (ФПО) включають вимоги щодо формування інформаційно-цифрової компетентності, яка передбачає здатність безпечно використовувати цифрові технології. Проте аналіз чинних стандартів, виконаний авторами монографії [42], показує, що питання ІБ часто розглядаються фрагментарно, без системного підходу до формування

відповідних навичок.

Сучасний стан дослідження проблеми ІБ в освіті характеризується міждисциплінарним підходом, який охоплює технічні, організаційні, правові та педагогічні аспекти забезпечення безпечного освітнього середовища. У вітчизняній науковій думці особлива увага приділяється питанням формування компетентностей з ІБ у здобувачів освіти та педагогів (А. Гедзик [5]; О. Муковіз, Л. Красюк [29]), розвитку цифрової та безпекової культури (І. Чичкань, С. Спасітєлєва, Ю. Жданова [47]), а також захисту персональних даних в умовах цифрової трансформації та євроінтеграції (А. Литвинчук та ін. [18]). Значна частина досліджень спрямована на виявлення загроз і викликів, що постають перед закладами освіти в умовах воєнного стану (Г. Дей [10]; А. Чорномидз [48]; І. Радомський [35]), а також на створення безпечних освітніх екосистем [33]. Зарубіжні науковці акцентують увагу на питаннях підготовки фахівців з кібербезпеки у закладах професійної освіти, інтеграції безпекової освіти в навчальні програми (J. Kuforiji [55]; L. Shihua et al. [59]; G. Vladut, I. Hamburg [61]), а також впровадженні інноваційних підходів до навчання ІБ через гейміфікацію та цифрові технології (X. Yang, C. Yang [62]). Таким чином, наукові дослідження засвідчують зростання ролі ІБ як ключової складової освітньої політики та педагогічної практики в умовах глобальних інформаційних викликів.

Як зазначено у статті [48], основою ІБ в освіті є модель CIA (Confidentiality, Integrity, Availability), тобто: конфіденційність, цілісність, доступність (рис. 1.1).

Різні автори [19; 20; 33] акцентують увагу на специфічних складових поняття ІБ – від захисту інформаційних ресурсів і персональних даних до формування інформаційної культури та критичного мислення учасників освітнього процесу. Для систематизації наукових підходів до визначення сутності ІБ в освіті доцільно проаналізувати найбільш репрезентативні

тлумачення, подані дослідниками (табл. 1.1).

Рис. 1.1 Модель CIA

Таблиця 1.1

Систематизація наукових підходів до визначення сутності ІБ в освіті

Автор(и)	Визначення
О. Чубукова, І. Пономаренко [49]	ІБ закладу освіти – це «складна система, яка передбачає захист наявного в організації інформаційного простору та унеможливлює пошкодження або викрадення персональних даних усіх учасників освітнього процесу, а також інформації, що дозволяє установі функціонувати та має грошову, освітню, інтелектуальну цінність».
І. Радомський [35]	ІБ в освіті – «комплекс заходів, спрямованих на захист інформації користувача незалежно від того, де вона зберігається чи якими носіями використовується, з урахуванням специфічних аспектів довіри й ідентичності, на яких базується взаємодія та спілкування між учасниками освітнього процесу».
І. Цісарук, В. Цісарук, О. Омельчук [46]	ІБ в освітньому середовищі – це «стан захищеності учасників освітнього процесу від інформаційних загроз в мережі Інтернет, що включає захист від ризиків пов'язаних із вмістом матеріалів, небажаними контактами, комерційними загрозами та неправомірним використанням персональних даних».
В. Биков [1]	ІБ в освіті – це «забезпечення інформаційно-комунікаційних потреб учасників навчально-виховного процесу з одночасним захистом засобів, технологій та інформаційних ресурсів від несанкціонованого доступу, що включає оцінювання компетентностей педагогів та учнів щодо критичного оцінювання ресурсів Інтернету».
А. Литвинчук та ін. [18]	ІБ в освітніх інформаційних системах – «забезпечення конфіденційності, цілісності та доступності персональних даних учасників освітнього процесу відповідно до принципів законності та добросовісної обробки в умовах цифрової трансформації, що вимагає поєднання технічних, організаційних та правових інструментів».

У контексті нашого дослідження *інформаційну безпеку* доцільно визначати як *стан захищеності освітнього середовища, що забезпечує конфіденційність, цілісність і доступність інформації та персональних даних усіх учасників освітнього процесу, запобігає інформаційним загрозам і несанкціонованому доступу, а також передбачає формування у здобувачів ФПО відповідних навичок*.

Воєнний стан в Україні суттєво загострив проблему ІБ в освітньому середовищі. За даними досліджень [33; 35; 48; 57], проведених у 2022-2024 роках, спостерігається значне зростання кількості кібератак на освітні установи, витоків персональних даних учасників освітнього процесу та випадків поширення дезінформації через освітні платформи.

Так, А. Чорномидз у своєму дослідженні [48] виділяє основні загрози, з якими стикаються учасники освітнього процесу: фішинг; шкідливе програмне забезпечення; DDoS-атаки; ризики розголошення особистої інформації; використання соціальних мереж як інструменту пропаганди та дезінформації. Автор наголошує на психологічних чинниках, які впливають на здатність зберігати інформаційну стійкість в умовах інформаційного перевантаження та емоційного вигорання.

Г. Дей у роботі [10] описав основні види кіберзлочинів, які є характерними для закладів освіти: фішинг і соціальна інженерія; програми-вимагачі; DDoS-атаки; крадіжка особистих і академічних даних; кібербулінг та онлайн-харасмент; неправомірний контент і його поширення.

І. Радомський у статті [35] акцентує увагу на тому, що прискорене переміщення навчання в онлайн-формат не супроводжувалося належною підтримкою з питань ІБ. Науковець виділяє три групи інформації, яка потребує захисту в освітніх установах: 1) персональні дані учасників освітнього процесу; 2) інформація що забезпечує освітній процес (освітні програми, бази даних, бібліотеки); 3) наукові напрацювання з ознаками інтелектуальної власності.

Дослідники X. Yang, C. Yang також зазначають, що специфіка ФПО створює додаткові виклики у формуванні навичок ІБ. Здобувачі цього рівня освіти знаходяться у віковій категорії 15–20 років, яка характеризується високим рівнем довіри до інформації в соціальних мережах; схильністю до надмірного розкриття персональної інформації онлайн; недооцінкою ризиків цифрового середовища; впливом групового тиску на онлайн-поведінку [62].

І. Цісарук, В. Цісарук та О. Омельчук у дослідженні [46] виділяють чотири загальні категорії ризику для здобувачів освіти:

1) ризик, пов’язаний із вмістом матеріалів в Інтернеті;

2) ризик небажаних контактів;

3) комерційний ризик;

4) ризик використання персональних даних.

Дослідники зазначають, що в межах розроблення ефективної стратегії ІБ закладів освіти необхідно враховувати нормативно-правове забезпечення, організаційні аспекти, профілактичну роботу, адміністративно-організаційний, фізичний і технічний напрями [44]. Одним з основних нормативних документів, які регулюють питання ІБ, є Закон України «Про захист персональних даних» [34], і саме його потрібно брати за основу для роботи з чутливою інформацією про учасників освітнього процесу.

Автори статті [18] розглядають проблему в контексті адаптації української освітньої системи до європейських стандартів. Дослідження показує суттєві відмінності між підходами ЄС та України в контексті правового регулювання, інституційної структури, технічних стандартів і прав суб’єктів персональних даних. Аналіз міжнародного досвіду показує різноманітні підходи до формування навичок інформаційної безпеки. У країнах ЄС діє комплексна система регулювання, що передбачає інтеграцію заходів безпеки на всіх етапах роботи з даними.

Отже, узагальнивши сучасні дослідження проблеми ІБ у закладах освіти,

можна виділити наступні основні загрози ІБ, з якими стикаються учасники освітнього процесу в Україні (табл. 1.2). Ці загрози вимагають комплексного підходу до забезпечення ІБ, що включає технічні, організаційні, поведінкові та психологічні заходи захисту для всіх учасників освітнього процесу.

Таблиця 1.2

Основні загрози ІБ, з якими стикаються учасники освітнього процесу в Україні

Вид загрози	Назва	Опис та можливі наслідки
Кіберзагрози та технічні атаки	Фішинг	Один з найефективніших інструментів кіберзлочинців, особливо в період тривожності та інформаційного перевантаження. Викладачі та здобувачі отримують підроблені листи, замасковані під офіційні повідомлення від керівництва, з темами про «термінове оновлення облікових записів», «зміни у процедурі евакуації» або «інансову допомогу від держави». Перехід за такими посиланнями веде до фальшивих сторінок авторизації, де відбувається крадіжка облікових даних.
	Шкідливе програмне забезпечення	Поширюється через підроблені документи (інструкції, списки, новини), заражені архіви в групах викладачів або компрометовані сайти зі зниженими рівнями безпеки. Зловмисники використовують трояни та програми-вимагачі, які крадуть збережені паролі, шифрують дані або блокують доступ до важливої інформації, вимагаючи викуп.
	DDoS-атаки	Такі атаки нечасто спрямовані особисто на викладачів або здобувачів, проте можуть вивести з ладу онлайн-платформи навчання (Zoom, Moodle, Google Workspace, Microsoft Teams), порушують проведення занять і руйнують довіру до цифрової стабільності навчального процесу.
Загрози конфіденційності персональних даних	Розголошення особистої інформації	Стало особливо небезпечним в умовах воєнного стану. Публікації з геолокацією, згадки про маршрути переміщення, участь у гуманітарних місіях, поширення номерів, адрес або інформації про дітей і родину можуть бути використані у ворожих цілях. Викладачі, які діляться такою інформацією в соціальних мережах, стають об’єктами дзвінків із погрозами або маніпуляціями.
	Витік персональних даних	Може відбуватися через незахищені бази даних закладів освіти, недостатній захист інформаційних систем або людські помилки. Це включає списки здобувачів, службову інформацію, персональні дані викладачів та адміністрації.

Вид загрози	Назва	Опис та можливі наслідки
Загрози через соціальні мережі та месенджери	Злам акаунтів	Призводить до поширення неправдивих дописів від імені учасників освітнього процесу. Масовані інформаційні атаки через Telegram-канали, TikTok і псевдопатріотичні сторінки можуть використовуватися для дискредитації закладів освіти.
	Маніпулятивні повідомлення	Повідомлення в месенджерах, запрошення до «неофіційних груп» із фейковим адміністратором можуть стати каналами впливу та поширення шкідливого контенту.
Дезінформація та пропаганда	Дезінформаційні кампанії	Підривають довіру до офіційних рішень, створюють паніку серед викладачів і здобувачів, спрямовані на деструкцію авторитету науки та освіти. Викладачі як інтелектуальні лідери особливо вразливі до маніпулятивних звітів, фальсифікованих інтерв'ю, спотворених цитувань.
	Фейкові новини	Можуть поширюватися через компрометовані акаунти у соціальних мережах, наприклад, фальшива «заява МОН про припинення навчання в регіоні».
Психологічні загрози	Соціальна інженерія	Зловмисники використовують психологічні методи маніпулювання для отримання конфіденційної інформації або доступу до систем. Це включає обман, створення правдоподібних приводів для контакту, заманювання на шкідливі ресурси через використання тем, що викликають емоційну реакцію в умовах війни.
	Інформаційна втома та когнітивне перевантаження	Виникають внаслідок безперервного потоку тривожних або суперечливих новин, що знижує здатність обробляти й аналізувати інформацію, підвищує вразливість до дезінформації.
	Емоційне виснаження та вигоряння	Посилюються постійним тиском, необхідністю підтримувати освітній процес, високими очікуваннями та відчуттям постійного тиску.
	Емоційні атаки в інформаційному середовищі	Через публічні обговорення або осуд у соцмережах, інформаційні провокації, персональні атаки через фейкові профілі дестабілізують психологічний стан і знижують готовність до конструктивної професійної комунікації.
Організаційно-технічні проблеми	Використання застарілих і небезпечних платформ	Встановлення піратського програмного забезпечення, низька кваліфікація обслуговуючого персоналу (або взагалі відсутність фахівця з підтримки інформаційних систем), відсутність практики регулярного контролю безпеки створюють додаткові вразливості в системі ІБ закладу освіти.
	Відсутність чітких інструкцій	Відсутність чітких інструкцій щодо ІБ в деяких закладах освіти, обмеженість ресурсів (немає VPN, недостатній захист Wi-Fi у гуртожитках) та

Вид загрози	Назва	Опис та можливі наслідки
		необхідність самостійно шукати способи захисту без належної технічної підтримки ускладнюють забезпечення безпеки.
Загрози для здобувачів	Цифровий булінг	Недостовірна інформація, кібершахрайство, пропаганда терористичної та екстремістської діяльності становлять серйозну загрозу для молодого покоління, яке постійно взаємодіє з онлайн-ресурсами.
	Вразливість до негативного інформаційного впливу	Може призвести до агресивної поведінки по відношенню до оточуючих або закладу освіти.

У межах цього дослідження ми приділяємо особливу увагу формуванню навичок з ІБ здобувачів ФПО. Поняття навичок ІБ охоплює широкий комплекс знань, умінь і ціннісних орієнтацій, спрямованих на забезпечення особистої та інформаційної захищеності в цифровому просторі. Ці навички включають усвідомлення різновидів загроз (крадіжки даних, хакерських атак, шахрайства, фішингу тощо), а також здатність розпізнавати й запобігати таким загрозам. Не менш важливим є опанування безпечних практик створення та зберігання паролів, розуміння механізмів захисту персональних даних і конфіденційної інформації [54].

ІБ передбачає також уміння налаштовувати параметри конфіденційності на різних онлайн-платформах та критично ставитися до інформаційних потоків у мережі Інтернет. Базовим компонентом цього процесу є інформаційна грамотність, що включає здатність розпізнавати дезінформацію, оцінювати достовірність джерел і розуміти можливі упередження, притаманні різним форматам медіа [53].

Важливу роль у ІБ безпеки відіграє комп’ютерна грамотність – знання принципів функціонування апаратного забезпечення, операційних систем, програмних застосунків і протоколів безпеки. Разом із цим необхідним є усвідомлення правових та етичних аспектів діяльності в Інтернеті, дотримання

норм цифрової етики та практикування відповідальної поведінки у віртуальному середовищі [54].

До системи навичок ІБ належать і навички цифрової комунікації, які забезпечують безпечну, етичну та доброзичливу взаємодію в онлайнових спільнотах. Вони передбачають розуміння норм мережевого етикету, ризиків кібербулінгу, а також наслідків некоректного чи необережного спілкування.

Застосування практичних методів ІБ – таких як використання антивірусного програмного забезпечення, управління паролями, дотримання правил безпечного перегляду вебресурсів – є необхідною умовою захисту персональних даних і цифрових активів. Крім того, формування культури етичного користування технологіями сприяє підвищенню рівня безпеки та психологічного благополуччя користувачів, а також забезпечує повагу до прав і приватності інших осіб [54].

Використаємо у нашому дослідження відначення навичок ІБ, сформульоване В. Дубинським. *Навички з інформаційної безпеки – це «сукупність знань та умінь для безпечного, відповідального та етичного використання цифрових технологій, яка забезпечує особі захист особистих даних, цифрової ідентичності, пристроїв і мереж від кібератак, а також сприяє свідомому онлайн-спілкуванню»* [13, с. 45].

Навички з ІБ охоплюють технічні, інформаційні, комунікаційні та правові аспекти діяльності в цифровому середовищі (рис. 1.2).

Таким чином, система ФПО опинилася перед необхідністю швидкої адаптації до нових безпекових викликів. Водночас аналіз наукових досліджень та освітньої практики виявляє суттєві прогалини в теоретико-методологічному забезпеченні процесу формування навичок ІБ. Відсутність системного підходу, фрагментарність освітніх програм, недостатня підготовленість педагогічних кадрів створюють розрив між реальними потребами в забезпеченні ІБ та можливостями освітньої системи відповісти на ці виклики.

Тому дослідження проблеми формування навичок з ІБ здобувачів ФПО є актуальним науковим завданням, вирішення якого має важливе теоретичне та практичне значення.

Рис. 1.2 Навички з інформаційної безпеки

1.2 Цифрові технології як засіб формування навичок з інформаційної безпеки

Рамка цифрової компетентності для громадян України (DigComp UA for Citizens), яка визначає ключові компетентності для життя та роботи в цифровому суспільстві, виділяє безпеку як одну з п’яти основних областей цифрової компетентності. Четверта область компетентності «Безпека» включає такі ключові компоненти: захист пристроїв, захист персональних даних та конфіденційності, захист здоров’я та благополуччя, а також захист навколишнього середовища [36]. Це підкреслює критичну важливість формування навичок ІБ як невід’ємної складової цифрової грамотності сучасного громадянина.

Автори посібника [34] стверджують, що для ефективного формування навичок з ІБ необхідно активно використовувати саме ті цифрові технології (ЦТ), безпечному поводженню з якими потрібно навчити. Це створює унікальну освітню ситуацію, коли інструмент навчання одночасно є і предметом вивчення. ЦТ виступають не лише як засіб доставки навчального контенту, але й як середовище для практичного відпрацювання навичок безпечної поведінки в кіберпросторі.

Використання ЦТ для формування навичок ІБ має кілька переваг [20]:

– забезпечення автентичність навчального досвіду – здобувачі вчаться захищати ті самі системи та застосунки, які використовують щоденно;

– створення безпечних просторів для експериментів з потенційно небезпечними технологіями без ризику реальної шкоди;

– перетворення складних концепцій ІБ на більш доступні для розуміння.

Сучасні освітні технології – від масових відкритих онлайн-курсів до мобільних застосунків та віртуальних лабораторій – створюють безпрецедентні

можливості для масштабного та ефективного навчання ІБ. Інтеграція цих технологій в освітній процес дозволяє подолати традиційні обмеження, пов’язані з браком спеціалізованого обладнання, кваліфікованих викладачів та актуальних навчальних матеріалів, роблячи якісну освіту з ІБ доступною для широкого кола здобувачів освіти [18].

Сучасне навчальне середовище характеризується широким спектром *відкритих навчальних ресурсів*, які можуть ефективно використовуватися для формування навичок з ІБ. На думку В. Бикова, ці ресурси можна класифікувати за кількома критеріями: за типом доступу (безкоштовні та умовно-безкоштовні); за мовою викладання (україномовні, англомовні, мультимовні); за рівнем складності (початковий, середній, професійний); за форматом подання матеріалу (відеокурси, інтерактивні платформи, текстові матеріали) [1].

Ефективне використання відкритих навчальних ресурсів потребує чіткого визначення критеріїв їх відбору та розробки методики інтеграції в освітній процес для здобувачів ФПО. Узагальнимо ці критерії за [11; 41] (табл 1.3).

Таблиця 1.3

Критерії відбору відкритих навчальних ресурсів

Критерій	Опис критерію
Організаційний	Включає оцінку доступності ресурсу, зручності інтерфейсу користувача, можливості реєстрації необмеженої кількості користувачів та наявності різних ролей (здобувач, викладач, адміністратор). Важливим аспектом є технічні вимоги до обладнання та програмного забезпечення, необхідного для використання ресурсу.
Функціонально-дидактичний	Охоплює відповідність програми курсу освітнім стандартам та навчальним планам, модульність структури, різноманітність форматів представлення навчального матеріалу, наявність системи тестування, електронного журналу успішності та календаря навчальних подій. Особливе значення має можливість отримання сертифікатів після успішного завершення курсу, що підвищує мотивацію до навчання.
Змістовий	Передбачає оцінку актуальності та достовірності навчального матеріалу, його відповідності сучасному стану розвитку технологій ІБ, наявності практичних прикладів та кейсів з реальної практики. Важливою є адаптація контенту до специфіки професійної діяльності майбутніх фахівців та врахування галузевих особливостей застосування заходів ІБ.

Розглянемо приклади відкритих навчальних ресурсів з ІБ, відібрані за наведеними у табл. 1.3 критеріями.

Міжнародна мережева академія CISCO представляє один з найбільш комплексних наборів курсів з ІБ. Програма «Introduction to Cybersecurity» охоплює базові концепції захисту інформації та спрямована на формування первинного розуміння кіберзагроз та методів протидії їм. Курс «Cybersecurity Essentials» поглиблює знання здобувачів, розглядаючи технічні аспекти захисту мереж, криптографії та управління інцидентами безпеки. Для підготовки професіоналів початкового рівня пропонуються спеціалізовані програми «CCNA Cybersecurity Operations» та «CCNA Security», які включають практичні лабораторні роботи та симуляції реальних сценаріїв кібератак. Важливою перевагою курсів CISCO є їх модульна структура, що дозволяє адаптувати навчальний процес до індивідуальних потреб здобувачів. Кожен модуль містить теоретичний матеріал, представлений у різних форматах (текст, відео, інтерактивні презентації), практичні завдання, тестові питання для самоперевірки та підсумкові іспити. Система автоматичного оцінювання забезпечує миттєвий зворотний зв’язок, що сприяє ефективному засвоєнню матеріалу [50].

Microsoft Virtual Academy пропонує спеціалізовані курси, орієнтовані на вивчення технологій безпеки в екосистемі Microsoft. Курс «Introduction to security in Microsoft 365» складається з 7 модулів, які охоплюють питання управління ідентифікацією, захисту даних, забезпечення відповідності нормативним вимогам та реагування на інциденти. Програма «Secure your organization with built-in, intelligent security from Microsoft 365» фокусується на практичних аспектах впровадження комплексних рішень безпеки в корпоративному середовищі [56].

Платформа Coursera надає доступ до 41 курсу з кібербезпеки від провідних університетів та технологічних компаній світу. Особливу увагу

заслуговує спеціалізація «Cybersecurity for Business», яка орієнтована на формування управлінських компетентностей у сфері ІБ. Курс «IT Fundamentals for Cybersecurity Specialization» забезпечує фундаментальну підготовку з основ інформаційних технологій, мережевих протоколів та операційних систем, що є необхідною базою для подальшого вивчення спеціалізованих аспектів ІБ [51].

Вітчизняні освітні платформи також активно розвивають напрямок навчання інформаційній безпеці. Платформа Prometheus представляє масовий відкритий онлайн-курс «Основи інформаційної безпеки», розроблений фахівцями КПІ ім. Ігоря Сікорського (рис. 1.3). Курс зосереджується на формуванні базових правил поводження з персональною інформацією в умовах реального зближення фізичного та віртуального світів, приділяючи особливу увагу питанням безпеки електронних фінансів [58].

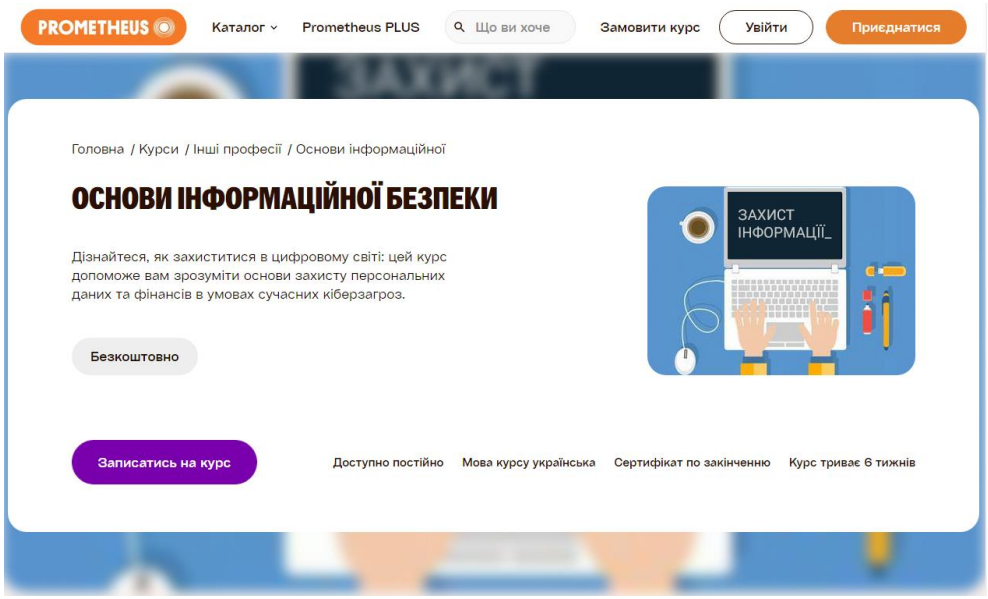


Рис. 1.3 Онлайн-курс «Основи інформаційної безпеки» на платформі Prometheus

Особливе місце серед вітчизняних освітніх ініціатив у сфері ІБ займає національна онлайн-платформа «Дія.Освіта», яка стала важливим елементом державної стратегії цифрової трансформації України. За запитом «інформаційна безпека» на платформі можна знайти 75 різноманітних навчальних матеріалів:

освітні серіали, гайди, симулятори тощо (рис. 1.4). Отже, курси з ІБ на цій платформі представляють собою комплексну освітню програму, спрямовану на формування базових навичок безпечної поведінки в цифровому середовищі для широкої аудиторії користувачів. Важливою перевагою платформи «Дія.Освіта» є її повна безкоштовність та доступність для всіх громадян України [12].

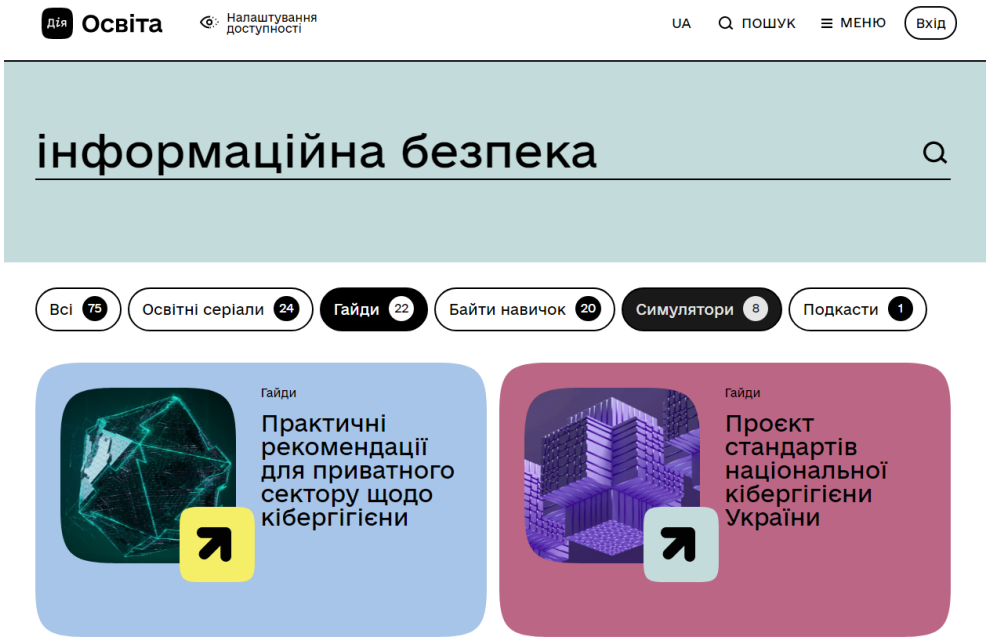


Рис. 1.4 Навчальні матеріали з ІБ на платформі «Дія.Освіта»

Унікальність платформи «Дія.Освіта» полягає в її орієнтації на практичні аспекти повсякденної ІБ, доступні для розуміння користувачам без спеціальної технічної підготовки. Освітні ресурси охоплюють найактуальніші теми: створення надійних паролів та використання менеджерів паролів, налаштування двофакторної автентифікації, безпечне використання публічних Wi-Fi мереж, розпізнавання фішингових атак та соціальної інженерії, захист персональних даних у соціальних мережах, безпечні онлайн-платежі та покупки, резервне копіювання даних та відновлення після інцидентів [12].

Методична структура курсів базується на принципах мікронавчання, що дозволяє засвоювати матеріал невеликими порціями. Кожен модуль містить

короткі відеолекції з анімованими поясненнями, інтерактивні вправи для закріплення матеріалу, реальні кейси та приклади кібератак, практичні чек-листи для самоперевірки безпеки власних пристроїв та акаунтів. Така організація навчального процесу забезпечує високий рівень залученості користувачів та ефективне засвоєння матеріалу [12].

Інтеграція матеріалів з ІБ в освітній процес закладів ФПО може здійснюватися як обов'язковий компонент для здобувачів усіх спеціальностей у рамках формування цифрової компетентності. Викладачі можуть використовувати матеріали «Дія.Освіта» як додаткові ресурси для проведення практичних занять, організації самостійної роботи, підготовки до дискусій з питань ІБ. Платформа надає детальну аналітику прогресу кожного здобувача, що спрощує моніторинг та оцінювання результатів навчання [12].

Мобільні технології революціонізують підходи до навчання ІБ, забезпечуючи безперервний доступ до освітніх ресурсів незалежно від місця та часу. Концепція мобільного навчання базується на використанні портативних цифрових пристроїв – смартфонів, планшетів, електронних книг – як основних інструментів освітнього процесу [9; 39]. Це особливо актуально для формування навичок ІБ, оскільки дозволяє здобувачам вивчати методи захисту інформації безпосередньо на тих пристроях, які вони використовують щоденно.

Інтеграція *мобільних застосунків* з ІБ в освітній процес сприяє підвищенню мотивації здобувачів через гейміфікацію навчання. Багато застосунків використовують ігрові механіки для засвоєння складних концепцій ІБ – від квестів з розшифрування повідомлень до симуляцій кібератак [6; 21]. Така форма подання матеріалу особливо ефективна для здобувачів ФПО, які звикли до інтерактивної взаємодії з цифровим контентом.

Мобільні застосунки забезпечують персоналізацію навчального процесу через адаптивні алгоритми, які аналізують прогрес кожного здобувача та пропонують індивідуальну траєкторію навчання. Системи штучного інтелекту

визначають слабкі місця в знаннях здобувачів та автоматично підбирають додаткові матеріали для їх усунення. Це дозволяє досягти високого рівня засвоєння матеріалу при мінімальних часових витратах [3].

Проаналізувавши наукові праці [4; 14; 23], ми визначили, що мобільні застосунки для формування навичок з ІБ здобувачів ФПО можна класифікувати за кількома категоріями (табл. 1.4).

Таблиця 1.4

Класифікація мобільних застосунків для формування навичок з ІБ

Категорія	**Опис**
Навчальні застосунки	Містять структуровані курси з теоретичним матеріалом, практичними завданнями та тестами. Прикладом є мобільна версія платформи Cybrary, яка надає доступ до сотень курсів з різних аспектів ІБ – від основ мережевої безпеки до етичного хакінгу та форензики.
Застосунки-симулятори	Дозволяють практикувати навички в безпечному віртуальному середовищі. Застосунок Hacker 101 від HackerOne пропонує інтерактивні лабораторні роботи з пошуку вразливостей у веб-застосунках. Здобувачі можуть випробувати різні техніки атак – SQL-ін'єкції, XSS, CSRF – на спеціально підготовлених вразливих застосунках без ризику завдати шкоди реальним системам.
Довідкові застосунки	Слугують мобільними енциклопедіями з ІБ. Застосунок OWASP Mobile Security Testing Guide містить детальні рекомендації щодо тестування безпеки мобільних застосунків, включаючи методології, інструменти та чек-листи. Такі застосунки особливо корисні для швидкого доступу до довідкової інформації під час практичних занять або виконання проектів.
Застосунки для моніторингу та аналізу безпеки	Network Analyzer дозволяє сканувати мережі Wi-Fi, визначати підключені пристрої, аналізувати мережевий трафік. Fing – Network Tools надає можливості для діагностики мережевих проблем, виявлення вразливостей та моніторингу безпеки домашньої або офісної мережі. Використання таких застосунків формує практичні навички роботи з реальними інструментами ІБ.
Криптографічні застосунки	Демонструють принципи шифрування та дешифрування даних. Застосунок Crypto Tools містить реалізації різних алгоритмів шифрування – від класичних шифрів Цезаря та Віженера до сучасних AES та RSA. Здобувачі можуть експериментувати з різними параметрами шифрування, аналізувати стійкість алгоритмів, вивчати принципи криптоаналізу.

У досліджені В. Краснопольського, О. Поліщука та О. Демченка [23] наголошується, що нтеграція мобільних застосунків в освітній процес вимагає розробки методичних рекомендацій щодо їх використання. Ефективною

практикою є створення мобільних квестів з ІБ, де здобувачі виконують серію завдань, використовуючи різні додатки. Наприклад, квест може включати сканування QR-кодів з зашифрованими повідомленнями, їх розшифрування за допомогою криптографічних застосунків, пошук вразливостей у навчальній мережі та розробку рекомендацій щодо їх усунення.

В. Ігнатенко та Ю. Мирошніченко відмічають, що використання технології доповненої реальності відкриває нові можливості для візуалізації концепцій ІБ. Застосунки з доповненою реальністю дозволяють «побачити» потоки даних у мережі, візуалізувати процеси шифрування, демонструвати наслідки кібератак у тривимірному просторі. Це особливо ефективно для пояснення складних абстрактних концепцій, таких як механізми роботи протоколів безпеки або архітектура захищених мереж [17].

Мобільні застосунки забезпечують можливість мікронавчання – засвоєння матеріалу невеликими порціями протягом коротких проміжків часу. Здобувачі можуть використовувати час у транспорті або перерви між заняттями для проходження коротких уроків, виконання тестових завдань або перегляду навчальних відео. Дослідження О. Задоріної, А. Громик та С. Бондар показує, що такий підхід підвищує загальну ефективність навчання на 17-23% порівняно з традиційними методами [14].

Важливим аспектом є використання мобільних застосунків для формування культури безпечної поведінки в цифровому середовищі. Застосунки-антивіруси, менеджери паролів, VPN-клієнти не лише захищають пристрої здобувачів, але й служать практичними прикладами застосування технологій безпеки. Регулярне використання таких застосунків формує звички безпечної роботи з цифровими пристроями та даними (рис. 1.5, 1.6).

Отже, можна стверджувати, що цифрові технології кардинально трансформують підходи до формування навичок з ІБ, створюючи нові можливості для ефективного, доступного та персоналізованого навчання.

Інтеграція відкритих освітніх ресурсів, мобільних застосунків та інноваційних педагогічних методик дозволяє створити комплексне навчальне середовище, яке відповідає вимогам сучасного цифрового суспільства та потребам ринку праці в кваліфікованих фахівцях.

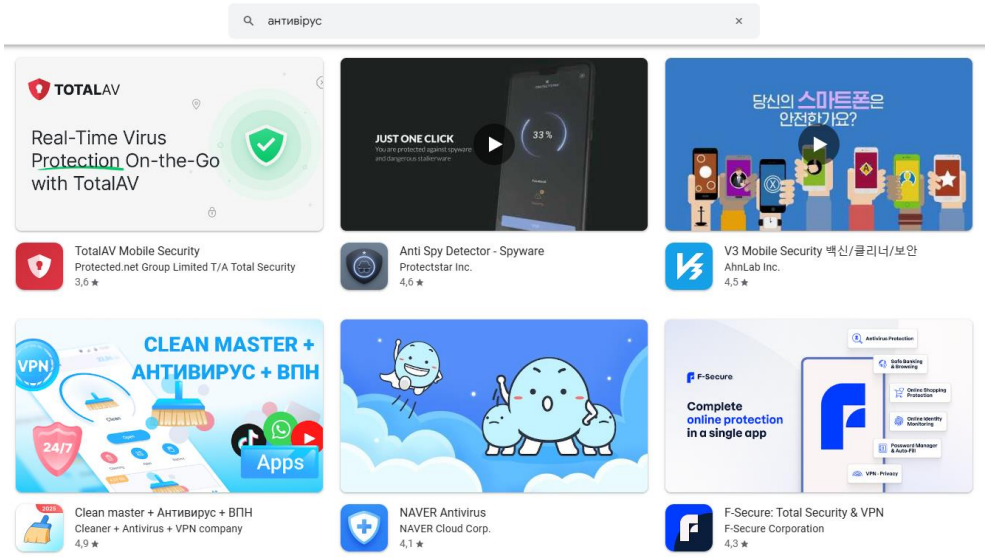


Рис. 1.5 Мобільні застосунки-антивіруси (Google Play)

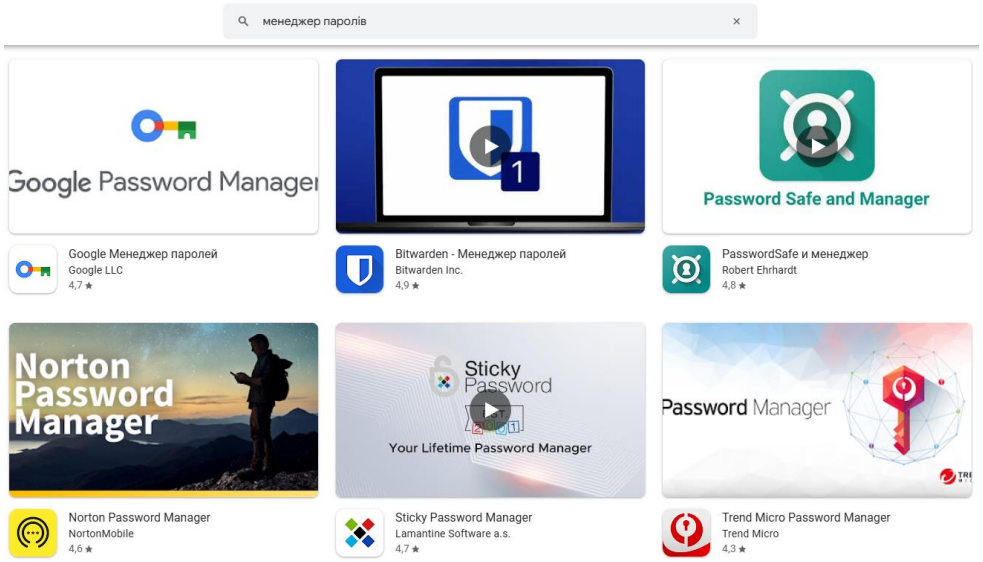


Рис. 1.6 Мобільні застосунки-менеджери паролів (Google Play)

1.3 Організаційно-педагогічні умови використання цифрових технологій для формування навичок з інформаційної безпеки здобувачів фахової передвищої освіти

Організаційно-педагогічні умови є одним із ключових понять сучасної педагогічної науки, що відображає сукупність взаємопов'язаних факторів, обставин та заходів, які забезпечують ефективність освітнього процесу та досягнення визначених педагогічних цілей. Розуміння сутності організаційно-педагогічних умов є принципово важливим для проектування та реалізації будь-яких освітніх інновацій, зокрема у контексті цифровізації навчання.

У педагогічній літературі організаційно-педагогічні умови розглядаються як обставини, від яких залежить ефективність функціонування педагогічної системи. За визначенням В. Лозової та Г. Троцко, «організаційно-педагогічні умови є сукупністю об'єктивних можливостей, змісту, форм, методів, прийомів, спрямованих на вирішення поставлених дослідницьких завдань» [25, с. 212]. Це визначення підкреслює комплексний характер організаційно-педагогічних умов, які охоплюють різні аспекти освітнього процесу.

Науковці А. Рацул та Т. Довга виділяють наступні характеристики організаційно-педагогічних умов [37]:

1) організаційно-педагогічні мають цілеспрямований характер, тобто їх визначення завжди пов'язане з конкретною педагогічною метою чи завданням;

2) організаційно-педагогічні умови характеризуються системністю – вони не існують ізольовано, а перебувають у взаємозв'язку та взаємозалежності;

3) організаційно-педагогічні умови мають керований характер, що означає можливість їх цілеспрямованого створення та модифікації педагогами та управлінцями освіти.

На думку І. Дичківської [11], у структурі організаційно-педагогічних умов

можна виділити три основні компоненти: організаційний, змістовий та педагогічний (рис. 1.7).

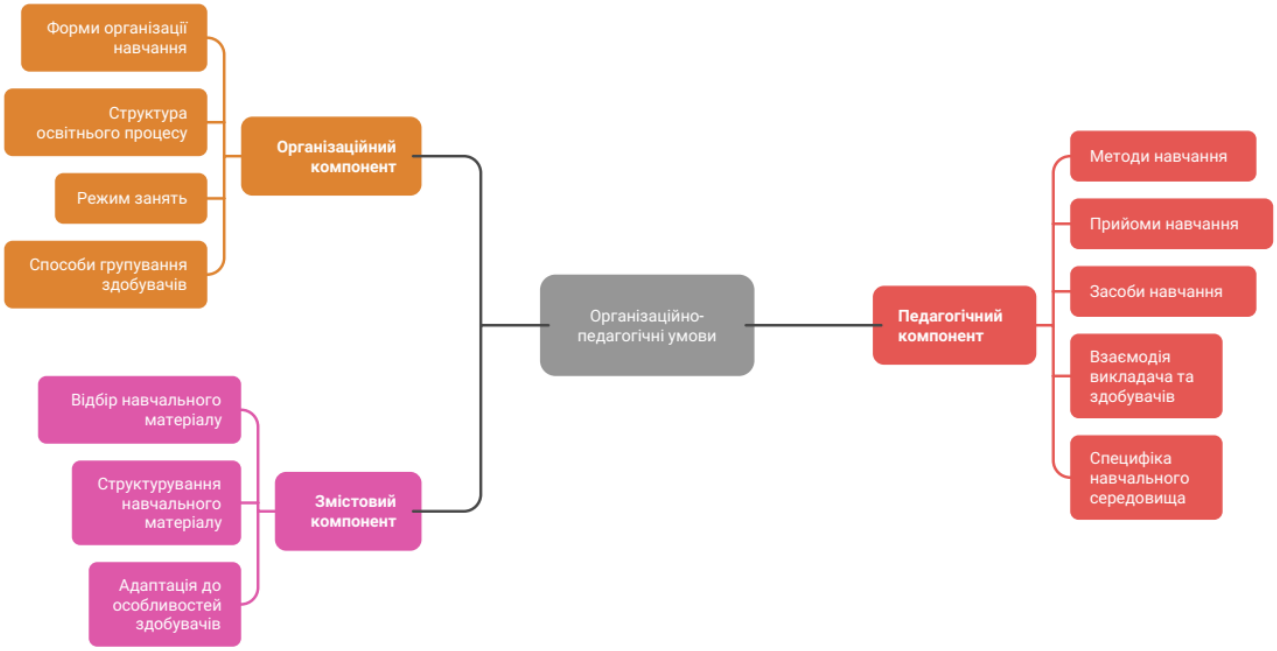


Рис. 1.7 Компоненти структури організаційно-педагогічних умов

Процес визначення організаційно-педагогічних умов у педагогічному дослідженні передбачає кілька етапів [30]:

– аналіз педагогічної проблеми та мети дослідження;

– вивчення теоретичних джерел та узагальнення педагогічного досвіду для виявлення потенційних умов;

– формулювання гіпотетичних організаційно-педагогічних умов, які підлягають експериментальній перевірці;

– уточнення та обґрунтувати ефективності визначених умов у ході педагогічного експерименту.

Важливою характеристикою організаційно-педагогічних умов є їх достатність та необхідність для досягнення поставленої мети. Необхідні умови – це такі, без яких неможливо досягти педагогічної мети. Достатні умови – ті, яких цілком вистачає для досягнення результату. В ідеалі, визначені в

досліджені організаційно-педагогічні умови мають бути одночасно необхідними та достатніми [25].

Дослідники О. Спірін, А. Яцишин, С. Іванова та Л. Лупаренко зазначають, що «у контексті використання цифрових технологій організаційно-педагогічні умови набувають особливого значення, оскільки мають враховувати специфіку цифрового освітнього середовища, особливості взаємодії здобувачів з технологіями, нові можливості для індивідуалізації та персоналізації навчання. Ефективно визначені організаційно-педагогічні умови створюють основу для успішної інтеграції інноваційних технологій у традиційний освітній процес, забезпечуючи баланс між технологічними можливостями та педагогічною доцільністю» [27, с. 136].

У контексті формування навичок з ІБ за допомогою ЦТ організаційно-педагогічні умови набувають особливого значення, оскільки визначають не лише зміст навчання, але й способи його реалізації. Визначимо наступні *організаційно-педагогічні умови ефективного використання цифрових технологій для формування навичок з інформаційної безпеки здобувачів фахової передвищої освіти*:

1) реалізація мобільного навчання як форми організації навчальної діяльності з формування навичок інформаційної безпеки здобувачів фахової передвищої освіти;

2) впровадження технології гейміфікації як інноваційного засобу організації навчальної діяльності з формування навичок інформаційної безпеки здобувачів фахової передвищої освіти.

На нашу думку, ці умови відповідають сучасним тенденціям розвитку освіти, враховують психологічні особливості здобувачів ФПО та створюють можливості для активного, самостійного та мотивованого навчання.

Перша організаційно-педагогічна умова – реалізація мобільного навчання як форми організації навчальної діяльності з формування навичок

інформаційної безпеки здобувачів фахової передвищої освіти.

Мобільне навчання визначається як форма організації освітнього процесу, що здійснюється з використанням мобільних пристроїв та забезпечує доступ до освітніх ресурсів у будь-який час та будь-якому місці [39]. За визначенням ЮНЕСКО, мобільне навчання передбачає використання мобільних технологій окремо або в поєднанні з іншими ІКТ для організації навчання незалежно від місця і часу [60]. Р. Горбатюк та Ю. Тулашвілі визначають мобільне навчання як «процес, що відбувається тоді, коли здобувач не знаходиться в фіксованому, заздалегідь визначеному місці, або коли здобувач користується можливостями навчання, що надаються мобільними технологіями» [8, с. 32]. Н. Рашевська та В. Ткачук розглядають мобільне навчання як «процес пізнання, що відбувається через різні контексти та за допомогою соціальних і змістових взаємодій з використанням персональних цифрових пристроїв» [38, с. 295].

Специфіка ФПО, що орієнтована на практичну підготовку фахівців, зумовлює особливу актуальність впровадження мобільного навчання. Здобувачі ФПО часто поєднують навчання з роботою, мають обмежений час для аудиторних занять, що робить мобільне навчання оптимальним засобом організації освітнього процесу [59]. Крім того, формування навичок з ІБ передбачає розвиток практичних умінь роботи з різними мобільними пристроями та застосунками, що природним чином інтегрується з концепцією мобільного навчання.

Аналіз джерел [9; 39; 52] дає можливість стверджувати, що педагогічний потенціал мобільного навчання для формування навичок з ІБ здобувачів ФПО визначається такими характеристиками:

– мобільні пристрої забезпечують персоналізацію навчання, дозволяючи здобувачам освіти вибирати власний темп, час та місце вивчення матеріалу. Це особливо важливо для формування навичок ІБ, оскільки кожен здобувач має індивідуальний рівень цифрової грамотності та потребує диференційованого

підходу;

– мобільні технології створюють умови для контекстного навчання, коли освітній контент безпосередньо пов’язаний з реальними ситуаціями використання цифрових технологій. Здобувачі можуть негайно застосовувати отримані знання про ІБ в реальних умовах роботи з мобільними застосунками, соціальними мережами, електронною поштою.

Методичні аспекти мобільного навчання ІБ передбачають використання різноманітних форм організації навчальної діяльності. Ефективним є мікронавчання, коли освітній контент розбивається на невеликі модулі тривалістю декілька хвилин, що можуть бути опрацьовані здобувачами в будь-який вільний час [24].

Важливою складовою мобільного навчання є використання системи сповіщень та нагадувань, що дозволяє підтримувати постійну увагу здобувачів до питань ІБ [17]. Регулярні повідомлення про нові загрози, поради щодо безпечної поведінки в мережі, нагадування про необхідність оновлення паролів формують у здобувачів стійку звичку дотримуватися правил ІБ. Водночас, викладач має дбати про те, щоб кількість сповіщень була оптимальною і не викликала відчуття перевантаження.

На думку А. Грушевої та Л. Філіппової, колаборативні можливості мобільних технологій створюють умови для організації спільної навчальної діяльності здобувачів. Використання мобільних месенджерів, спеціалізованих платформ для групової роботи дозволяє організовувати дискусії з питань ІБ, обмін досвідом, взаємне навчання. Здобувачі можуть створювати спільні проєкти, аналізувати конкретні ситуації порушення ІБ, розробляти рекомендації. Така взаємодія сприяє не лише формуванню знань і навичок, але й розвитку критичного мислення, здатності до рефлексії власної поведінки в цифровому середовищі [9].

Як зазначають С. Семеріков, М. Стрюк та Н. Моісеєнко, важливим

аспектом організації мобільного навчання є забезпечення доступності освітніх ресурсів для всіх здобувачів. Не всі здобувачі мають сучасні мобільні пристрої з високою продуктивністю, тому при розробці мобільних застосунків та адаптації веб-ресурсів необхідно враховувати різні технічні можливості. Освітній контент має бути оптимізованим для роботи на пристроях з різними розмірами екранів, операційними системами, швидкістю Інтернет-з'єднання. Альтернативним підходом може бути організація мобільних класів у навчальному закладі, де здобувачі можуть скористатися планшетами чи смартфонами для виконання навчальних завдань [39].

Оцінювання результатів навчання в умовах мобільного навчання має свої особливості [38]. Мобільні технології дозволяють організовувати різні форми контролю: тестування, виконання практичних завдань, створення портфоліо, взаємооцінювання. Особливо ефективними для формування навичок з ІБ є ситуаційні завдання, коли здобувачі мають проаналізувати конкретну ситуацію (наприклад, отримання підозрілого електронного листа) та прийняти рішення щодо подальших дій. Результати виконання таких завдань можуть автоматично фіксуватися в системі управління навчанням, що дозволяє викладачу відстежувати прогрес кожного здобувача та вчасно надавати зворотний зв'язок.

Реалізація мобільного навчання вимагає також врахування етичних та правових аспектів. Використання мобільних технологій пов'язане зі збором та обробкою персональних даних здобувачів, тому навчальний заклад має забезпечити дотримання вимог законодавства про захист персональних даних. Здобувачі мають бути поінформовані про те, які дані збираються, як вони використовуються, які заходи вживаються для їх захисту [34].

Друга організаційно-педагогічна умова – впровадження технології гейміфікації як інноваційного засобу організації навчальної діяльності з формування навичок інформаційної безпеки здобувачів фахової передвищої освіти.

Гейміфікація визначається як використання ігрових елементів та механік у неігрових контекстах для підвищення залученості, мотивації та ефективності діяльності [6]. У освітньому процесі гейміфікація передбачає застосування ігрових принципів та механізмів для організації навчальної діяльності з метою підвищення мотивації здобувачів, активізації їх пізнавальної діяльності, створення емоційно позитивної атмосфери навчання [21].

Специфіка формування навичок з ІБ особливо сприятлива для використання гейміфікації [22; 35]: 1) тематика ІБ сама по собі має елементи змагання, протиборства (користувач проти кіберзлочинців), що легко трансформується в ігрову механіку; 2) практичні навички з ІБ краще формуються через активну діяльність, моделювання ситуацій, що природно реалізується в ігровій формі; 3) гейміфікація дозволяє створити безпечне середовище для навчання, де здобувачі можуть робити помилки, експериментувати, не боячись реальних негативних наслідків.

Різні види ігор є потужним інструментом формування практичних навичок з ІБ. Так, симуляції та рольові ігри дозволяють моделювати різні сценарії кіберінцидентів: фішингову атаку, зараження вірусом, витік конфіденційних даних, DDoS-атаку, соціальну інженерію. Здобувачі мають діяти в реальному часі, приймати рішення в умовах обмеженої інформації та часового тиску. Після завершення симуляції проводиться детальний розбір дій здобувачів, аналіз помилок, обговорення альтернативних стратегій [33].

Натомість командні ігри та змагання розвивають навички співпраці та комунікації [45]. Можуть організовуватися командні квести, де кожен учасник відповідає за певний аспект ІБ, і успіх залежить від ефективної координації дій команди. Змагання, де команди змагаються в розв’язанні завдань з кібербезпеки, є популярною формою гейміфікованого навчання у сфері ІКТ. Адаптовані версії таких змагань можуть використовуватися в закладах ФПО.

С. Переяславська та О. Смагіна вважають негайний зворотний зв’язок

критично важливим елементом гейміфікації [31]. На відміну від традиційного навчання, де здобувачі отримують оцінки після виконання завдання, гейміфіковане середовище надає миттєву інформацію про правильність дій, нараховує бали, змінює статус здобувача. Такий зворотний зв’язок дозволяє здобувачам швидко коригувати свої дії, учитися на помилках, бачити прямий зв’язок між зусиллями та результатом.

На думку С. Толочко, адаптивність ігрового середовища забезпечує індивідуалізацію навчання. Система може автоматично підбирати завдання відповідно до рівня підготовки здобувача: пропонувати простіші завдання тим, хто має труднощі, та більш складні виклики для просунутих користувачів. Така адаптивність підтримує мотивацію здобувачів на оптимальному рівні, запобігаючи як нудьзі від занадто простих завдань, так і фрустрації від непосильних викликів [45].

Дослідниця Я. Карлінська у статті [21] зазначає, що соціальні механіки в гейміфікованому навчанні включають можливості взаємодії здобувачів між собою. Створення спільнот, форуми для обговорення стратегій, можливість ділитися досягненнями, допомагати іншим користувачам формують соціальний контекст навчання. Взаємне навчання, коли більш досвідчені здобувачі виступають менторами для новачків, підсилює засвоєння матеріалу у обох сторін. Соціальне визнання досягнень, можливість похвалитися отриманими значками у соціальних мережах створюють додаткову мотивацію.

Естетика та дизайн гейміфікованого навчального середовища мають значний вплив на залученість здобувачів [21]. Візуально привабливий інтерфейс, якісна графіка, продумана кольорова схема, анімації та звукові ефекти створюють приємний користувацький досвід. Водночас, дизайн має бути функціональним, не відволікати від навчальних цілей. Стилістика може відображати тематику кібербезпеки: використання образів хакерів та захисників, візуалізація мережевих з’єднань, цифрових даних, що створює

відповідну атмосферу.

Балансування складності є критичним аспектом проектування гейміфікованого навчання. Завдання мають бути достатньо складними, щоб викликати інтерес, але досяжними при зусиллях. Поступове збільшення складності, можливість вибору рівня складності, надання допомоги при необхідності забезпечують оптимальний рівень виклику [22]. У контексті ІБ це може означати перехід від простих завдань (створення надійного пароля) до складних сценаріїв (комплексний захист інформаційної системи від множинних загроз).

Інтеграція гейміфікації в навчальний план вимагає ретельного планування. Гейміфіковані елементи мають бути узгоджені з навчальними цілями, програмними результатами навчання, критеріями оцінювання. Важливо, щоб гра не ставала самоціллю, а служила засобом досягнення освітніх результатів. Викладач має чітко визначити, які саме навички з ІБ формуються через кожен ігровий елемент, як оцінюється їх сформованість.

Автори дослідження [6] вважають, що технічна реалізація гейміфікованого навчання може здійснюватися різними способами. Найпростіший варіант – використання готових платформ для гейміфікації навчання, які дозволяють швидко створити гейміфіковані завдання без програмування. Більш складний підхід – розробка спеціалізованого програмного забезпечення для навчання ІБ, що вимагає залучення програмістів та дизайнерів. Проміжним варіантом є використання конструкторів освітніх ігор, які надають шаблони та інструменти для створення власних навчальних ігор.

Однак, на думку Д. Касьянова, потенційні ризики та обмеження гейміфікації мають враховуватися при її впровадженні. Надмірне фокусування на балах та рейтингах може призвести до того, що здобувачі будуть орієнтуватися на формальні показники, а не на реальне засвоєння знань.

Змагальний момент може викликати стрес у деяких здобувачів, особливо у тих, хто не має схильності до конкуренції. Гейміфікація може бути менш ефективною для дорослих здобувачів або для тих, хто не цікавиться іграми. Тому важливо надавати альтернативні шляхи навчання для тих, кому гейміфікований підхід не підходить [22].

Отже, сформульовані організаційно-педагогічні умови є ізольованими, а перебувають у тісному взаємозв'язку та взаємодоповненні. Мобільне навчання забезпечує гнучкість, доступність та контекстуальність освітнього процесу, відповідаючи специфіці підготовки фахівців-практиків. Гейміфікація підвищує мотивацію, залученість та активність здобувачів, створює емоційно позитивну атмосферу навчання. Комплексна реалізація цих умов дозволяє досягти високої ефективності формування навичок з ІБ у здобувачів ФПО, що є критично важливим в умовах цифровізації всіх сфер життя суспільства.

Висновки до першого розділу

У першому розділі магістерської роботи проведено комплексний аналіз теоретичних основ використання ЦТ для формування навичок ІБ здобувачів ФПО. На основі вивчення науково-педагогічних джерел, нормативно-правових документів та узагальнення досвіду впровадження ЦТ в освітній процес отримано наступні результати.

1. Аналіз стану дослідження проблеми формування навичок ІБ показав, що в умовах інтенсивної цифровізації освіти та воєнного стану в Україні питання ІБ набувають критичного значення. Визначено, що ІБ доцільно розглядати як стан захищеності освітнього середовища, що забезпечує конфіденційність, цілісність і доступність інформації та персональних даних усіх учасників освітнього процесу, запобігає інформаційним загрозам і несанкціонованому доступу, а також передбачає формування у здобувачів ФПО відповідних навичок. Уточнено визначення навичок ІБ як сукупності знань та умінь для безпечного, відповідального та етичного використання ЦТ, що забезпечує особі захист особистих даних, цифрової ідентичності, пристроїв і мереж від кібератак, а також сприяє свідомому онлайн-спілкуванню.

2. Обґрунтовано доцільність використання ЦТ як засобу формування навичок з ІБ. Проаналізовано різні типи відкритих навчальних ресурсів та визначено критерії їх відбору. Розкрито потенціал мобільних застосунків для формування навичок ІБ та подано їх класифікацію.

3. Визначено та теоретично обґрунтовано організаційно-педагогічні умови ефективного використання ЦТ для формування навичок з ІБ здобувачів ФПО: реалізація мобільного навчання як форми організації навчальної діяльності з формування навичок інформаційної безпеки здобувачів фахової передвищої освіти; впровадження технології гейміфікації як інноваційного засобу

організації навчальної діяльності з формування навичок інформаційної безпеки здобувачів фахової передвищої освіти.

4. Розкрито педагогічний потенціал мобільного навчання та гейміфікації для формування навичок ІБ здобувачів ФПО. Встановлено, що ефективна інтеграція ЦТ у процес формування навичок ІБ вимагає системного підходу, який охоплює організаційні, методичні, технологічні та змістові аспекти.

РОЗДІЛ 2

МЕТОДИЧНІ ОСНОВИ ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ ДЛЯ ФОРМУВАННЯ НАВИЧОК З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗДОБУВАЧІВ ФАХОВОЇ ПЕРЕДВИЩОЇ ОСВІТИ

РОЗДІЛ 2
МЕТОДИЧНІ ОСНОВИ ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ ДЛЯ ФОРМУВАННЯ НАВИЧОК З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗДОБУВАЧІВ ФАХОВОЇ ПЕРЕДВИЩОЇ ОСВІТИ

2.1 Модель використання цифрових технологій для формування навичок з інформаційної безпеки здобувачів фахової передвищої освіти

Методика, згідно з визначенням А. Рацул та Т. Довгої, це «сукупність методів, прийомів доцільного проведення певної роботи, що ґрунтується на науково обґрунтованих закономірностях, нормах і правилах» [34, с. 156]. У контексті нашого дослідження методика використання ЦТ для формування навичок ІБ здобувачів ФПО становить систему науково обґрунтованих методів, форм і засобів організації навчальної діяльності, спрямованої на розвиток навичок безпечної поведінки в цифровому середовищі.

У процесі розроблення методики важливим етапом є її моделювання, оскільки воно забезпечує наукове обґрунтування структури, змісту та логіки взаємозв’язків між компонентами методичної системи [30]. Моделювання дозволяє не лише відобразити основні елементи методики у формалізованому вигляді, а й виявити причинно-наслідкові зв’язки між застосуванням цифрових технологій та формуванням навичок ІБ здобувачів освіти, що створює підґрунтя для її подальшої експериментальної перевірки та вдосконалення.

Моделювання є одним із ключових методів наукового пізнання в педагогіці. За визначенням Р. Мартинової, моделювання – це «науковий метод пізнання явищ та процесів за допомогою відтворення їх характеристик на інших об’єктах – спеціально створених з цією метою моделях» [26, с. 62]. При цьому

модель розглядається як «абстрактне подання теорії, її операціоналізація, яку можна передати емпіричним шляхом» [26, с. 63].

Дослідниці В. Лозова та Г. Троцко тлумачать моделювання як «метод дослідження (чи навчання), який передбачає створення штучних чи природних систем (моделей), котрі імітують суттєві властивості оригіналу» [25, с. 46]. Основний зміст моделювання полягає в тому, щоб за результатами дослідів з моделями можна було отримати відповідь про характер ефектів, які пов'язані з досліджуваним об’єктом.

Педагогічна модель, згідно з концепцією Р. Мартинової, являє собою цілісне відображення реального об’єкта в ідеальній формі, виконане засобами наукових понять. Така модель «уможливлює виокремлення актуальних і перспективних завдань навчально-виховного процесу, наукове обґрунтування умов зближення між імовірними, очікуваними та бажаними змінами об’єкта» [26, с. 63]. Педагогічні моделі спрощують оригінал, узагальнюють його, сприяючи впорядкуванню та систематизації інформації про педагогічний об’єкт.

Важливою характеристикою педагогічного моделювання є його системність. Дослідники зазначають, що невід’ємною властивістю наукових моделей є системність, при якій система розглядається як «сукупність визначених елементів, між якими існує закономірний зв’язок чи взаємодія» [26, с. 65]. Успішність моделювання значною мірою залежить від наявності теорії, що описує явище, яке підлягає моделюванню, а також від міри формалізації положень цієї теорії.

У ході дослідження нами розроблено модель використання цифрових технологій для формування навичок з інформаційної безпеки здобувачів фахової передвищої освіти (рис. 2.1), яка складається з таких блоків: 1) цільового; 2) теоретико-методологічного; 3) змістового; 4) організаційно-методичного; 5) діагностико-результативного.

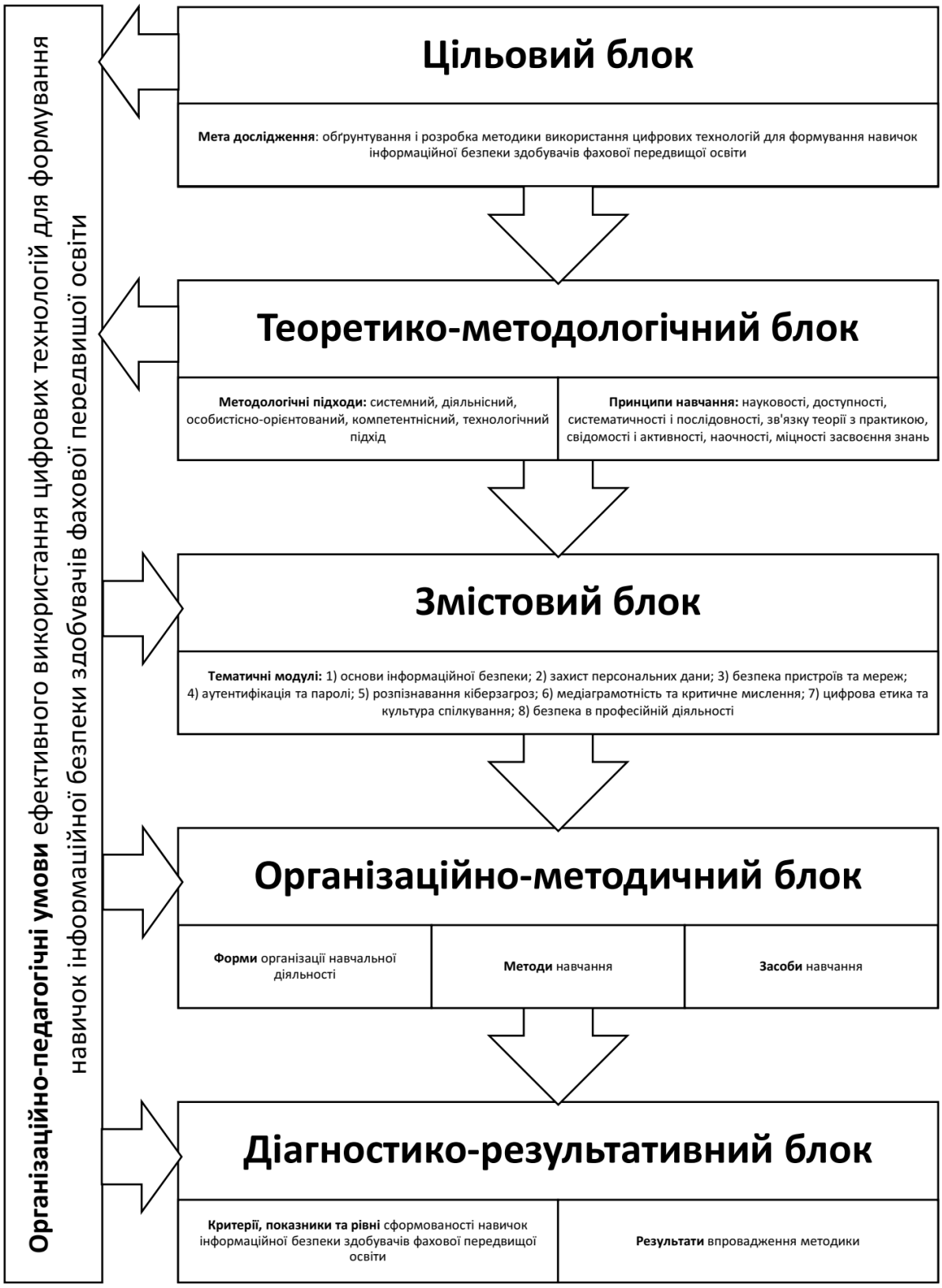


Рис. 2.1 Модель використання цифрових технологій для формування навичок з інформаційної безпеки здобувачів фахової передвищої освіти

Цільовий блок містить мету нашого дослідження: обґрунтування і розробка методики використання цифрових технологій для формування навичок ІБ здобувачів ФПО. Мета конкретизується через систему завдань, спрямованих на формування у здобувачів навичок безпечно, відповідально та етично використовувати ЦТ, захищати особисті дані, цифрову ідентичність, пристрої і мережі від кібератак, а також здійснювати свідоме онлайн-спілкування.

Теоретико-методологічний блок моделі включає методологічні підходи й принципи, які взято за основу під час обґрунтування й розробки методики використання ЦТ для формування навичок ІБ здобувачів ФПО.

Методологічні підходи, узагальнені на основі аналізу праць В. Бондаря [2], І. Дичківської [11], В. Дубинського [13], В. Лозової, Г. Троцко [25], А. Рацул, Т. Довгої [37], представлені у табл. 2.1.

Таблиця 2.1

Методологічні підходи до формування навичок ІБ здобувачів ФПО

Системний підхід	Розгляд процесу формування навичок ІБ як цілісної системи взаємопов'язаних компонентів (цілей, змісту, методів, форм, засобів навчання), що забезпечує комплексний вплив на розвиток особистості здобувача.
Діяльнісний підхід	Орієнтація на активну навчально-пізнавальну діяльність здобувачів, організацію практичної роботи з цифровими технологіями, формування навичок через виконання конкретних завдань з ІБ.
Особистісно-орієнтований підхід	Урахування індивідуальних особливостей, потреб та інтересів здобувачів, створення умов для розвитку їхньої особистості, забезпечення права вибору індивідуальної освітньої траєкторії.
Компетентнісний підхід	Спрямованість освітнього процесу на формування ключових компетентностей, зокрема інформаційно-цифрової компетентності та компетентності з ІБ, здатності застосовувати знання і навички в реальних життєвих ситуаціях.
Технологічний підхід	Використання сучасних освітніх технологій, зокрема мобільного навчання та гейміфікації, для підвищення ефективності навчального процесу та досягнення запланованих результатів навчання.

Принципи навчання, структуровані згідно до підручників В. Бондаря [2], М. Вовк, Ю. Грищенко, С. Соломахи, Н. Філіпчук та С. Ходаківської [30], які покладено в основу методики, подано у табл. 2.2.

Таблиця 2.2

Принципи навчання, які покладено в основу розробленої методики

Принцип науковості	Забезпечення відповідності змісту навчання сучасному рівню розвитку науки про інформаційну безпеку, використання достовірної та актуальної інформації про кіберзагрози та методи захисту.
Принцип доступності	Врахування вікових та індивідуальних особливостей здобувачів, відповідність змісту та методів навчання їхнім можливостям, поступове ускладнення навчального матеріалу.
Принцип систематичності і послідовності	Логічна побудова змісту навчання, послідовне формування навичок від простих до складних, забезпечення міцних зв’язків між окремими темами та розділами.
Принцип зв'язку теорії з практикою	Спрямованість навчання на формування практичних навичок безпечної роботи з цифровими технологіями, застосування теоретичних знань у реальних ситуаціях.
Принцип свідомості і активності	Формування усвідомленого ставлення здобувачів до питань інформаційної безпеки, стимулювання їхньої активної участі в навчальному процесі, розвиток самостійності та ініціативності.
Принцип наочності	Використання різноманітних засобів візуалізації, мультимедійних матеріалів, інтерактивних симуляцій для кращого розуміння концепцій інформаційної безпеки.
Принцип міцності засвоєння знань	Забезпечення глибокого та тривалого засвоєння знань і навичок через повторення, закріплення, систематичне використання цифрових технологій у навчальній та повсякденній діяльності.

Змістовий блок моделі містить рекомендації для викладачів закладів ФПО щодо результативного використання ЦТ для формування навичок ІБ здобувачів. Змістовий блок включає тематичні модулі, зміст яких визначено відповідно до сучасних досліджень О. Мозгаллі, Я. Рибалко, Р. Синицького [28] та І. Чичкань, С. Спасітєлєвої, Ю. Жданової [47] (табл. 2.3).

Таблиця 2.3

Тематичні модулі

№ з/п	**Назва модуля**	**Зміст модуля**
1	Основи інформаційної безпеки	Визначення поняття інформаційної безпеки, модель CIA (конфіденційність, цілісність, доступність), види інформаційних загроз, правові аспекти інформаційної безпеки в Україні.
2	Захист персональних даних	Поняття персональних даних, принципи обробки персональних даних, налаштування параметрів конфіденційності в соціальних мережах, захист персональної

№ з/п	Назва модуля	Зміст модуля
		інформації онлайн.
3	Безпека пристроїв та мереж	Захист мобільних пристроїв, комп'ютерів, використання антивірусного програмного забезпечення, безпечне підключення до WiFi-мереж, налаштування мережевих параметрів безпеки.
4	Аутентифікація та паролі	Створення надійних паролів, використання менеджерів паролів, двофакторна автентифікація, біометричні методи захисту.
5	Розпізнавання кіберзагроз	Фішинг та соціальна інженерія, шкідливе програмне забезпечення, онлайн-шахрайство, способи розпізнавання та захисту від кіберзагроз.
6	Медіаграмотність та критичне мислення	Перевірка достовірності інформації, розпізнавання дезінформації та маніпуляцій, критичне ставлення до контенту в соціальних мережах.
7	Цифрова етика та культура спілкування	Норми поведінки в онлайн-середовищі, протидія кібербулінгу, відповідальне використання цифрових технологій.
8	Безпека в професійній діяльності	Захист корпоративної інформації, безпечна робота з хмарними сервісами, використання VPN, резервне копіювання даних.

Організаційно-методичний блок моделі використання ЦТ для формування навичок ІБ здобувачів ФПО передбачає реалізацію визначених нами організаційно-педагогічних умов.

Перша умова (реалізація мобільного навчання як форми організації навчальної діяльності з формування навичок ІБ здобувачів ФПО) передбачає:

– використання мобільних застосунків для навчання ІБ (навчальні платформи, симулятори, практичні інструменти);

– організацію мікронавчання – подання навчального матеріалу короткими модулями тривалістю 3-7 хвилин;

– використання push-повідомлень та нагадувань для підтримання уваги до питань безпеки;

– забезпечення доступу до навчальних ресурсів у будь-який час та будь-якому місці;

– організацію практичних завдань, що виконуються на мобільних пристроях здобувачів;

– проведення мобільних квестів з ІБ.

Друга умова (впровадження технології гейміфікації як інноваційного засобу організації навчальної діяльності з формування навичок ІБ здобувачів ФПО) передбачає:

– використання системи балів та рівнів для оцінювання прогресу здобувачів;

– створення значків та досягнень за виконання завдань з ІБ;

– організацію рейтингів та таблиць лідерів для підтримання мотивації;

– розробку завдань та квестів, що моделюють реальні ситуації кіберзагроз;

– проведення симуляцій кібератак у безпечному навчальному середовищі;

– організацію командних змагань з інформаційної безпеки;

– забезпечення негайного зворотного зв’язку про правильність дій здобувачів.

Форми організації навчальної діяльності включають:

– лекції з використанням мультимедійних презентацій та відеоматеріалів;

– практичні заняття у комп’ютерних класах та з використанням мобільних пристроїв;

– лабораторні роботи з налаштування параметрів безпеки;

– семінарські заняття з обговорення кейсів порушення ІБ;

– самостійну роботу з використанням онлайн-курсів та мобільних застосунків;

– проєктну діяльність з розробки рекомендацій щодо ІБ;

– дистанційне навчання через освітні платформи.

Методи навчання охоплюють:

– словесні методи (пояснення, бесіда, дискусія);

– наочні методи (демонстрація, ілюстрація, відеоматеріали);

– практичні методи (вправи, лабораторні роботи, проєкти);

– інтерактивні методи (рольові ігри, симуляції, кейс-стаді);

– проблемні методи (проблемні ситуації, дослідницькі завдання);

– ігрові методи (навчальні ігри, змагання, квести).

Засоби навчання включають:

– комп’ютери та мобільні пристрої;

– програмне забезпечення для навчання ІБ;

– онлайн-платформи та масові відкриті онлайн-курси;

– мобільні застосунки для формування навичок безпеки;

– навчальні відео та мультимедійні матеріали;

– тестові системи та системи управління навчанням.

Діагностико-результативний блок включає критерії, показники та рівні сформованості навичок інформаційної безпеки здобувачів фахової передвищої освіти, що дають змогу досягнути мети дослідження та оцінити ефективність розробленої методики. Детальний опис критеріїв, показників та рівнів представлено у підрозділі 3.1.

Очікувані результати впровадження методики:

– підвищення рівня знань здобувачів про ІБ;

– формування практичних навичок з ІБ;

– розвиток критичного мислення та інформаційної грамотності;

– усвідомлення важливості захисту персональних даних;

– формування звичок безпечної поведінки в онлайн-середовищі;

– підготовка до професійної діяльності в умовах цифрового суспільства.

Розроблена модель є основою методики використання ЦТ для формування навичок ІБ здобувачів ФПО.

2.2 Елементи методики використання цифрових технологій для формування навичок з інформаційної безпеки здобувачів фахової передвищої освіти

Задля впровадження методики використання ЦТ для формування навичок з ІБ здобувачів ФПО нами розроблено план-конспект заняття з інформатики. Заняття побудовано відповідно до структури та принципів розробленої моделі.

У процесі проведення заняття реалізуються визначені організаційно-педагогічні умови:

1) реалізація мобільного навчання як форми організації навчальної діяльності з формування навичок ІБ здобувачів ФПО – використання мобільних застосунків, мікронавчання, push-повідомлень, мобільного квесту;

2) впровадження технології гейміфікації як інноваційного засобу організації навчальної діяльності з формування навичок ІБ здобувачів ФПО – система балів та рівнів, значки та досягнення, рейтинги, симуляції кіберзагроз, командні змагання.

Заняття ґрунтується на методологічних підходах, визначених у розробленій методиці: системному, діяльнісному, особистісно-орієнтованому, компетентнісному та технологічному. Реалізуються принципи навчання: науковості, доступності, систематичності і послідовності, зв’язку теорії з практикою, свідомості і активності, наочності, міцності засвоєння знань.

Змістовий компонент заняття відповідає тематичному модулю «Захист персональних даних» із розробленої системи модулів і включає: поняття персональних даних, принципи їх обробки, налаштування параметрів конфіденційності в соціальних мережах, захист персональної інформації онлайн.

Використовуються рекомендовані засоби навчання: мобільні пристрої,

програмне забезпечення для навчання ІБ, онлайн-платформа «Дія. Освіта», мобільні застосунки для формування навичок безпеки, навчальні відео та мультимедійні матеріали, тестові системи.

Таким чином, даний план-конспект є практичною апробацією теоретично обґрунтованої методики та демонструє конкретні механізми її впровадження у навчальний процес закладів ФПО.

План-конспект заняття з теми

«Захист персональних даних у цифровому середовищі»

Мета заняття:

навчальна: ознайомлення здобувачів з поняттям персональних даних та принципами їх обробки, навчанні налаштовувати параметри конфіденційності у соціальних мережах та формуванні практичних навичок захисту особистої інформації онлайн;

розвивальна: розвиток критичного мислення щодо поширення особистої інформації та формування медіаграмотності і цифрової культури;

виховна: виховання відповідального ставлення до власних персональних даних та формування свідомої поведінки у цифровому середовищі.

Тип заняття: комбіноване

Методологічне забезпечення

Підходи: діяльнісний (практична робота на мобільних пристроях), особистісно-орієнтований (індивідуальні темпи виконання завдань), технологічний (мобільне навчання, гейміфікація).

Принципи: зв’язку теорії з практикою, свідомості і активності, доступності.

Методи: словесні (лекція, пояснення), інтерактивні (квест), практичні (вправи на мобільних пристроях), ігрові (змагання, система балів).

Засоби: мобільні пристрої здобувачів (смартфони/планшети), платформа «Дія. Освіта», мобільний застосунок Bitwarden, Google Форми для тестування,

мультимедійна презентація.

План заняття

1. Організаційний момент (3 хв.)

Викладач вітає здобувачів, перевіряє присутність, оголошує тему, мету та формат заняття. Особлива увага приділяється поясненню правил гейміфікації: на занятті діє система балів від 0 до 100, передбачені три рівні досягнень та ведеться таблиця лідерів у режиму реального часу.

Здобувачі готують мобільні пристрої до роботи та сканують QR-код для входу в систему оцінювання. Реєстрація в онлайн-таблиці лідерів (Google Таблиця) дає кожному учаснику стартові 10 балів за участь у занятті, що одразу активізує ігрову механіку та мотивує до активної роботи.

2. Мотивація та актуалізація (7 хв.)

Мікромодуль 1. Що таке персональні дані?

Викладач демонструє короткий двохвилинний відеоролик з платформи «Дія.Освіта» про реальний випадок витоку персональних даних, який яскраво ілюструє актуальність теми. Після перегляду ставиться провокаційне запитання до аудиторії: «Якими персональними даними ви ділилися сьогодні онлайн?».

Здобувачі переглядають відео на власних пристроях, що є першим практичним елементом мобільного навчання, після чого беруть участь у бліц-опитуванні через Google Форму. У якості практичного завдання-розминки пропонується відкрити власний профіль у будь-якій соціальній мережі та підрахувати, скільки персональних даних є у відкритому доступі. Цей простий, але ефективний прийом дозволяє здобувачам особисто усвідомити масштаб проблеми. За участь у опитуванні нараховується 5 балів, а ті, хто знайшов понад 10 елементів персональних даних у своєму профілі, отримують додатково 10 балів, що стимулює ретельність виконання завдання.

3. Міні-лекція з інформаційної безпеки (15 хв.)

Теоретична частина заняття побудована у форматі інтерактивної лекції з

використанням мультимедійної презентації (див. додаток А) та мобільних технологій. Викладач викладає матеріал за допомогою презентації (рис. 2.2), демонструє приклади на власному мобільному пристрої з дублюванням екрану, робить паузи для запитань після кожного логічного блоку та надсилає push-повідомлення з ключовими тезами на пристрої здобувачів.

Рис. 2.2 Презентація «Інформаційна безпека»

Здобувачі слухають лекцію, переглядають презентацію та конспектують основні положення у цифровому форматі, використовуючи Google Keep або інші застосунки на власний вибір.

Зміст лекції

Персональні дані: поняття та класифікація (4 хв.)

Лекція розпочинається з чіткого визначення поняття персональних даних та їх класифікації. Викладач пояснює, що персональні дані включають базові ідентифікаційні дані (ПІБ, дату народження, адресу), контактні дані (телефон, email), біометричні дані (фото, відбитки пальців), цифровий слід (IP-адресу, геолокацію, cookies) та фінансові дані. Особлива увага приділяється поняттю чутливих або особливих персональних даних, розголошення яких може призвести до дискримінації чи інших серйозних наслідків.

Загрози та ризики (4 хв.)

Викладач детально розглядає такі наслідки витоку персональних даних, як крадіжка ідентичності, фінансові втрати, репутаційні ризики, кібербулінг та шантаж. Наводиться актуальна статистика витоків даних в Україні та світі, що робить загрози більш відчутними та реальними.

Принципи та методи захисту (4 хв.)

Викладач розкриває законодавче регулювання захисту персональних даних, зокрема положення Закону України «Про захист персональних даних». Детально пояснюються принципи обробки персональних даних: мінімізація даних (збір лише необхідної інформації), прозорість обробки (чітке інформування про мету збору), обмеження мети (використання даних лише за призначенням), контроль з боку користувача (можливість перегляду та виправлення даних) та право на видалення або право на забуття.

Викладач демонструє основні методи захисту персональних даних, включаючи налаштування конфіденційності в різних сервісах, створення сильних паролів та використання двофакторної автентифікації, шифрування даних, обмеження доступу до дозволів мобільних застосунків та регулярний аудит власного цифрового сліду. Кожен метод ілюструється практичним прикладом на екрані.

Безпечна поведінка в цифровому середовищі (3 хв.)

Обговорюються правила безпечного спілкування в соціальних мережах, детально розглядається питання про те, що не варто публікувати онлайн (адресу проживання, номери документів, розпорядок дня, інформацію про подорожі в режимі реального часу). Викладач наголошує на важливості регулярної перевірки налаштувань конфіденційності, усвідомленого надання згоди на обробку даних та дотримання базових порад щодо захисту особистої інформації.

Після кожного блоку організовуються експрес-опитування, що дозволяє

одразу перевірити розуміння матеріалу.

За активне конспектування здобувачі отримують 5 балів (підтверджується скриншотом конспекту), за найкраще запитання до лекції (визначається голосуванням або викладачем) нараховується 10 балів, а за участь у проміжних опитуваннях додається ще 5 балів.

4. Закріплення теоретичного матеріалу (10 хв.)

Мікромодуль 2. Перевірка розуміння

Після завершення лекції викладач організовує міні-тест за допомогою Google Форми та здійснює моніторинг результатів у режимі реального часу. Здобувачі проходять тест з 10 питань на власних пристроях, що дозволяє їм відразу побачити свої помилки та проаналізувати їх. Проходження тесту з результатом 80% і вище оцінюється в 15 балів, що стимулює уважне вивчення теоретичного матеріалу.

Мікромодуль 3. Кейс-обговорення

Для глибшого осмислення матеріалу викладач надсилає на мобільні пристрої здобувачів опис трьох реальних ситуацій порушення інформаційної безпеки та організовує групове обговорення. Здобувачі протягом двох хвилин читають кейси, після чого поділяються на міні-групи по 3-4 особи для обговорення ключового питання: «Як можна було уникнути цієї ситуації?». Кожна група отримує 10 балів за презентацію своїх висновків (1 хвилина на групу), а додатковий бонус у 5 балів нараховується за найкреативнішу відповідь, яка визначається голосуванням.

5. Практична робота (30 хв.)

Мобільний квест «Захисти свої персональні дані»

Центральною частиною заняття є мобільний квест, під час якого здобувачі індивідуально проходять 5 практичних станцій на власних мобільних пристроях. Кожна станція моделює реальну ситуацію, де потрібно застосувати отримані знання для захисту персональних даних.

Станція 1. Аудит приватності (5 хв.)

На першій станції здобувачі проводять ретельний аналіз налаштувань конфіденційності у двох соціальних мережах на вибір (Facebook/Instagram або TikTok). Використовуючи спеціально розроблений чек-лист у Google Формах, вони перевіряють такі параметри як видимість профілю, доступ до особистої інформації, налаштування публікацій, можливість позначати на фото, доступ до списку друзів тощо. За виявлення та виправлення 5 і більше небезпечних налаштувань здобувач отримує 15 балів.

Чек-лист для перевірки налаштувань приватності

- ✓ Зробити профіль приватним
- ✓ Приховати дату народження (рік)
- ✓ Приховати номер телефону
- ✓ Приховати email
- ✓ Налаштувати «Хто може бачити друзів» → Тільки я / Друзі
- ✓ Вимкнути геолокацію в публікаціях
- ✓ Налаштувати «Хто може позначати на фото» → З підтвердженням
- ✓ Увімкнути двофакторну автентифікацію (якщо можливо)
- ✓ Переглянути підключені застосунки, видалити непотрібні
- ✓ Перевірити активні сесії, завершити підозрілі

Станція 2. Менеджер паролів (5 хв.)

Друга станція присвячена одному з найважливіших аспектів цифрової безпеки – надійним паролям. Здобувачі встановлюють на свій пристрій застосунок Bitwarden (рис. 2.3) та створюють три надійні паролі згідно з критеріями: мінімум 12 символів, комбінація великих і малих літер, цифр та спеціальних символів. Успішне виконання цього завдання оцінюється в 20 балів.

Станція 3. Детектив з персональних даних (6 хв.)

Третя станція пропонує здобувачам провести розслідування власного

цифрового сліду. Вони здійснюють пошук власних персональних даних у Google, використовуючи своє ім’я, e-mail та номер телефону як пошукові запити. Після пошуку необхідно проаналізувати, які дані були знайдені та які з них потрібно видалити або заховати. Детальний звіт обсягом мінімум 100 слів оцінюється в 15 балів.

Рис. 2.3 Bitwarden Password Manager

Станція 4. Симулятор фішингу (7 хв.)

Четверта станція використовує інтерактивний тренінг з розпізнавання фішингу. Здобувачам пропонується розпізнати 8 електронних листів і визначити, які з них є фішингом, а які – легітимними повідомленнями. Здобувачі мають звертати увагу на підозрілі ознаки: помилки в тексті, підроблені адреси відправників, підозрілі посилання, надмірну терміновість тощо. За результат 7 і більше правильних відповідей із восьми нараховується 25 балів, що є найвищою оцінкою серед станцій квесту.

Приклади повідомлень

Повідомлення 1

```
Від: support@privatbank.ua.verify.com
Ваш рахунок заблоковано! Перейдіть ТЕРМІНОВО:
http://bit.ly/pb-verify
```

Правильна відповідь: фішинг.

Повідомлення 2

```
Viber: Привіт! Дивись який кльовий сайт знайшов:
```

www.super-prizz.com

Можна виграти айфон!

Відповідь: фішинг.

Повідомлення 3:

Від: no-reply@google.com

Subject: Новий вхід у ваш обліковий запис Google

Пристрій: iPhone 13

Місце: Київ, Україна

Час: 14:23, 8 листопада 2024

Якщо це були не ви, змініть пароль.

Відповідь: легітимне.

Станція 5. Налаштування конфіденційності (7 хв.)

П’ята завершальна станція вимагає комплексного застосування всіх отриманих знань. Здобувачі повинні виконати три практичні завдання: вимкнути геолокацію для застосунків, яким вона об’єктивно не потрібна (наприклад, калькулятор чи ліхтарик), налаштувати двофакторну автентифікацію хоча б для одного важливого сервісу (пошта, банківський додаток) та ретельно перевірити дозволи всіх встановлених мобільних застосунків. За виконання всіх трьох пунктів з підтвердженням скриншотами нараховується 25 балів.

Під час проходження квесту викладач активно консультує здобувачів, моніторить їхній прогрес у таблиці лідерів, надсилає мотиваційні push-повідомлення та надає допомогу тим, хто відстає або стикається з технічними труднощами. На кожну станцію встановлено таймер, а прогрес відображається в режимі реального часу, що додає динамічності та змагальності. Три найшвидші учасники, які успішно виконали всі завдання, отримують бонус у 10 балів.

6. Підсумкове закріплення матеріалу (10 хв.)

Мікромодуль 4. Битва знань

Заняття наближається до завершення інтерактивною вікториною в Kahoot!, яка об’єднує всі вивчені теми (рис. 2.4). Викладач запускає гру з 15 ретельно підібраних питань різної складності та модерує процес, коментуючи правильні відповіді та пояснюючи типові помилки.

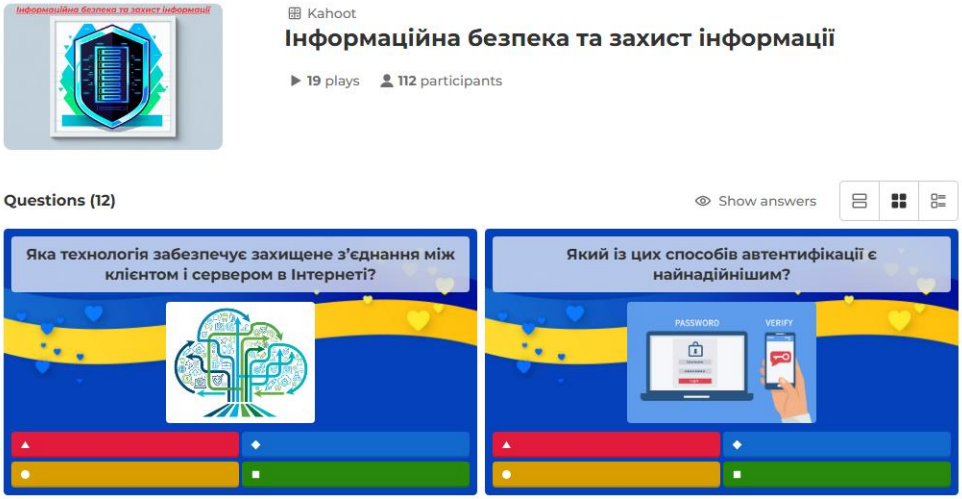


Рис. 2.4 Вікторина в Kahoot!

Питання охоплюють визначення персональних даних, ризики та загрози їх розголошення, методи захисту, законодавство про захист даних та практичні ситуації з реального життя. Після кожного питання відбувається короткий аналіз помилок, що має важливе навчальне значення. Топ-3 гравці за підсумками вікторини отримують відповідно 30, 20 та 10 балів, а всі інші учасники заохочуються 5 балами за активну участь.

7. Рефлексія та підбиття підсумків (5 хв.)

Викладач оголошує переможців згідно з таблицею лідерів та проводить урочисте нагородження віртуальними значками. Здобувачі, які набрали 80 і більше балів, отримують почесний значок «Гуру приватності», ті, хто набрав від 60 до 79 балів – значок «Захисник даних», а учасники з результатом від 40 до 59 балів нагороджуються значком «Свідомий користувач».

Здобувачі беруть участь у експрес-опитуванні «Що нового ми

дізналися?», результати якого відображаються на спільному екрані. У спільному документі здобувачі залишають смайлики-емоції, які відображають їхнє ставлення до заняття: ☺ означає, що все зрозуміло і здобувач готовий застосовувати знання на практиці, 😐 сигналізує про наявність запитань і потребу в додатковій консультації, а вказує на складність матеріалу та необхідність його повторення.

8. Домашнє завдання (5 хв.)

Базовий рівень: проходження повного курсу «Кібербезпека» на платформі «Дія. Освіта» з акцентом на модулі про персональні дані та надсилання отриманого сертифіката.

Середній рівень: створення власної інфографіки «5 правил захисту персональних даних» у Canva.

Високий рівень: провести аудит цифрової безпеки для члена родини (батьків, бабусі або дідуся) та підготувати детальний звіт з персональними рекомендаціями.

Додаткове завдання: встановити на тиждень застосунок для моніторингу дозволів мобільних застосунків (наприклад, App Privacy Manager) та проаналізувати результати його роботи.

Гейміфікація поширюється і на домашнє завдання: за виконання до наступного заняття нараховується 20 балів, за особливо оперативне виконання у перші три дні додається бонус 10 балів, а публікація роботи у чаті групи приносить додаткові 15 балів.

Таким чином, реалізація мобільного навчання на занятті забезпечується через доступність всіх навчальних матеріалів через мобільні застосунки, що дозволяє здобувачам працювати з будь-якого місця. Принцип мікронавчання втілюється через поділ матеріалу на короткі блоки тривалістю 3-7 хвилин, кожен з яких має конкретну мікроціль. Система push-повідомлень підтримує

увагу здобувачів протягом усього заняття, нагадуючи про ключові моменти та мотивуючи до активності. Під час квесту здобувачі мають можливість працювати у власному темпі, що особливо важливо для реалізації особистісно-орієнтованого підходу. Навіть конспектування здійснюється на мобільних пристроях, що робить процес навчання природним для сучасних здобувачів.

Гейміфікація пронизує всю структуру заняття через прозору систему балів та рівнів досягнень, яка чітко мотивує здобувачів. Таблиця лідерів оновлюється в режимі реального часу, створюючи атмосферу здорової конкуренції та дозволяючи кожному відстежувати свій прогрес. Система значків та досягнень забезпечує візуальне визнання успіхів здобувачів. Елементи змагання закладені в квест та вікторину. Негайний зворотний зв’язок після кожного завдання дозволяє здобувачам одразу бачити результати своєї роботи та коригувати дії.

Таким чином, заняття дозволяє впровадити розроблену методику та реалізувати організаційно-педагогічні умови.

Висновки до другого розділу

У другому розділі дипломної роботи здійснено розробку та впровадження методики використання ЦТ для формування навичок з ІБ здобувачів ФПО, що дозволяє сформулювати наступні висновки.

1. Розроблено модель використання ЦТ для формування навичок з ІБ, яка включає п’ять взаємопов’язаних блоків: цільовий (визначає мету та завдання), теоретико-методологічний (обґрунтовує підходи та принципи), змістовий (містить тематичні модулі), організаційно-методичний (конкретизує форми, методи та засоби навчання) та діагностико-результативний (визначає критерії оцінювання ефективності). Модель є теоретичною основою методики та забезпечує системність і цілісність процесу формування навичок з ІБ.

2. Практично реалізовано елементи методики шляхом створення детального плану-конспекту заняття на тему «Захист персональних даних у цифровому середовищі». Заняття побудоване з урахуванням усіх компонентів моделі та передбачає реалізацію визначених організаційно-педагогічних умов. Розроблені матеріали можуть бути використані викладачами закладів ФПО для формування навичок з ІБ здобувачів різних спеціальностей.

Таким чином, у другому розділі вирішено завдання дослідження щодо розробки та впровадження елементів методики використання ЦТ для формування навичок з ІБ здобувачів ФПО, створено необхідне теоретичне та методичне підґрунтя для проведення експериментальної перевірки ефективності методики.

РОЗДІЛ 3

ДОСЛІДНО-ЕКСПЕРИМЕНТАЛЬНА ПЕРЕВІРКА ЕФЕКТИВНОСТІ МЕТОДИКИ ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ ДЛЯ ФОРМУВАННЯ НАВИЧОК З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗДОБУВАЧІВ ФАХОВОЇ ПЕРЕДВИЩОЇ ОСВІТИ

РОЗДІЛ 3
ДОСЛІДНО-ЕКСПЕРИМЕНТАЛЬНА ПЕРЕВІРКА ЕФЕКТИВНОСТІ МЕТОДИКИ ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ ДЛЯ ФОРМУВАННЯ НАВИЧОК З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗДОБУВАЧІВ ФАХОВОЇ ПЕРЕДВИЩОЇ ОСВІТИ

3.1 Критерії та показники ефективності використання цифрових технологій для формування навичок з інформаційної безпеки здобувачів фахової передвищої освіти

Ефективність будь-якого педагогічного дослідження значною мірою залежить від правильно обраних критеріїв та показників, які дозволяють об’єктивно оцінити результати експериментальної роботи. У контексті нашого дослідження особливої актуальності набуває питання визначення критеріїв та показників сформованості навичок з ІБ у здобувачів ФПО, оскільки саме вони становлять методологічну основу для діагностики, вимірювання та оцінювання ефективності педагогічних впливів.

У педагогічній науці поняття «критерій» трактується як ознака, на підставі якої здійснюється оцінка, визначення або класифікація певного явища чи процесу [41]. За визначенням С. Гончаренка, критерій – це «ознака, на основі якої проводиться оцінка, судження; мірило оцінки» [7, с. 182]. Критерії виконують важливу функцію в педагогічному дослідженні, оскільки вони дозволяють перевести якісні характеристики досліджуваного явища в площину емпіричного виміру та аналізу. О. Пометун та Л. Пироженко зазначають, що «критерії – це якості, властивості, ознаки досліджуваного об’єкта, які дають змогу оцінити його стан і рівень функціонування та розвитку» [32, с. 89].

Тісно пов’язаним з поняттям критерію є поняття показника. Якщо критерій визначає загальний напрям оцінювання, то показник конкретизує його, відображаючи певні прояви, характеристики або ступінь вияву критерію. Показники виступають як конкретні, доступні для спостереження та фіксації якісні або кількісні характеристики, що дозволяють судити про наявність і ступінь розвитку того чи іншого критерію. «Показник – це складова частина критерію, конкретна міра його вияву, за якою можна судити про наявність певної якості й рівень її розвитку» [40, с. 156]. Таким чином, співвідношення між критерієм і показником можна визначити як співвідношення між загальним і конкретним, між сутністю явища і формами його прояву.

У педагогічному експерименті критерії та показники відіграють ключову роль на різних етапах дослідження. На підготовчому етапі вони забезпечують можливість діагностики початкового стану досліджуваного явища, що є необхідною умовою для подальшого порівняння результатів. На формувальному етапі критерії та показники виступають як орієнтири для здійснення педагогічних впливів, допомагаючи визначити напрями та зміст експериментальної роботи. На контрольному етапі вони дозволяють об’єктивно оцінити ефективність проведеної роботи, зафіксувати зміни, що відбулися, та зробити обґрунтовані висновки щодо підтвердження або спростування гіпотези дослідження.

Визначення критеріїв та показників у педагогічному дослідженні має відповідати низці вимог [32, с. 90–91]:

– критерії повинні бути об’єктивними, тобто відображати сутнісні, закономірні ознаки досліджуваного явища, а не випадкові чи другорядні його характеристики;

– критерії мають бути валідними, тобто дійсно вимірювати саме те явище, для оцінки якого вони призначені;

– критерії та показники повинні бути надійними, забезпечуючи

стабільність результатів вимірювання незалежно від часу проведення діагностики та особи дослідника;

– критерії мають бути достатніми для всебічної характеристики досліджуваного явища і водночас не надмірними, щоб не ускладнювати процедуру діагностики;

– показники повинні бути доступними для спостереження, фіксації та вимірювання.

Особливу складність становить визначення критеріїв та показників для оцінювання сформованості навичок, які за своєю природою є складними, багатокомпонентними утвореннями. Навички з ІБ не є винятком – вони інтегрують у собі когнітивний, діяльнісний, мотиваційний та рефлексивний компоненти, кожен з яких потребує окремого оцінювання. Тому для комплексної діагностики рівня сформованості навичок з ІБ необхідна система критеріїв, яка охоплювала б усі ці компоненти та давала можливість отримати цілісне уявлення про готовність здобувачів до безпечної діяльності в цифровому середовищі.

Крім критеріїв та показників, важливим елементом діагностичного апарату є визначення рівнів сформованості досліджуваної якості. Рівні відображають ступінь, міру вияву певної якості і дозволяють диференціювати здобувачів за досягнутими результатами. У педагогічних дослідженнях найчастіше виділяють три або чотири рівні сформованості певної якості, що забезпечує достатню диференціацію результатів і водночас зберігає простоту та зручність оцінювання. Характеристика рівнів здійснюється на основі усіх виокремлених критеріїв та їх показників, що дозволяє створити цілісний «портрет» здобувача, який перебуває на певному рівні сформованості навичок [40, с. 157–158].

Таким чином, розробка системи критеріїв, показників та рівнів сформованості навичок з ІБ є важливим етапом нашого дослідження, що

створює методологічну основу для проведення діагностики, здійснення формувальної роботи та оцінювання її ефективності. Ця система має забезпечити об'єктивність, валідність та надійність результатів експериментального дослідження, а також можливість порівняння даних, отриманих на різних етапах експерименту.

Аналіз психолого-педагогічної літератури [7; 13; 32; 40] та специфіки навичок з ІБ дозволив нам виокремити чотири основні критерії оцінювання: інформаційно-теоретичний, операційно-практичний, ціннісно-мотиваційний та оцінювально-аналітичний. Кожен із цих критеріїв відображає певний аспект готовності здобувачів до безпечної діяльності в цифровому середовищі та характеризується відповідними показниками (табл. 3.1).

Таблиця 3.1

Критерії та показники оцінки сформованості навичок з ІБ здобувачів ФПО

Критерій	**Опис критерію**	**Показники критерію**
Інформаційно-теоретичний	Характеризує рівень знань здобувачів про ІБ, розуміння основних концепцій, видів загроз, методів захисту інформації. Цей критерій є базовим, оскільки саме знання становлять теоретичну основу для формування практичних навичок безпечної поведінки в цифровому просторі.	– розуміння сутності та значення ІБ в сучасному суспільстві; – знання основних видів цифрових загроз (віруси, фішинг, соціальна інженерія, кібербулінг тощо); – обізнаність щодо методів та інструментів захисту особистої інформації; – знання основних правил безпечної поведінки в мережі Інтернет; – розуміння правових аспектів використання цифрової інформації та захисту персональних даних; – знання принципів створення надійних паролів та управління обліковими записами
Операційно-практичний	Відображає здатність здобувачів практично застосовувати знання з ІБ, використовувати інструменти захисту, налаштовувати параметри безпеки пристроїв та застосунків. Цей критерій демонструє перехід від теоретичних знань до їх	– уміння встановлювати та налаштовувати антивірусне програмне забезпечення; – здатність налаштовувати параметри приватності в соціальних мережах та інших онлайн-сервісах; – навички створення та використання надійних паролів, застосування багатофакторної автентифікації; – уміння розпізнавати фішингові повідомлення та підозрілі веб-сайти;

Критерій	Опис критерію	Показники критерію
	практичної реалізації в повсякденній цифровій діяльності.	– навички резервного копіювання важливої інформації; – уміння реагувати на інциденти ІБ та звертатися по допомогу
Ціннісно-мотиваційний	Визначає ставлення здобувачів до питань ІБ, усвідомлення важливості захисту інформації, готовність дотримуватися правил безпечної поведінки в цифровому середовищі. Цей критерій є визначальним для формування стійкої поведінкової моделі, оскільки саме внутрішня мотивація та ціннісні орієнтації забезпечують систематичне дотримання правил ІБ.	– усвідомлення особистої відповідальності за безпеку власної інформації та даних інших користувачів; – розуміння цінності конфіденційності та приватності в цифровому середовищі; – інтерес до вивчення питань ІБ та бажання вдосконалювати відповідні навички; – готовність витрачати час та зусилля на забезпечення власної ІБ; – прагнення дотримуватися етичних норм поведінки в цифровому просторі; – бажання допомагати іншим у питаннях ІБ та поширювати культуру безпечної поведінки
Оцінювально-аналітичний	Характеризує здатність здобувачів аналізувати власну поведінку в цифровому середовищі, оцінювати ризики, приймати обґрунтовані рішення щодо ІБ. Цей критерій відображає найвищий рівень сформованості навичок, що передбачає не лише знання та вміння, а й здатність до критичного мислення та самоаналізу	– здатність критично оцінювати інформацію, що надходить з різних цифрових джерел; – уміння аналізувати потенційні ризики перед здійсненням певних дій в онлайн-середовищі; – навички самоаналізу власної цифрової поведінки та виявлення небезпечних практик; – здатність приймати виважені рішення в ситуаціях, пов’язаних з ІБ; – уміння прогнозувати можливі наслідки власних дій у цифровому просторі; – здатність адаптувати свою поведінку залежно від рівня ризику та специфіки цифрового середовища.

На основі виокремлених критеріїв та їх показників нами визначено три рівні сформованості навичок з ІБ: високий, середній та початковий. Охарактеризуємо кожен із цих рівнів детальніше (табл. 3.2).

На нашу думку, визначені критерії, показники та рівні сформованості навичок з ІБ створюють методологічну основу для діагностики та оцінювання ефективності педагогічних впливів, спрямованих на формування цих навичок у

здобувачів ФПО. Вони також дозволяють здійснювати моніторинг динаміки розвитку навичок з ІБ та своєчасно коригувати освітній процес відповідно до потреб здобувачів. Комплексний характер запропонованих критеріїв забезпечує всебічну оцінку готовності здобувачів до безпечної діяльності в цифровому середовищі, охоплюючи як когнітивну, так і практичну, ціннісну та рефлексивну складові цієї готовності.

Таблиця 3.2

Рівні сформованості навичок з ІБ здобувачів ФПО

Рівень	**Опис рівня**
Високий	Характеризується системними та глибокими знаннями про ІБ, усвідомленням різноманітних видів цифрових загроз та методів захисту від них. Здобувачі з високим рівнем демонструють впевнене володіння практичними навичками використання інструментів захисту інформації, самостійно налаштовують параметри безпеки пристроїв та застосунків, проактивно застосовують заходи захисту. Вони характеризуються високою внутрішньою мотивацією до забезпечення власної ІБ, усвідомлюють відповідальність за збереження інформації, виявляють ініціативу у вивченні нових аспектів ІБ. Здобувачі цього рівня здатні критично аналізувати різноманітні ситуації в цифровому середовищі, самостійно оцінювати ризики, приймати обґрунтовані рішення навіть у нестандартних ситуаціях, а також коригувати власну поведінку на основі рефлексії та аналізу попереднього досвіду.
Середній	Відзначається загальним розумінням основних концепцій ІБ, знанням найпоширеніших видів загроз та базових методів захисту, проте знання можуть бути фрагментарними або поверхневими. Здобувачі цього рівня володіють базовими практичними навичками забезпечення ІБ, можуть використовувати стандартні інструменти захисту за інструкцією або підказкою, проте не завжди застосовують їх систематично. Вони розуміють важливість ІБ, однак їхня мотивація до дотримання правил безпечної поведінки є непостійною та залежить від зовнішніх факторів або нагадувань. Здобувачі середнього рівня здатні оцінювати очевидні ризики у типових ситуаціях, проте відчувають труднощі при аналізі складних або нестандартних випадків, їхня рефлексія власної цифрової поведінки є епізодичною та потребує зовнішнього стимулювання.
Початковий	Характеризується обмеженими та несистемними знаннями про ІБ, фрагментарним розумінням цифрових загроз, відсутністю чіткого уявлення про методи захисту інформації. Практичні навички забезпечення ІБ у здобувачів цього рівня несформовані або сформовані на елементарному рівні, вони відчувають значні труднощі при використанні навіть базових інструментів захисту, потребують постійної допомоги та контролю. Мотивація до забезпечення власної

Рівень	Опис рівня
	ІБ у них відсутня або є дуже низькою, вони не усвідомлюють важливості захисту інформації, не виявляють інтересу до вивчення відповідних питань. Здобувачі початкового рівня не здатні самостійно оцінювати ризики в цифровому середовищі, не аналізують власну поведінку, не усвідомлюють можливих наслідків своїх дій в онлайн-просторі, їхні рішення щодо ІБ є імпульсивними та необґрунтованими.

3.2 Організація, проведення та аналіз результатів констатувального етапу педагогічного експерименту

Діагностичні процедури на констатувальному та формувальному етапах педагогічного експерименту проводилися на базі ВСП «Гірничо-електромеханічний фаховий коледж» Криворізького національного університету. В експерименті взяли участь 25 здобувачів ФПО. Здобувачі були розподілені на дві групи: експериментальну групу (ЕГ), до якої увійшло 13 осіб, та контрольну групу (КГ), до якої увійшло 12 осіб. Розподіл здобувачів між групами здійснювався випадковим чином з урахуванням приблизно однакової успішності та гендерного складу груп.

У нашому дослідженні ми використовували 5 взаємодоповнюючих методик діагностики, кожна з яких спрямована на оцінювання певних аспектів сформованості навичок з ІБ у здобувачів ФПО. Організація педагогічної діагностики здійснювалася на констатувальному етапі експерименту з метою визначення початкового рівня сформованості навичок з ІБ у здобувачів контрольної та експериментальної груп, а також на формувальному етапі для виявлення динаміки змін та оцінювання ефективності впроваджених організаційно-педагогічних умов.

Для діагностики *інформаційно-теоретичного критерію* нами було розроблено комплексний тест (див. додаток Б). Тест охоплював основні

тематичні блоки: поняття та сутність інформаційної безпеки, види цифрових загроз, методи та засоби захисту інформації, правила безпечної поведінки в мережі Інтернет, правові аспекти інформаційної безпеки, принципи створення та управління паролями. Структура тесту була побудована таким чином, щоб охопити всі показники інформаційно-теоретичного критерію. Тестування проводилося з використанням Google Форм, що забезпечувало автоматизовану перевірку більшості завдань та зручність обробки результатів. Результати діагностики за інформаційно-теоретичним критерієм представлено в табл. 3.3.

Таблиця 3.3

Розподіл здобувачів за рівнями сформованості навичок з ІБ за інформаційно-теоретичним критерієм на констатувальному етапі експерименту

Рівень	**ЕГ (*n* = 13)**		**КГ (*n* = 12)**	
	Кількість осіб	%	Кількість осіб	%
Високий	2	15,4	2	16,7
Середній	6	46,2	5	41,7
Початковий	5	38,4	5	41,6
Разом	**13**	**100**	**12**	**100**

Як свідчать дані таблиці 3.3, на констатувальному етапі експерименту рівень теоретичних знань з ІБ у більшості здобувачів обох груп виявився недостатнім. Високий рівень продемонстрували лише 2 здобувачі (15,4%) в ЕГ та 2 здобувачі (16,7%) у КГ. Середній рівень зафіксовано у 6 здобувачів (46,2%) ЕГ та 5 здобувачів (41,7%) КГ. На початковому рівні перебували 5 здобувачів (38,4%) ЕГ та 5 здобувачів (41,6%) КГ.

Для оцінювання *операційно-практичного критерію* використовувалася методика практичних ситуаційних завдань, яка дозволяла виявити здатність здобувачів практично застосовувати знання з ІБ в реальних або наближених до реальних ситуаціях. Було розроблено комплекс з 7 практичних завдань, кожне з яких моделювало типову ситуацію, що потребує застосування навичок з ІБ (додаток В). Виконання практичних завдань здійснювалося індивідуально в

комп'ютерному класі, де кожен здобувач мав доступ до необхідного програмного забезпечення та Інтернет-ресурсів. Результати діагностики за операційно-практичним критерієм представлено в таблиці 3.4.

Дані таблиці 3.4 засвідчують, що практичні навички застосування інструментів та методів ІБ у здобувачів обох груп сформовані на низькому рівні. Високий рівень виявлено лише в 1 здобувача (7,7%) ЕГ та 1 здобувача (8,3%) КГ. Середній рівень зафіксовано у 5 здобувачів (38,5%) ЕГ та 4 здобувачів (33,3%) КГ. Більшість здобувачів перебувала на початковому рівні: 7 осіб (53,8%) в ЕГ та 7 осіб (58,4%) у КГ. Це свідчить про недостатню практичну підготовку здобувачів у галузі ІБ та необхідність посилення практичної складової навчання.

Таблиця 3.4

Розподіл здобувачів за рівнями сформованості навичок з ІБ за операційно-практичним критерієм на констатувальному етапі експерименту

Рівень	**ЕГ (*n* = 13)**		**КГ (*n* = 12)**	
	Кількість осіб	%	Кількість осіб	%
Високий	1	7,7	1	8,3
Середній	5	38,5	4	33,3
Початковий	7	53,8	7	58,4
Разом	**13**	**100**	**12**	**100**

Для діагностики *ціннісно-мотиваційного критерію* була розроблена анкета, яка містила твердження, що відображали різні аспекти ставлення здобувачів до питань ІБ (додаток Д). Твердження анкети були згруповані відповідно до показників ціннісно-мотиваційного критерію: усвідомлення особистої відповідальності за безпеку інформації; розуміння цінності конфіденційності та приватності; інтерес до вивчення питань ІБ; готовність витрачати зусилля на забезпечення безпеки; дотримання етичних норм; бажання допомагати іншим. Анкетування проводилося анонімно для забезпечення щирості відповідей здобувачів. Результати діагностики за ціннісно-

мотиваційним критерієм представлено в таблиці 3.5.

Таблиця 3.5

Розподіл здобувачів за рівнями сформованості навичок з ІБ за ціннісно-мотиваційним критерієм на констатувальному етапі експерименту

Рівень	**ЕГ (*n* = 13)**		**КГ (*n* = 12)**	
	Кількість осіб	%	Кількість осіб	%
Високий	3	23,1	2	16,7
Середній	7	53,8	7	58,3
Початковий	3	23,1	3	25,0
Разом	**13**	**100**	**12**	**100**

Як показують дані таблиці 3.5, ціннісно-мотиваційна складова навичок з ІБ у здобувачів обох груп виявилася дещо краще сформованою порівняно з операційно-практичним критерієм. Високий рівень продемонстрували 3 здобувачі (23,1%) ЕГ та 2 здобувачі (16,7%) КГ. Переважна більшість здобувачів перебувала на середньому рівні: 7 осіб (53,8%) в ЕГ та 7 осіб (58,3%) у КГ. Початковий рівень зафіксовано у 3 здобувачів (23,1%) ЕГ та 3 здобувачів (25,0%) КГ. Це свідчить про те, що здобувачі загалом усвідомлюють важливість ІБ, однак їхня мотивація до систематичного дотримання правил безпечної поведінки є недостатньо стійкою.

Для діагностики *оцінювально-аналітичного критерію* використовувалася методика аналізу кейсів – проблемних ситуацій, що потребують критичного осмислення, оцінки ризиків та прийняття обґрунтованих рішень щодо інформаційної безпеки. Було розроблено 5 кейсів різного рівня складності, кожен з яких моделював реальну ситуацію, типову для цифрового середовища (додаток Е). Аналіз кейсів здійснювався здобувачами індивідуально у письмовій формі. Результати діагностики за оцінювально-аналітичним критерієм представлено в таблиці 3.6.

Дані таблиці 3.6 свідчать про низький рівень розвитку аналітичних та рефлексивних здібностей здобувачів у контексті ІБ. Високий рівень виявлено у

2 здобувачів (15,4%) ЕГ та 1 здобувача (8,3%) КГ. Середній рівень продемонстрували 4 здобувачі (30,8%) ЕГ та 4 здобувачі (33,3%) КГ. Більшість здобувачів перебувала на початковому рівні: 7 осіб (53,8%) в ЕГта 7 осіб (58,4%) у КГ. Здобувачі відчували значні труднощі при аналізі складних ситуацій, оцінці ризиків та прийнятті обґрунтованих рішень щодо ІБ.

Таблиця 3.6

Розподіл здобувачів за рівнями сформованості навичок з ІБ за оцінювально-аналітичним критерієм на констатувальному етапі експерименту

Рівень	**ЕГ (*n* = 13)**		**КГ (*n* = 12)**	
	Кількість осіб	%	Кількість осіб	%
Високий	2	15,4	1	8,3
Середній	4	30,8	4	33,3
Початковий	7	53,8	7	58,4
Разом	**13**	**100**	**12**	**100**

Додатковим методом діагностики, який дозволяв оцінити рефлексивні здібності здобувачів та їхню реальну поведінку в цифровому середовищі, було самооцінювання на основі щоденника цифрової активності (додаток Ж). Здобувачам пропонувалося протягом одного тижня фіксувати свою цифрову активність та аналізувати власну поведінку з точки зору ІБ. Щоденник містив структуровану форму для щоденних записів. Наприкінці тижня здобувачі мали проаналізувати зібрані дані та відповісти на узагальнюючі питання.

Ця методика дозволила оцінити не лише здатність здобувачів до рефлексії власної цифрової поведінки, але й виявити реальні практики використання цифрових технологій, які не завжди відповідають декларованим знанням та установкам. Порівняння результатів самооцінювання з результатами інших методик давало можливість виявити невідповідності між знаннями, ставленням та реальною поведінкою здобувачів.

Для визначення загального рівня сформованості навичок з ІБ результати всіх 5 методик узагальнювалися з урахуванням вагових коефіцієнтів, які

відображали значущість кожного критерію. Вагові коефіцієнти були визначені методом експертних оцінок за участю викладача інформатики згідно з рекомендаціями, наданими у посібнику [43]: інформаційно-теоретичний критерій – 0,20; операційно-практичний критерій – 0,30; ціннісно-мотиваційний критерій – 0,25; оцінювально-аналітичний критерій – 0,25.

Інтегральний показник (ІП) розраховувався за формулою:

$$ІП = (Б_1 \times 0{,}20) + (Б_2 \times 0{,}30) + (Б_3 \times 0{,}25) + (Б_4 \times 0{,}25) + (Б_5 \times 0{,}25),$$

де $Б_1$ – результат тестування (переведений у відсотки від максимального балу), $Б_2$ – результат практичних завдань (у відсотках), $Б_3$ – результат анкетування (у відсотках), $Б_4$ – результат аналізу кейсів (у відсотках), $Б_5$ – результат самооцінювання (у відсотках). У формулі сума коефіцієнтів дорівнює 1,25, оскільки методика самооцінювання розглядалася як додатковий діагностичний інструмент, що доповнює оцінювання оцінювально-аналітичного критерію. Тому підсумковий ІП нормувався діленням на 1,25.

Відповідно до отриманого ІП здобувачі розподілялися за рівнями: високий рівень – 80–100%, середній рівень – 50–79%, початковий рівень – 0–49%. Така інтегральна оцінка дозволяла отримати цілісне уявлення про рівень сформованості навичок з ІБ у кожного здобувача та в групі загалом. Узагальнені результати діагностики за всіма критеріями представлено в таблиці 3.7.

Таблиця 3.7

Узагальнені результати діагностики сформованості навичок з ІБ у здобувачів ФПО на констатувальному етапі експерименту (інтегральний показник)

Рівень	**ЕГ (*n* = 13)**		**КГ (*n* = 12)**	
	Кількість осіб	%	Кількість осіб	%
Високий	2	15,4	1	8,3
Середній	5	38,5	5	41,7
Початковий	6	46,1	6	50,0
Разом	**13**	**100**	**12**	**100**

Узагальнені дані таблиці 3.7 демонструють, що на констатувальному етапі

експерименту загальний рівень сформованості навичок з ІБ у здобувачів обох груп є низьким. Високий рівень зафіксовано лише у 2 здобувачів (15,4%) ЕГ та 1 здобувача (8,3%) КГ. Середній рівень продемонстрували 5 здобувачів (38,5%) ЕГ та 5 здобувачів (41,7%) КГ. Майже половина здобувачів перебувала на початковому рівні: 6 осіб (46,1%) в ЕГ та 6 осіб (50,0%) у КГ (рис. 3.1).

Поглиблений аналіз результатів діагностики дозволив виявити низку характерних проблем та особливостей у рівні сформованості навичок з ІБ у здобувачів ФПО. Так, за інформаційно-теоретичним критерієм було виявлено, що здобувачі мають фрагментарні знання про ІБ. Найбільші труднощі викликали питання, пов’язані з правовими аспектами захисту персональних даних, принципами роботи криптографічних методів захисту інформації та технічними деталями функціонування мережевих загроз. Водночас здобувачі демонстрували краще розуміння базових понять та загальновідомих видів загроз, таких як віруси та фішинг.

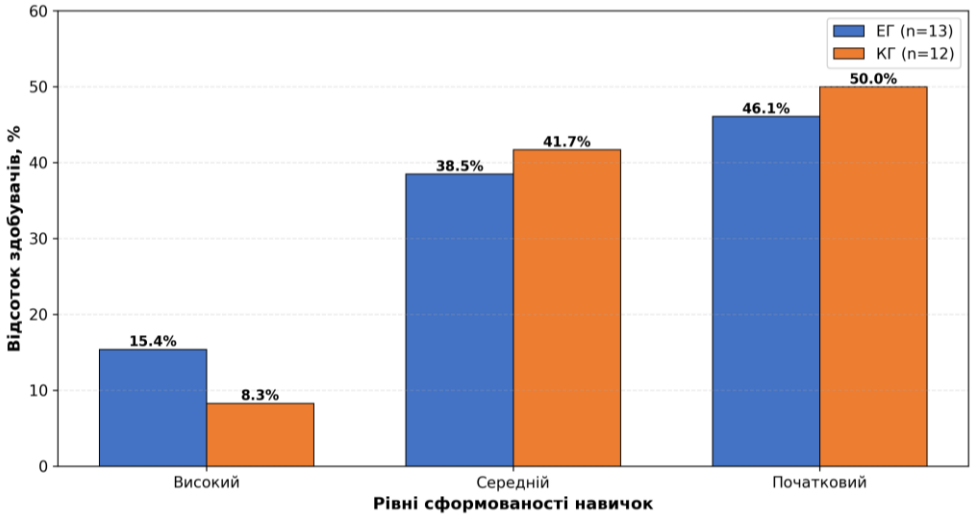


Рис. 3.1 Розподіл здобувачів за рівнями сформованості навичок з ІБ на констатувальному етапі експерименту

Результати виконання практичних ситуаційних завдань показали, що навіть за наявності теоретичних знань здобувачі часто не можуть застосувати їх на практиці. Особливо проблемними виявилися завдання на налаштування

параметрів приватності в соціальних мережах та створення надійних паролів.

Анкетування виявило певну суперечність між усвідомленням важливості ІБ та готовністю дотримуватися відповідних правил. Більшість здобувачів погоджувалися з твердженнями про важливість захисту особистих даних та необхідність використання заходів безпеки, однак значно менше здобувачів були готові витрачати час та зусилля на практичне впровадження цих заходів. Багато здобувачів відзначали, що питання ІБ здаються їм занадто складними для повсякденного застосування.

Аналіз кейсів показав, що здобувачі відчувають значні труднощі при оцінці ризиків у нестандартних ситуаціях. Вони схильні приймати інтуїтивні, необґрунтовані рішення, не аналізуючи всіх можливих наслідків. При цьому здобувачі рідко враховували контекстуальні фактори, які могли б вплинути на оцінку ситуації.

Самооцінювання цифрової поведінки виявило низький рівень рефлексії у більшості здобувачів. Багато щоденників містили лише поверхневі описи дій без глибокого аналізу. Здобувачі нечасто виявляли власні помилки або небезпечні практики, схильні були оцінювати свою поведінку як цілком безпечну. Плани щодо покращення власної цифрової поведінки часто були загальними та неконкретними, без чітких дій та термінів реалізації.

Таким чином, результати констатувального етапу педагогічного експерименту підтвердили необхідність розробки та впровадження організаційно-педагогічних умов ефективного формування навичок з ІБ у здобувачів ФПО.

3.3 Організація, проведення та аналіз результатів формувального етапу педагогічного експерименту

Метою формувального етапу педагогічного експерименту було впровадження організаційно-педагогічних умов ефективного використання ЦТ для формування навичок з ІБ у здобувачів ЕГ та перевірка їхньої ефективності.

В ЕГ реалізовувалася спеціально розроблена методика формування навичок з ІБ, яка передбачала систематичне та цілеспрямоване навчання здобувачів через інтеграцію питань ІБ у зміст навчальних дисциплін, використання активних методів навчання, організацію практико-орієнтованих занять, проведення тренінгів з формування безпечної цифрової поведінки, залучення здобувачів до участі в онлайн-курсах з питань ІБ. КГ навчалася за традиційною методикою без впровадження організаційно-педагогічних умов, питання ІБ розглядалися фрагментарно у рамках окремих тем з інформатики.

Після завершення формувального етапу експерименту було проведено повторну діагностику рівня сформованості навичок з ІБ у здобувачів обох груп з використанням тих самих методик, що й на констатувальному етапі.

Результати контрольного зрізу за *інформаційно-теоретичним критерієм* представлено в таблиці 3.8.

Таблиця 3.8

Розподіл здобувачів за рівнями сформованості навичок з ІБ за інформаційно-теоретичним критерієм на формувальному етапі експерименту

Рівень	**ЕГ (*n* = 13)**		**КГ (*n* = 12)**	
	Кількість осіб	%	Кількість осіб	%
Високий	7	53,8	3	25,0
Середній	5	38,5	5	41,7
Початковий	1	7,7	4	33,3
Разом	**13**	**100**	**12**	**100**

Дані таблиці 3.8 свідчать про суттєве покращення рівня теоретичних знань з ІБ у здобувачів ЕГ. Кількість здобувачів з високим рівнем збільшилася з 2 осіб (15,4%) до 7 осіб (53,8%), тобто більше ніж утричі. Середній рівень продемонстрували 5 здобувачів (38,5%), що майже не змінилося порівняно з констатувальним етапом. Водночас кількість здобувачів на початковому рівні значно зменшилася – з 5 осіб (38,4%) до 1 особи (7,7%).

У КГ також спостерігалася позитивна динаміка, але значно менш виражена: високий рівень зафіксовано у 3 здобувачів (25,0%) порівняно з 2 особами (16,7%) на початку експерименту, кількість здобувачів на початковому рівні зменшилася з 5 осіб (41,6%) до 4 осіб (33,3%).

Результати контрольного зрізу за *операційно-практичним критерієм* представлено в таблиці 3.9.

Таблиця 3.9

Розподіл здобувачів за рівнями сформованості навичок з ІБ за операційно-практичним критерієм на формувальному етапі експерименту

Рівень	**ЕГ (*n* = 13)**		**КГ (*n* = 12)**	
	Кількість осіб	%	Кількість осіб	%
Високий	6	46,2	2	16,7
Середній	6	46,2	4	33,3
Початковий	1	7,6	6	50,0
Разом	**13**	**100**	**12**	**100**

За даними таблиці 3.9, в ЕГ відбулися найбільш значущі зміни саме за операційно-практичним критерієм. Кількість здобувачів з високим рівнем практичних навичок зросла з 1 особи (7,7%) до 6 осіб (46,2%), що свідчить про шестиразове збільшення. Середній рівень продемонстрували 6 здобувачів (46,2%) порівняно з 5 особами (38,5%) на констатувальному етапі. Лише 1 здобувач (7,6%) залишився на початковому рівні порівняно з 7 особами (53,8%) на початку експерименту.

У КГ покращення виявилися мінімальними: високий рівень показали 2 здобувачі (16,7%) замість 1 особи (8,3%), середній рівень – 4 здобувачі (33,3%) замість 4 осіб (33,3%), початковий рівень – 6 здобувачів (50,0%) замість 7 осіб (58,4%).

Результати контрольного зрізу за ціннісно-мотиваційним критерієм представлено в таблиці 3.10.

Таблиця 3.10

Розподіл здобувачів за рівнями сформованості навичок з ІБ за ціннісно-мотиваційним критерієм на формувальному етапі експерименту

Рівень	**ЕГ (*n* = 13)**		**КГ (*n* = 12)**	
	Кількість осіб	%	Кількість осіб	%
Високий	8	61,5	3	25,0
Середній	4	30,8	7	58,3
Початковий	1	7,7	2	16,7
Разом	**13**	**100**	**12**	**100**

Як показують дані таблиці 3.10, в ЕГ відбулися суттєві позитивні зміни у ціннісно-мотиваційній сфері. Кількість здобувачів з високим рівнем мотивації до дотримання правил ІБ зросла з 3 осіб (23,1%) до 8 осіб (61,5%). Середній рівень продемонстрували 4 здобувачі (30,8%) порівняно з 7 особами (53,8%) на початку експерименту. На початковому рівні залишилася лише 1 особа (7,7%) замість 3 осіб (23,1%).

У КГ також спостерігалися певні покращення, але менш виражені: високий рівень зафіксовано у 3 здобувачів (25,0%) замість 2 осіб (16,7%), кількість здобувачів на середньому рівні залишилася незмінною – 7 осіб (58,3%), а на початковому рівні зменшилася з 3 осіб (25,0%) до 2 осіб (16,7%).

Результати контрольного зрізу за оцінювально-аналітичним критерієм представлено в таблиці 3.11.

Дані таблиці 3.11 засвідчують позитивну динаміку розвитку аналітичних та рефлексивних здібностей здобувачів ЕГ. Кількість здобувачів з високим

рівнем збільшилася з 2 осіб (15,4%) до 5 осіб (38,5%). Середній рівень продемонстрували 7 здобувачів (53,8%) порівняно з 4 особами (30,8%) на констатувальному етапі. На початковому рівні залишилася лише 1 особа (7,7%) замість 7 осіб (53,8%).

Таблиця 3.11

Розподіл здобувачів за рівнями сформованості навичок з ІБ за оцінювально-аналітичним критерієм на формувальному етапі експерименту

Рівень	**ЕГ (*n* = 13)**		**КГ (*n* = 12)**	
	Кількість осіб	%	Кількість осіб	%
Високий	5	38,5	1	8,3
Середній	7	53,8	5	41,7
Початковий	1	7,7	6	50,0
Разом	**13**	**100**	**12**	**100**

У КГ зміни були мінімальними: кількість здобувачів на високому рівні залишилася незмінною – 1 особа (8,3%), середній рівень показали 5 здобувачів (41,7%) замість 4 осіб (33,3%), початковий рівень – 6 здобувачів (50,0%) замість 7 осіб (58,4%).

Узагальнені результати контрольного зрізу за всіма критеріями представлено в таблиці 3.12 та на діаграмі (рис. 3.2).

Узагальнені дані таблиці 3.12 демонструють, що на формувальному етапі експерименту загальний рівень сформованості навичок з ІБ у здобувачів ЕГ значно підвищився. Високий рівень зафіксовано у 7 здобувачів (53,8%) порівняно з 2 особами (15,4%) на початку експерименту, що свідчить про майже чотириразове збільшення. Середній рівень продемонстрували 5 здобувачів (38,5%), що майже не змінилося. Кількість здобувачів на початковому рівні значно зменшилася – з 6 осіб (46,1%) до 1 особи (7,7%).

У КГ також спостерігалася деяка позитивна динаміка, проте вона була значно менш вираженою: високий рівень показали 2 здобувачі (16,7%) замість 1

особи (8,3%), середній рівень – 6 здобувачів (50,0%) замість 5 осіб (41,7%), початковий рівень – 4 здобувачі (33,3%) замість 6 осіб (50,0%).

Таблиця 3.12

Узагальнені результати діагностики сформованості навичок з ІБ у здобувачів на формувальному етапі експерименту (інтегральний показник)

Рівень	**ЕГ (*n* = 13)**		**КГ (*n* = 12)**	
	Кількість осіб	%	Кількість осіб	%
Високий	7	53,8	2	16,7
Середній	5	38,5	6	50,0
Початковий	1	7,7	4	33,3
Разом	**13**	**100**	**12**	**100**

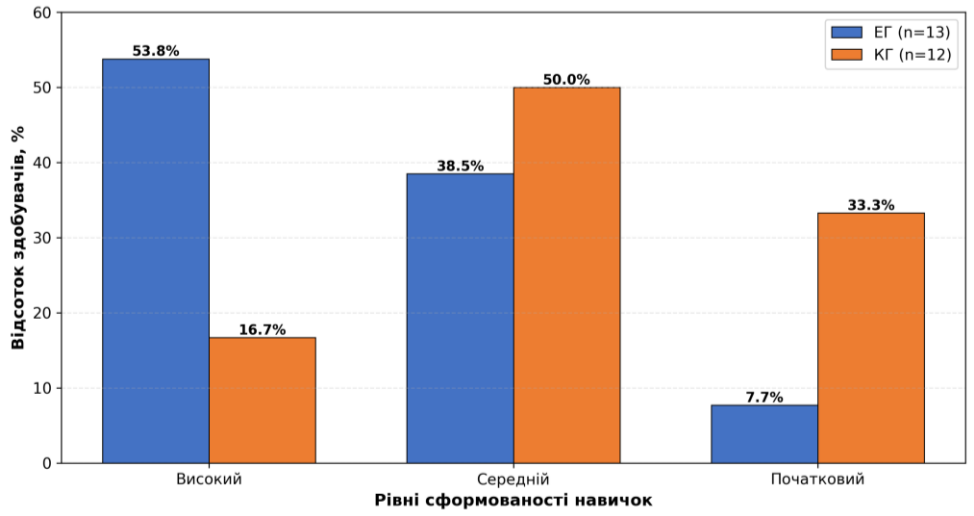


Рис. 3.2 Розподіл здобувачів за рівнями сформованості навичок з ІБ на формувальному етапі експерименту

Для визначення статистичної значущості відмінностей між ЕГ та КГ на формувальному етапі експерименту було використано критерій χ^2 Пірсона [43]. Цей критерій дозволяє визначити, чи існують статистично значущі відмінності між розподілами здобувачів за рівнями сформованості навичок у двох групах. Критерій χ^2 розраховується за формулою:

$$\chi^2 = \Sigma\ [(O - E)^2 / E],$$

де O – спостережувана частота (фактична кількість здобувачів на певному рівні), E – очікувана частота (теоретична кількість здобувачів, якщо розподіли однакові).

Очікувана частота для кожної комірки таблиці розраховується за формулою:

E = (сума рядка × сума стовпця) / загальна сума.

Виконаємо розрахунок критерію χ^2 для ІП на формувальному етапі (за таблицею 3.12). Результати розрахунків представлено у таблиці 3.13.

Таблиця 3.13

Розрахунок критерію Пірсона для ІП на формувальному етапі експерименту

Рівень	**ЕГ (O)**	**КГ (O)**	**Сума рядка**	**E (ЕГ)**	**E (КГ)**	**$(O-E)^2/E$ (ЕГ)**	**$(O-E)^2/E$ (КГ)**
Високий	7	2	9	4,68	4,32	1,150	1,245
Середній	5	6	11	5,72	5,28	0,091	0,098
Початковий	1	4	5	2,60	2,40	0,985	1,067
Разом	**13**	**12**	**25**	–	–	**2,226**	**2,410**

χ^2спостер. = 2,226 + 2,410 = 4,636.

Для визначення критичного значення χ^2 необхідно встановити рівень значущості та кількість ступенів свободи. Приймаємо рівень значущості $\alpha = 0,05$ (що відповідає 95% довірчій ймовірності). Кількість ступенів свободи визначається за формулою:

df = (кількість рядків – 1) × (кількість стовпців – 1) = (3 – 1) × (2 – 1) = 2.

За таблицею критичних значень χ^2 для df = 2 та $\alpha = 0,05$: χ^2критич. = 5,991.

Оскільки χ^2спостер. = 4,636 < χ^2критич. = 5,991, формально відмінності між групами не досягають рівня статистичної значущості при $\alpha = 0,05$. Проте значення χ^2спостер. наближається до критичного, що свідчить про тенденцію до статистично значущих відмінностей.

Для більш детального аналізу ефективності експерименту доцільно також порівняти динаміку змін всередині кожної групи. Для цього застосуємо

критерій χ^2 Пірсона для порівняння результатів констатувального та формувального етапів окремо для ЕГ та КГ (табл. 3.14, 3.15).

Таблиця 3.14

ЕГ, порівняння констатувального та формувального етапів експерименту

Рівень	**Констатувальний (О)**	**Формувальний (О)**	**Сума**	**Е (конст.)**	**Е (форм.)**	**(О-Е)²/Е (конст.)**	**(О-Е)²/Е (форм.)**
Високий	2	7	9	4,5	4,5	1,389	1,389
Середній	5	5	10	5,0	5,0	0,000	0,000
Початковий	6	1	7	3,5	3,5	1,786	1,786
Разом	**13**	**13**	**26**	–	–	**3,175**	**3,175**

χ^2спостер. = 3,175 + 3,175 = 6,350.

За таблицею критичних значень χ^2 для df = 2 та α = 0,05: χ^2критич. = 5,991.

Оскільки χ^2спостер. = 6,350 > χ^2критич. = 5,991, відмінності між результатами констатувального та формувального етапів в ЕГ є статистично значущими (p < 0,05). Це підтверджує ефективність впроваджених організаційно-педагогічних умов.

Таблиця 3.15

КГ, порівняння констатувального та формувального етапів експерименту

Рівень	**Констатувальний (О)**	**Формувальний (О)**	**Сума**	**Е (конст.)**	**Е (форм.)**	**(О-Е)²/Е (конст.)**	**(О-Е)²/Е (форм.)**
Високий	1	2	3	1,5	1,5	0,167	0,167
Середній	5	6	11	5,5	5,5	0,045	0,045
Початковий	6	4	10	5,0	5,0	0,200	0,200
Разом	**12**	**12**	**24**	-	-	**0,412**	**0,412**

χ^2спостер. = 0,412 + 0,412 = 0,824.

За таблицею критичних значень χ^2 для df = 2 та α = 0,05: χ^2критич. = 5,991.

Оскільки χ^2спостер. = 0,824 < χ^2критич. = 5,991, відмінності між результатами констатувального та формувального етапів у КГ не є статистично значущими (p > 0,05). Це означає, що зміни, які відбулися в КГ, можуть бути

пояснені природним перебігом освітнього процесу, а не цілеспрямованим педагогічним впливом.

Поглиблений аналіз результатів формувального етапу експерименту дозволив виявити якісні зміни, які відбулися у здобувачів ЕГ.

За інформаційно-теоретичним критерієм здобувачі ЕГ продемонстрували значно кращі результати при виконанні тестових завдань. Вони не лише знали основні поняття та види загроз, але й розуміли механізми їх функціонування, могли пояснити принципи роботи різних методів захисту інформації. Особливо помітним було покращення у знаннях правових аспектів ІБ та технічних деталей криптографічних методів захисту, які викликали найбільші труднощі на констатувальному етапі. Здобувачі продемонстрували системне розуміння взаємозв’язків між різними аспектами ІБ.

Виконання практичних ситуаційних завдань показало, що здобувачі ЕГ набули впевнених практичних навичок застосування інструментів та методів ІБ. Вони успішно налаштовували антивірусне програмне забезпечення, параметри приватності в соціальних мережах, створювали надійні паролі з використанням менеджерів паролів. Здобувачі почали використовувати ці навички не лише під час виконання завдань, але й у повсякденному житті. При розпізнаванні фішингових повідомлень здобувачі ЕГ звертали увагу на різноманітні індикатори загроз, включаючи тонкі технічні деталі, які раніше залишалися поза їхньою увагою.

Результати повторного анкетування виявили суттєві позитивні зміни у ціннісно-мотиваційній сфері здобувачів ЕГ. Вони не лише декларували важливість ІБ, але й демонстрували реальну готовність витрачати час та зусилля на її забезпечення. Багато здобувачів відзначали, що питання ІБ перестали здаватися їм занадто складними, оскільки вони набули необхідних знань та навичок. Здобувачі висловлювали бажання допомагати друзям та родичам у питаннях ІБ, ділитися отриманими знаннями.

Аналіз кейсів показав значне покращення аналітичних здібностей здобувачів ЕГ. Вони демонстрували системний підхід до аналізу проблемних ситуацій, враховували різноманітні фактори, оцінювали потенційні ризики з різних точок зору. Рішення, які приймали здобувачі, були добре обґрунтованими, враховували баланс між безпекою та зручністю, передбачали можливі наслідки. Здобувачі не обмежувалися простими категоричними рішеннями, а розглядали різні альтернативи та вибирали оптимальні варіанти залежно від контексту ситуації.

Повторне самооцінювання цифрової поведінки виявило значне підвищення рівня рефлексії у здобувачів ЕГ. Їхні щоденники містили детальний та глибокий аналіз власної цифрової активності. Здобувачі самостійно виявляли помилки та небезпечні практики у своїй поведінці, критично оцінювали прийняті рішення. Плани щодо покращення власної цифрової поведінки були конкретними, реалістичними та містили чіткі кроки з термінами реалізації. Багато здобувачів відзначали, що процес самоаналізу допоміг їм усвідомити приховані ризики у власній цифровій поведінці та мотивував їх до змін.

У КГ також спостерігалися певні покращення, що є природним наслідком освітнього процесу. Проте ці зміни були значно менш вираженими та менш системними порівняно з ЕГ. Здобувачі КГ продемонстрували деяке покращення навичок з ІБ, однак воно мало фрагментарний характер і не супроводжувалося суттєвими змінами у мотиваційній та рефлексивній сферах.

Результати формувального етапу педагогічного експерименту підтвердили ефективність впроваджених організаційно-педагогічних умов формування навичок з ІБ у здобувачів ФПО. В ЕГ відбулися статистично значущі позитивні зміни за всіма визначеними критеріями: інформаційно-теоретичним, операційно-практичним, ціннісно-мотиваційним та оцінювально-аналітичним.

Висновки до третього розділу

У третьому розділі дипломної роботи здійснено дослідно-експериментальну перевірку ефективності методики використання ЦТ для формування навичок з ІБ здобувачів ФПО, що дозволяє сформулювати наступні висновки.

1. Визначені критерії, показники та рівні сформованості навичок з ІБ здобувачів ФПО, які є методологічною основою для діагностики та оцінювання ефективності педагогічних впливів, спрямованих на формування цих навичок у здобувачів ФПО.

2. Результати констатувального етапу педагогічного експерименту підтвердили необхідність розробки та впровадження організаційно-педагогічних умов ефективного формування навичок з ІБ у здобувачів ФПО.

3. Результати формувального етапу педагогічного експерименту підтвердили ефективність впроваджених організаційно-педагогічних умов формування навичок з ІБ у здобувачів ФПО. В ЕГ відбулися статистично значущі позитивні зміни за всіма визначеними критеріями: інформаційно-теоретичним, операційно-практичним, ціннісно-мотиваційним та оцінювально-аналітичним. Найбільш виражені зміни спостерігалися за операційно-практичним критерієм, що свідчить про ефективність практико-орієнтованого підходу до навчання, використання активних методів та організації занять. Значущі позитивні зміни відбулися також у ціннісно-мотиваційній сфері, що підтверджує важливість формування не лише знань та вмінь, але й ціннісного ставлення до питань ІБ.

4. Статистичний аналіз з використанням критерію Пірсона підтвердив, що зміни в ЕГ є статистично значущими, тоді як у контрольній групі статистично значущих змін не виявлено. Це дозволяє стверджувати, що покращення

результатів в ЕГ є наслідком впровадження організаційно-педагогічних умов, а не природного перебігу освітнього процесу.

5. Кількісні та якісні результати експерименту дають підстави для висновку про те, що розроблена методика формування навичок з ІБ є ефективною і може бути рекомендована для впровадження у практику роботи закладів ФПО.

ВИСНОВКИ

У магістерській роботі здійснено теоретичне обґрунтування та експериментальну перевірку методики використання ЦТ для формування навичок з ІБ здобувачів ФПО. Проведене дослідження дозволяє сформулювати наступні висновки.

1. Проаналізовано науково-методичну, психолого-педагогічну та навчальну літературу з проблеми дослідження. Встановлено, що в умовах інтенсивної цифровізації освіти та воєнного стану в Україні питання ІБ набувають критичного значення. Систематизовано наукові підходи до визначення сутності ІБ в освіті та конкретизовано поняття навичок з ІБ як сукупності знань та умінь для безпечного, відповідального та етичного використання цифрових технологій. Виявлено основні загрози ІБ, з якими стикаються учасники освітнього процесу.

2. Визначено та теоретично обґрунтовано організаційно-педагогічні умови використання ЦТ у формуванні навичок з ІБ. Першою умовою визначено реалізацію мобільного навчання як форми організації навчальної діяльності з формування навичок ІБ здобувачів ФПО. Другою умовою є впровадження технології гейміфікації як інноваційного засобу організації навчальної діяльності з формування навичок ІБ здобувачів ФПО. Розкрито педагогічний потенціал ЦТ, зокрема відкритих освітніх ресурсів та мобільних застосунків для формування навичок з ІБ.

3. Розроблено модель використання ЦТ для формування навичок з ІБ у здобувачів ФПО. Модель включає п’ять взаємопов’язаних блоків: цільовий (визначає мету та завдання дослідження), теоретико-методологічний (обґрунтовує системний, діяльнісний, особистісно-орієнтований, компетентнісний та технологічний підходи, а також принципи навчання),

змістовий (містить тематичні модулі з основ ІБ, захисту персональних даних, кібербезпеки, безпечної комунікації та правових аспектів), організаційно-методичний (конкретизує форми, методи та засоби навчання з урахуванням визначених організаційно-педагогічних умов) та діагностико-результативний (визначає критерії, показники та рівні оцінювання ефективності).

4. Упроваджено елементи методики використання ЦТ для формування навичок з ІБ здобувачів ФПО. Практична реалізація методики здійснена через розробку та апробацію плану-конспекту заняття на тему «Захист персональних даних у цифровому середовищі», яке інтегрує обидві організаційно-педагогічні умови.

5. Експериментально перевірено методику використання ЦТ для формування навичок з ІБ здобувачів ФПО. Визначено чотири критерії оцінювання сформованості навичок: інформаційно-теоретичний, операційно-практичний, ціннісно-мотиваційний та оцінювально-аналітичний, для кожного з яких розроблено відповідні показники та діагностичний інструментарій. Педагогічний експеримент, проведений на базі ВСП «Гірничо-електромеханічний фаховий коледж» Криворізького національного університету за участю 25 здобувачів, підтвердив ефективність впроваджених організаційно-педагогічних умов. В ЕГ відбулися статистично значущі позитивні зміни за всіма критеріями. У КГ статистично значущих змін не виявлено.

Результати дослідження підтверджують висунуту гіпотезу про те, що використання ЦТ для формування навичок з ІБ здобувачів ФПО є ефективним за умови реалізації мобільного навчання та впровадження технології гейміфікації. Розроблена методика може бути рекомендована для впровадження у практику роботи закладів ФПО.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Биков В. Ю. Навчальне середовище сучасних педагогічних систем. *Професійна освіта: педагогіка і психологія. Україно-польський журнал.* Видання IV. Ченстохова: Видавництво Вищої педагогічної школи у Ченстохові, 2004. С. 59–80.

2. Бондар В. І. Дидактика: підручник для студ. вищих пед. навч. закл. Київ: Либідь, 2005. 264 с.

3. Бондаренко В. Мобільні застосунки як інструмент самоосвіти в середовищі покоління Z. *Український журнал з бібліотекознавства та інформаційних наук*. 2018. №. 1. С. 86–98.

4. Вінс В., Кудирко Л. Ринок освітніх мобільних додатків в умовах цифрової трансформації освіти. *Universum*. 2025. №. 20. С. 111–116.

5. Гедзик А. Формування компетентностей з інформаційної безпеки під час підготовки майбутніх педагогів професійного навчання. *Молодь і ринок*. 2024. № 1(221). С. 173–177.

6. Гейміфікація як один із трендів сучасної освіти / Н. Мошкова та ін. *Молодь і ринок*. 2024. № 4/224. С. 82–87.

7. Гончаренко С. У. Український педагогічний словник. Київ: Либідь, 1997. 376 с.

8. Горбатюк Р., Тулашвілі Ю. Мобільне навчання як нова технологія вищої освіти. *Науковий вісник Ужгородського національного університету. Серія: Педагогіка. Соціальна робота*. 2013. №. 27. С. 31–34.

9. Грушева А. А., Філіппова Л. Л. Мобільне навчання: за і проти. *Професійна освіта: проблеми і перспективи*. 2015. №. 8. С. 100–106.

10. Дей Г. А. Кібербезпека в українських закладах освіти: основні проблеми та шляхи розв’язання. *Таврійський науковий вісник. Серія: Публічне*

управління та адміністрування. 2025. Вип. 2. С. 35–43. DOI: https://doi.org/10.32782/tnv-pub.2025.2.5.

11. Дичківська І. М. Інноваційні педагогічні технології: підручник. 2-е вид., доп. Київ: Академвидав, 2012. 352 с.

12. Дія.Освіта. Національна онлайн-платформа з цифрової грамотності. URL: https://osvita.diia.gov.ua/ (дата звернення: 15.12.2024).

13. Дубинський В. О. Формування готовності майбутніх учителів інформатики до розвитку навичок цифрової безпеки учнів на засадах інформаційного підходу: дисертація на здобуття наукового ступеня доктора філософії: 015 Професійна освіта (цифрові технології) (01 Освіта) / Сумський державний педагогічний університет імені А. С. Макаренка. Суми, 2025. 238 с.

14. Задоріна О. М., Громик А. П., Бондар С. А. Використання чат-ботів зі штучним інтелектом для покращення комунікації та підтримки здобувачів освіти в мобільних застосунках для дистанційного навчання. *Педагогічна Академія: наукові записки*. 2025. №. 17. С. 28–34.

15. Закон України «Про освіту»: № 2145-VIII від 05.09.2017 / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2145-19 (дата звернення: 18.06.2025).

16. Закон України «Про фахову передвищу освіту»: № 2745-VIII від 06.06.2019 / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2745-19 (дата звернення: 18.06.2025).

17. Ігнатенко В. О., Мирошніченко Ю. Б. Інформаційна безпека в сучасному цифровому освітньому середовищі. *Педагогічні науки*. 2025. Вип. 160. С. 44–49.

18. Інформаційна безпека в освітніх інформаційних системах в умовах цифрової трансформації та євроінтеграції: аспекти захисту персональних даних / А. О. Литвинчук, Г. М. Терещенко, А. В. Кир'янов, Ю. М. Криворучко, Я. Д. Сологуб. *Освітня аналітика України*. 2025. № 2(34). С. 48–65. DOI:

10.32987/2617-8532-2025-2-48-65.

19. Інформаційна безпека: навчальний посібник / Ю. Я. Бобало та ін.; за заг. ред. Ю. Я. Бобала та І. В. Горбатого. Львів: Видавництво Львівської політехніки, 2019. 580 с.

20. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. Київ: Видавництво Ліра-К, 2021. 412 с.

21. Карлінська Я. В. Гейміфікація як невідємний чинник підвищення якості освіти. *Модернізація змісту професійної освіти – умова підготовки компетентного фахівця нової формації*. 2017. С. 260–264.

22. Касьянов Д. В. Гейміфікація в сучасних українських дослідженнях. *Наукові записки Малої академії наук України*. 2024. №. 2. С. 30.

23. Краснопольський В. Е., Поліщук О. А., Демченко О. М. Інтеграція мобільних додатків у освітній процес: аналіз ефективності та можливостей для здобувачів освіти. *Академічні візії*. 2024. №. 32. С. 44–53.

24. Литвинова С. Г. Мікронавчання ІК-технологій педагогів в умовах онлайнового марафону як парадигма цифрової трансформації освіти. *Вісник Національної академії педагогічних наук України*. 2021. Т. 3. №. 1. С. 1–6.

25. Лозова В. І., Троцко Г. В. Теоретичні основи виховання і навчання: навч. посіб. Харків: ОВС, 2002. 400 с.

26. Мартинова Р. Ю. Теорія і практика педагогічного моделювання: монографія. Одеса: Освіта України, 2022. 243 с.

27. Модель інформаційно-аналітичної підтримки педагогічних досліджень на основі електронних систем відкритого доступу / О. М. Спірін, А. В. Яцишин, С. М. Іванова, Л. А. Лупаренко. *Інформаційні технології і засоби навчання*. 2016. Т. 52. № 2. С. 134–154.

28. Мозгаллі О. П., Рибалко Я. В., Синицький Р. К. Інформаційна безпека у цифровій освіті в Україні. *Моделювання та інформаційні системи в економіці*:

збірник наукових праць. 2019. № 98. С. 157–167. DOI: 10.33111/mise.98.16.

29. Муковіз О., Красюк Л. Педагогічні умови формування інформаційно-цифрової компетентності в молодших школярів на уроках інформатики. *Збірник наукових праць Уманського державного педагогічного університету*. 2023. Вип. 1. С. 17–26.

30. Педагогічна освіта в Україні: теорія і практика: словник / М. П. Вовк, Ю. В. Грищенко, С. О. Соломаха, Н. О. Філіпчук, С. В. Ходаківська. Київ, 2021. 312 с.

31. Переяславська С., Смагіна О. Гейміфікація як сучасний напрям вітчизняної освіти. *Відкрите освітнє е-середовище сучасного університету*. 2019. С. 250–260.

32. Пометун О. І., Пироженко Л. В. Сучасний урок. Інтерактивні технології навчання: наук.-метод. посібн. Київ: Видавництво А.С.К., 2004. 192 с.

33. Про.Безпеку: безпечна освітня екосистема громади: навчально-методичний посібник / за заг. ред. Н. Софій, А. Аносової. Київ: Центр інноваційної освіти «Про.Світ», 2023. 518 с.

34. Про захист персональних даних: Закон України від 1 червня 2010 р. № 2297-VI (з останніми змінами, внесеними згідно із Законом № 3585-IX від 14.06.2025). URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 29.08.2025).

35. Радомський І. П. Інформаційна безпека та конфіденційність у змішаному навчанні в умовах війни. *Актуальні проблеми в системі освіти: загальноосвітній заклад середньої освіти – доуніверситетська підготовка – заклад вищої освіти*. 2024. № 1(4). С. 394–404. DOI: 10.18372/2786-5487.1.18755.

36. Рамка цифрової компетентності для громадян України (DigComp UA for Citizens). URL: https://thedigital.gov.ua/storage/uploads/files/news_post/2021/3/mintsifra-oprilyudnyue-ramku-tsifrovoi-kompetentnosti-dlya-gromadyan/%D0%9E%D0%A0%20%D0%A6%D0%9A.pdf (дата звернення:

18.10.2025).

37. Рацул А. Б., Довга Т. Я., Рацул А. В. Педагогіка: інформативний виклад: навч. посіб. 2-е вид., перероб. і доп. Київ: КНТ, 2015. 320 с.

38. Рашевська Н. В., Ткачук В. В. Технології мобільного навчання. *Педагогіка вищої та середньої школи*. 2012. Т. 1. №. 35. С. 295–301.

39. Семеріков С. О., Стрюк М. І., Моісеєнко Н. В. Мобільне навчання: історико-технологічний вимір. *Теорія і практика організації самостійної роботи студентів вищих навчальних закладів: монографія*. 2012. С. 188–242.

40. Сисоєва С. О. Основи педагогічної творчості: підручник. Київ: Міленіум, 2006. 344 с.

41. Спірін О. М. Критерії і показники якості інформаційно-комунікаційних технологій навчання. *Інформаційні технології і засоби навчання*. 2013. № 1 (33). С. 45–58.

42. Стандартизація професійної освіти: теорія і практика: монографія / А. А. Каленський та ін. Київ: НАПН України, 2018. 312 с.

43. Стеченко Д. М., Чмир О. С. Методологія наукових досліджень: підручник. 2 вид., перероб. і доп. Київ: Знання, 2007. 317 с.

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

45. Толочко С. В. Теоретико-методологічний аналіз гейміфікації як сучасного освітнього феномена. *Перспективи та інновації науки* (Серія «Педагогіка», Серія «Психологія», Серія «Медицина»). 2023. Т. 1. №. 19. С. 369–383.

46. Цісарук І. В., Цісарук В. Ю., Омельчук О. В. Безпека учасників освітнього процесу як елемент безпечного освітнього середовища. *Науковий вісник Кременецької обласної гуманітарно-педагогічної академії ім. Тараса Шевченка. Серія: Педагогічні науки*. 2023. Вип. 16. С. 51–57. DOI:

https://doi.org/10.32782/2410-2075-2023-16.7.

47. Чичкань І. В., Спасітєлєва С. О., Жданова Ю. Д. Освітнє середовище для формування культури безпекового поводження у кіберпросторі при підготовці фахівців з економіки та управління. *Інформаційні технології і засоби навчання*. 2021. Том 84, № 4. С. 354–375.

48. Чорномидз А. В. Інформаційна безпека викладачів вищих навчальних закладів в умовах воєнного стану: виклики та практичні рекомендації. *Медична освіта*. 2025. № 2. С. 67–71. DOI: https://doi.org/10.11603/m.2414-5998.2025.2.15490.

49. Чубукова О. Ю., Пономаренко І. В. Інформаційна безпека у навчальних закладах України. *Вісник Київського національного університету технологій та дизайну. Серія: Економічні науки. Спецвипуск: Ефективність організаційно-економічного механізму інноваційного розвитку вищої освіти України*: матеріали VIII Міжнародної науково-практичної конференції (5 жовтня 2018 р., м. Київ). 2018. С. 388–395.

50. CISCO Networking Academy. Cybersecurity Essentials Course. URL: https://www.netacad.com/courses/cybersecurity/cybersecurity-essentials (дата звернення: 15.12.2024).

51. Coursera. Cybersecurity Specializations. URL: https://www.coursera.org/browse/information-technology/security (дата звернення: 15.12.2024).

52. Crompton H., Burke D. The use of mobile learning in higher education: A systematic review. *Computers & Education*. 2018. Vol. 123. P. 53–64.

53. Cybersecurity and innovative digital educational environment / O. Burov, O. Butnik-Siversky, O. Orliuk, K. Horska. *Information Technologies and Learning Tools*. 2020. Vol. 80(6). P. 414–430. DOI: https://doi.org/10.33407/itlt.v80i6.4159.

54. Dubinsky V. Information approach in education and its use in the training of computer science teachers to form students' digital safety skills. *Академічні візії*.

2024. № 38. DOI: https://doi.org/10.5281/zenodo.14594487.

55. Kuforiji J. The Importance of Integrating Security Education into University Curricula and Professional Certifications. *International Journal of Technology, Management and Humanities.* 2025. Vol. 11(3). DOI: https://doi.org/10.21590/ijtmh.11.0301.

56. Microsoft Learn. Security fundamentals. URL: https://learn.microsoft.com/en-us/training/paths/describe-concepts-of-security-compliance-identity/ (дата звернення: 15.12.2024).

57. Organization of Training with the Use of Digital Technologies for Ensuring Cybersecurity in the Educational Space / L. Arsenovych, O. Nikolaievsky, O. Skliarenko, L. Lytvynenko, I. Kydriavskyi. *WSEAS Transactions on Computer Research.* 2024. Vol. 12. P. 524–536. DOI: https://doi.org/10.37394/232018.2024.12.51.

58. Prometheus. Інформаційна безпека. URL: https://prometheus.org.ua/ (дата звернення: 15.12.2024).

59. Shihua L., Zhanxiang Y., Hao Z. Study on the Training Mode of Network Security Practical Talent in Vocational and Technical College Based on Gamification and Leveling up. *The Journal of Education, Culture, and Society*. 2020. Vol. 5(4). DOI: 10.11648/J.IJECS.20200504.13.

60. UNESCO. Policy Guidelines for Mobile Learning. Paris: UNESCO, 2013. 41 p.

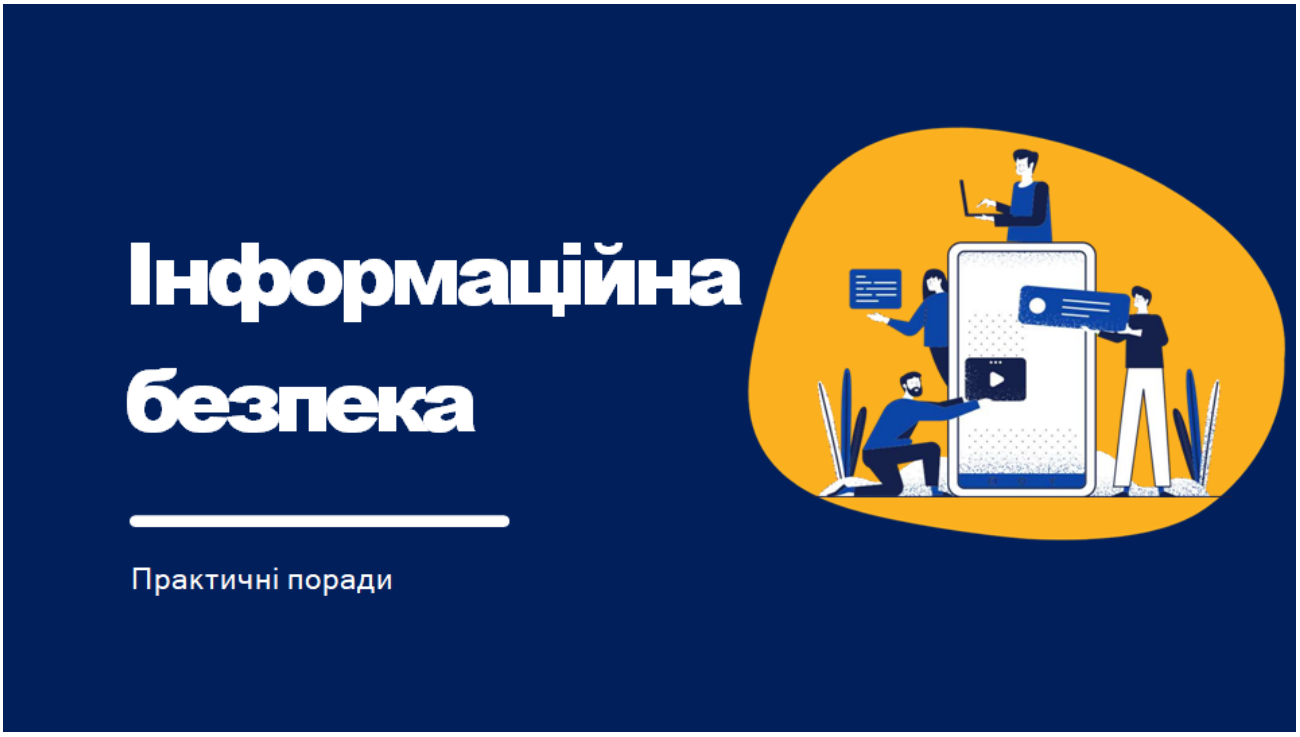
61. Vladut G., Hamburg I. Improving Cybersecurity Awareness and Basics in Vocational Education and Training. *Annals of Review and Research*. 2023. Vol. 9(5). DOI: 10.19080/arr.2023.09.555774.

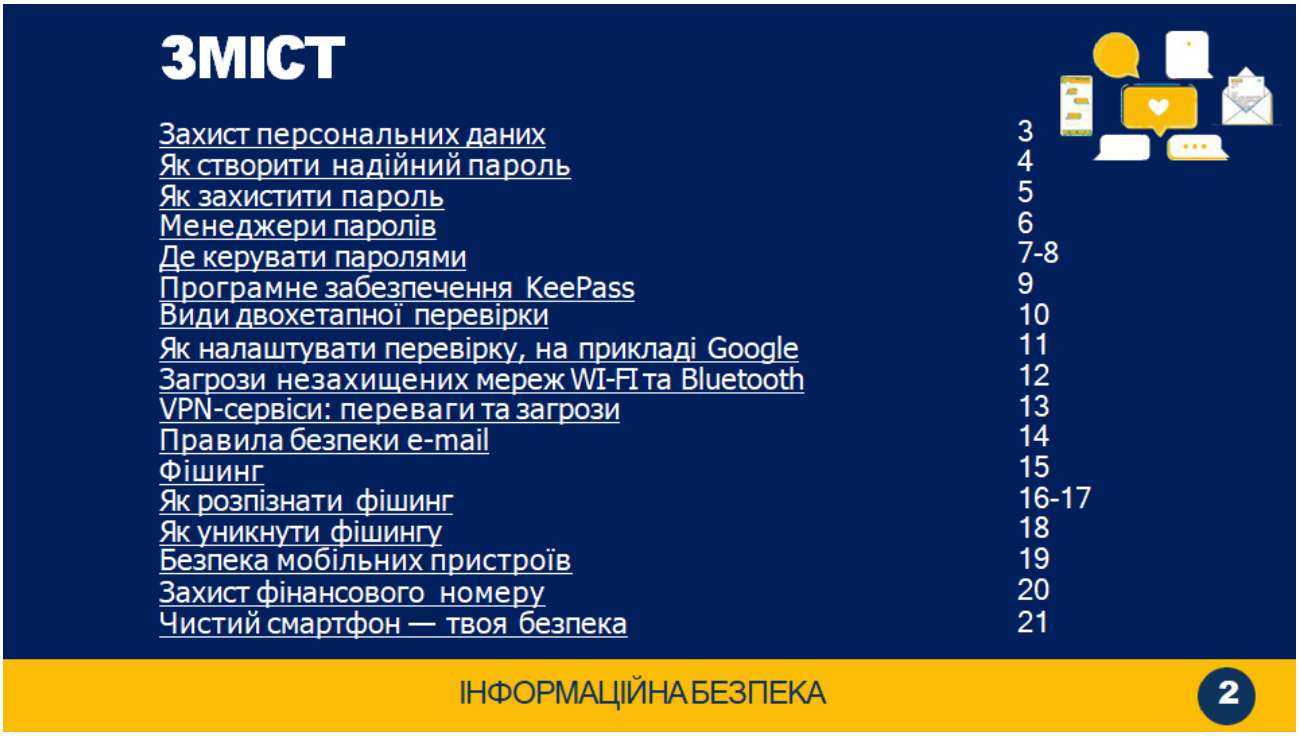
62. Yang X., Yang C. Transformation and Upgrading of Cyber Security Major in Vocational Colleges in the Context of New Quality Productive Forces. *Frontiers in artificial intelligence and applications*. 2024. DOI: 10.3233/faia241376.

ДОДАТКИ

Додаток А

ПРЕЗЕНТАЦІЯ «ІНФОРМАЦІЙНА БЕЗПЕКА: ПРАКТИЧНІ ПОРАДИ»





ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

Створюй складні паролі

Налаштуй двофакторну аутентифікацію

Дотримуйся приватності

Відмовся від геолокації

Захищай свої пристрої

ІНФОРМАЦІЙНА БЕЗПЕКА 3

ЯК СТВОРИТИ НАДІЙНИЙ ПАРОЛЬ

- складай пароль мінімум з 8–14 символів
- застосовуй прописні та строчні букви
- додавай цифри та символи
- застосовуй різні букви та цифри
- використовуй парольну фразу

Ненадійні паролі зазвичай стають причиною хакерських атак.

ІНФОРМАЦІЙНА БЕЗПЕКА 4

ЯК ЗАХИСТИТИ ПАРОЛЬ

- не використовуй особисті дані для пароля
- раз на квартал змінюй паролі
- використовуй менеджери паролів
- застосовуй двоетапну перевірку
- не забувай виходити зі своїх акаунтів
- не залишай паролі в пам'яті браузера

МЕНЕДЖЕРИ ПАРОЛІВ

програмне забезпечення з розширеним функціоналом, що полегшує доступ до паролів, ліцензійних ключів, Wi-Fi для доступу до вебсайтів та додатків.
Менеджери паролів дозволяють створювати зашифровані архіви, щоб надійно зберігати файли та завантажувати їх у хмарне сховище.

ДЕ КЕРУВАТИ ПАРОЛЯМИ

у налаштуваннях *веб-браузерів*, якщо використовуєш особистий пристрій, наприклад:


Google Chrome


Safari


Internet Explorer


Mozilla Firefox

Вбудовані менеджери паролів у браузерах не настільки потужні та корисні, як сторонні менеджери паролів.

ДЕ КЕРУВАТИ ПАРОЛЯМИ

у сторонніх менеджерах паролів, які генерують надійні паролі, запам'ятовують їх, і дозволяють входити до вебсайтів, наприклад:


LastPass


KeePass


1Password

На думку фахівців, *використання сторонніх менеджерів паролів є найбільш безпечним*.

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ KEEPASS

безкоштовне програмне забезпечення з відкритим кодом, має основні можливості менеджерів паролів для персонального використання.

Як легко користуватися KeePass

ВИДИ ДВОХЕТАПНОЇ ПЕРЕВІРКИ

- *резервний метод* входу до акаунта за допомогою SMS або виклику на телефон
- через програмні застосунки аутентифікатори *Google Authenticator, Authy (iOS, Android), Microsoft Authenticator*
- *апаратний ключ безпеки*

ЯК НАЛАШТУВАТИ ДВОХЕТАПНУ ПЕРЕВІРКУ, НА ПРИКЛАДІ GOOGLE?

- перейди у свій *обліковий запис Google*
- натисни *Управління акаунтом Google*
- на лівій панелі навігації натисни *Безпека*
- у блоці *Вхід в акаунт Google* натисни *Двохетапна аутентифікація* ✓ та *Почати*
- виконай подальші вказівки на екрані

ІНФОРМАЦІЙНА БЕЗПЕКА 11

ЗАГРОЗИ НЕЗАХИЩЕНИХ МЕРЕЖ WI-FI ТА BLUETOOTH

- не підключайся автоматично до мереж Wi-Fi
- використовуй лише захищені паролем мережі
- вимикай Wi-Fi, Bluetooth, коли їх не використовуєш
- відкривай сайти лише з шифруванням HTTPS
- використовуй перевірені VPN-з'єднання

ІНФОРМАЦІЙНА БЕЗПЕКА 12

VPN-СЕРВІСИ: ПЕРЕВАГИ ТА ЗАГРОЗИ

- ✓ анонімність IP-адреси в мережі
- ✓ маскування місцезнаходження
- ✓ відсутність географічних обмежень в доступі
- ✓ захищене з'єднання з віддаленою мережею

- ✓ VPN-сервіси збирають дані про користувачів
- ✓ є ризик передачі даних до мереж загального користування
- ✓ небезпека несанкціонованого використання мікрофону та камери пристроїв

ПРАВИЛА БЕЗПЕКИ E-MAIL

- не зазначай свою адресу на сумнівних сайтах
- не розпаковуй вкладені в листи підозрілі архіви
- видаляй листи від підозрілих адресатів
- не відповідай на спам листи, налаштуй фільтр
- використовуй безпечне шифрування HTTPS
- не користуйся чужими пристроями для входу на електронну пошту

ФІШИНГ

електронні листи від шахраїв, метою яких є отримання доступу до особистої та конфіденційної інформації.

Сьогодні фішинг маскується під офіційні сервіси підтримки, листи відписки від розсилок, сайти або оголошення.

ЯК РОЗПІЗНАТИ ФІШИНГ

підозрілі посилання	https://bit.ly/security-check-gmail
помилки в тексті	Заради вашої безпеки та приватносьті, вам треба
неперсональні звернення	Шановний користувач!

ЯК РОЗПІЗНАТИ ФІШИНГ

заклик до термінової дії

фейкова назва відправника

фейкова назва відправника

У вас лише 24 години, інакше акаунт буде видалено назавжди!

Служба підтримки
<no-reply@accounts.google.com>

ТЕРМІНОВО актуалізувати персональні дані...

https://bit.ly/3dfqXJY

17

ЯК УНИКНУТИ ФІШИНГУ

- перевіряй підозрілі URL-адреси та посилань
- будь уважним надаючи особисті дані
- остерігайся шахрайських листів
- перевіряй файли, перш ніж завантажувати
- остерігайся осіб, що видають себе за інших
- повідомляй про фішинг організації, від імені якої написали шахраї

http://surl.li/ckpv

БЕЗПЕКА МОБІЛЬНИХ ПРИСТРОЇВ

- використовуй біометрію
- не залишай смартфон без нагляду
- не переходь за посиланнями з SMS
- завантажуй застосунки з офіційних маркетів додатків
- уважно читай користувацькі угоди застосунків
- регулярно оновлюй програмне забезпечення

19

ЗАХИСТ ФІНАНСОВОГО НОМЕРА

- зареєструй SIM-картку у мобільного оператора, тоді сторонні не зможуть перевипустити твій номер телефону
- встанови власний ПІН-код на SIM-картку
- у разі втрати смартфону заблокуй SIM-картку

20

ЧИСТИЙ СМАРТФОН — ТВОЯ БЕЗПЕКА

вимкни мобільний пристрій

протри поверхню:

- сухою тканиною з мікроволокна
- тканиною змоченою у мильному розчині
- серветками для дезінфекції

не вмикай телефон поки повністю не висохне

ІНФОРМАЦІЙНА БЕЗПЕКА У ТВОЇХ РУКАХ!

Додаток Б

ТЕСТ «ДІАГНОСТИКА РІВНЯ СФОРМОВАНОСТІ НАВИЧОК З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

Інструкція для здобувачів

Тест містить 40 завдань різних типів. Уважно читайте кожне завдання та інструкції до нього.

Завдання 1–20: оберіть ОДНУ правильну відповідь (1 бал за кожне).

Завдання 21–30: оберіть ВСІ правильні відповіді (2 бали за кожне).

Завдання 31–35: встановіть відповідність (2 бали за кожне).

Завдання 36–40: дайте розгорнуту письмову відповідь (3 бали за кожне).

Час виконання: 45 хвилин.

Максимальна кількість балів: 60.

Блок 1. Поняття та сутність інформаційної безпеки (завдання 1–7)

Завдання 1. Інформаційна безпека – це:

А) Захист комп’ютера від вірусів.

Б) Стан захищеності інформаційного середовища суспільства, який забезпечує формування, використання та розвиток інформаційного середовища в інтересах громадян, організацій та держави.

В) Використання антивірусного програмного забезпечення.

Г) Створення резервних копій даних.

Завдання 2. Основною метою інформаційної безпеки є забезпечення:

А) Швидкості обробки інформації.

Б) Конфіденційності, цілісності та доступності інформації.

В) Зручності використання інформаційних систем.

Г) Економії ресурсів при роботі з інформацією.

Завдання 3. Конфіденційність інформації означає:

А) Можливість відновлення інформації після збою.

Б) Захист від несанкціонованого доступу та розголошення.

В) Швидкість передачі даних.

Г) Резервне копіювання даних.

Завдання 4. Цілісність даних – це властивість, що забезпечує:

А) Доступність інформації в будь-який час.

Б) Захист від несанкціонованої модифікації або знищення.

В) Швидку обробку великих обсягів даних.

Г) Можливість роботи з даними без підключення до Інтернету.

Завдання 5. Доступність інформації означає:

А) Відкритість всієї інформації для всіх користувачів.

Б) Можливість авторизованих користувачів отримати доступ до

інформації та ресурсів у потрібний час.

В) Безкоштовність доступу до інформації.

Г) Можливість завантажувати будь-які файли з Інтернету.

Завдання 6. До основних принципів інформаційної безпеки НЕ належить:

А) Принцип мінімізації привілеїв.

Б) Принцип ешелонованого захисту.

В) Принцип максимального доступу для зручності.

Г) Принцип розподілу обов’язків.

Завдання 7. Персональні дані – це:

А) Будь-яка інформація в комп’ютері.

Б) Відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

В) Логіни та паролі користувачів.

Г) Інформація про компанії та організації

Блок 2. Види цифрових загроз (завдання 8-15)

Завдання 8. Фішинг – це:

А) Вид комп'ютерного вірусу.

Б) Вид шахрайства, спрямований на отримання конфіденційної інформації шляхом маскування під довірені джерела.

В) Програма для захисту від вірусів.

Г) Метод шифрування даних.

Завдання 9. Шкідливе програмне забезпечення, що самостійно поширюється через мережу без участі користувача, називається:

А) Вірус.

Б) Троянська програма.

В) Черв’як.

Г) Шпигунське ПЗ.

Завдання 10. Ransomware (програма-вимагач) – це шкідливе ПЗ, яке:

А) Видаляє всі файли на комп’ютері.

Б) Шифрує дані користувача та вимагає викуп за їх розшифрування.

В) Показує рекламу на екрані.

Г) Сповільнює роботу комп’ютера.

Завдання 11. DDoS-атака спрямована на:

А) Крадіжку паролів користувачів.

Б) Порушення доступності веб-сайту або сервісу шляхом перевантаження запитами.

В) Встановлення шпигунського ПЗ.

Г) Шифрування даних на жорсткому диску.

Завдання 12. Соціальна інженерія – це:

А) Метод створення соціальних мереж.

Б) Психологічне маніпулювання людьми з метою виконання дій або розголошення конфіденційної інформації.

В) Технологія захисту даних.

Г) Спосіб налаштування приватності в соціальних мережах.

Завдання 13. Кібербулінг – це:

А) Вид комп’ютерного вірусу.

Б) Цькування, залякування, приниження особи за допомогою цифрових технологій.

В) Метод захисту від хакерських атак.

Г) Програма для блокування небажаного контенту.

Завдання 14. Спам – це:

А) Корисна розсилка від інтернет-магазинів.

Б) Масова розсилка небажаних повідомлень рекламного або шахрайського характеру.

В) Вірус, що блокує роботу електронної пошти.

Г) Програма для фільтрації електронних листів.

Завдання 15. Троянська програма – це шкідливе ПЗ, яке:

А) Самостійно поширюється через мережу.

Б) Маскується під легітимне ПЗ та виконує приховані шкідливі дії.

В) Шифрує файли користувача.

Г) Показує рекламні банери.

Блок 3. Методи та засоби захисту інформації (завдання 16-23)

Завдання 16. Антивірусне програмне забезпечення призначене для:

А) Прискорення роботи комп’ютера.

Б) Виявлення, блокування та видалення шкідливого ПЗ.

В) Очищення жорсткого диска від непотрібних файлів.

Г) Шифрування персональних даних.

Завдання 17. Брандмауер (firewall) виконує функцію:

А) Резервного копіювання даних.

Б) Контролю та фільтрації мережевого трафіку між мережами різного рівня довіри.

В) Шифрування файлів.

Г) Перевірки орфографії в документах.

Завдання 18. VPN (Virtual Private Network) використовується для:

А) Прискорення інтернет-з’єднання.

Б) Створення захищеного з’єднання через незахищену мережу.

В) Блокування реклами.

Г) Встановлення програмного забезпечення.

Завдання 19. HTTPS у порівнянні з HTTP забезпечує:

А) Швидшу завантаження сторінок.

Б) Шифрування даних між браузером та веб-сервером.

В) Безкоштовний доступ до контенту.

Г) Автоматичне резервне копіювання.

Завдання 20. Двофакторна автентифікація (2FA) – це:

А) Використання двох різних антивірусів.

Б) Метод підтвердження особи користувача за допомогою двох різних компонентів.

В) Створення двох різних паролів.

Г) Реєстрація в двох соціальних мережах.

Блок 4. Правила безпечної поведінки в Інтернеті (завдання 21-30)
Оберіть УСІ правильні відповіді

Завдання 21. До ознак фішингового електронного листа належать:

А) Терміновість та вимога негайних дій.

Б) Орфографічні та граматичні помилки.

В) Підозріла адреса відправника.

Г) Посилання на офіційний сайт організації.

Д) Запит конфіденційної інформації (паролів, номерів карток).

Е) Персоналізоване звернення на ім’я.

Завдання 22. Безпечна поведінка в публічних Wi-Fi мережах передбачає:

А) Уникнення введення паролів та особистої інформації.

Б) Використання VPN.

В) Відключення автоматичного підключення до відкритих мереж.

Г) Здійснення онлайн-платежів через безпечні сервіси.

Д) Перевірку наявності HTTPS на сайтах.

Е) Передачу конфіденційних документів електронною поштою.

Завдання 23. При налаштуванні приватності в соціальних мережах рекомендується:

А) Обмежити видимість особистої інформації (дати народження, номера телефону, адреси).

Б) Зробити профіль повністю відкритим для всіх.

В) Контролювати, хто може бачити ваші публікації.

Г) Приймати всі запити на дружбу без винятку.

Д) Регулярно переглядати та оновлювати налаштування приватності.

Е) Публікувати інформацію про поточне місцезнаходження в реальному часі.

Завдання 24. Безпечне використання онлайн-банкінгу включає:

А) Регулярну зміну паролів.

Б) Використання загальнодоступних комп’ютерів для входу.

В) Активацію повідомлень про транзакції.

Г) Збереження паролів у браузері на чужих пристроях.

Д) Перевірку URL-адреси банківського сайту.

Е) Використання двофакторної автентифікації.

Завдання 25. До правил безпечного завантаження файлів з Інтернету належать:

А) Завантаження лише з офіційних та перевірених джерел.

Б) Перевірка завантажених файлів антивірусом перед відкриттям.

В) Завантаження будь-яких файлів з торрент-трекерів.

Г) Увага до розширень файлів (.exe, .bat можуть бути небезпечними).

Д) Читання відгуків та рейтингів перед завантаженням.

Е) Відкриття всіх вкладень з електронних листів без перевірки.

Завдання 26. При створенні облікових записів на веб-сайтах рекомендується:

А) Використовувати різні паролі для різних сайтів.

Б) Використовувати один простий пароль для всіх сайтів.

В) Надавати мінімум необхідної особистої інформації.

Г) Вказувати справжню дату народження на всіх сайтах.

Д) Перевіряти політику конфіденційності сайту.

Е) Використовувати тимчасову електронну адресу для реєстрації на ненадійних сайтах.

Завдання 27. Безпечне спілкування в месенджерах та чатах передбачає:

А) Обережність при спілкуванні з незнайомцями.

Б) Використання наскрізного шифрування (end-to-end encryption).

В) Повідомлення особистої інформації всім контактам.

Г) Ігнорування підозрілих посилань у повідомленнях.

Д) Використання функції самознищення повідомлень для конфіденційної інформації.

Е) Пересилання повідомлень від незнайомців без перевірки.

Завдання 28. До ознак надійного інтернет-магазину належать:

А) Наявність HTTPS з'єднання та дійсного SSL-сертифіката.

Б) Відсутність контактної інформації.

В) Позитивні відгуки покупців на незалежних платформах.

Г) Наявність юридичної інформації про компанію.

Д) Пропозиції, які здаються занадто вигідними.

Е) Різноманітні способи оплати, включаючи безпечні платіжні системи.

Завдання 29. При роботі з хмарними сховищами для забезпечення безпеки слід:

А) Використовувати надійні паролі та двофакторну автентифікацію.

Б) Зберігати найбільш конфіденційні дані без шифрування.

В) Регулярно перевіряти активні сеанси та підключені пристрої.

Г) Використовувати шифрування файлів перед завантаженням.

Д) Надавати доступ до файлів усім бажаючим.

Е) Налаштовувати контроль доступу для спільних папок.

Завдання 30. Безпечне використання мобільних пристроїв включає:

А) Встановлення застосунків лише з офіційних магазинів (App Store, Google Play).

Б) Відключення блокування екрану для зручності.

В) Регулярне оновлення операційної системи та застосунків.

Г) Перевірку дозволів, які запитують застосунки.

Д) Увімкнення функції дистанційного стирання даних.

Е) Збереження паролів від банківських карток у нотатках на телефоні.

Блок 5. Правові аспекти інформаційної безпеки (завдання 31-35)
Встановіть відповідність

Завдання 31. Встановіть відповідність між термінами та їх визначеннями:

Термін	Визначення
1. GDPR	А) Закон України про захист персональних даних
2. Кіберзлочин	Б) Загальний регламент про захист персональних даних ЄС
3. Закон України «Про захист персональних даних»	В) Злочин, скоєний за допомогою комп’ютерних технологій
4. Інтелектуальна власність	Г) Права на результати інтелектуальної діяльності

Завдання 32. Встановіть відповідність між видами правопорушень та їх описом:

Правопорушення	Опис
1. Несанкціонований доступ до інформації	А) Створення і поширення комп'ютерних вірусів
2. Піратство програмного забезпечення	Б) Незаконне втручання в роботу комп’ютерних систем
3. Розповсюдження шкідливого ПЗ	В) Незаконне копіювання та використання ПЗ
4. Кібершахрайство	Г) Обман з метою отримання матеріальної вигоди через Інтернет

Завдання 33. Встановіть відповідність між правами суб’єкта персональних даних та їх змістом:

Право	Зміст
1. Право на доступ	А) Вимагати видалення своїх персональних даних
2. Право на виправлення	Б) Знати, які персональні дані про нього

	обробляються
3. Право на забуття	В) Вимагати виправлення неточних персональних даних
4. Право на обмеження обробки	Г) Вимагати припинення обробки персональних даних у певних випадках

Завдання 34. Встановіть відповідність між типами ліцензій програмного забезпечення та їх характеристиками:

Тип ліцензії	Характеристика
1. Proprietary (власницьке ПЗ)	А) Вільне використання, модифікація та поширення
2. Open Source (відкрите ПЗ)	Б) Платне ПЗ з обмеженими правами використання
3. Freeware	В) Безкоштовне, але з обмеженнями на комерційне використання
4. Shareware	Г) Безкоштовна пробна версія з обмеженнями

Завдання 35. Встановіть відповідність між органами та їх функціями у сфері кібербезпеки:

Орган	Функція
1. Кіберполіція України	А) Захист критичної інфраструктури від кіберзагроз
2. Уповноважений з прав людини	Б) Розслідування кіберзлочинів
3. Державна служба спеціального зв’язку та захисту інформації	В) Захист прав громадян, включаючи право на приватність
4. Служба безпеки України	Г) Контррозвідувальний захист у кіберпросторі

Блок 6. Принципи створення та управління паролями (завдання 36-40)
Дайте розгорнуту письмову відповідь

Завдання 36. Опишіть основні характеристики надійного пароля. Наведіть приклад шаблону для створення надійного пароля (без вказування конкретного пароля, який ви використовуєте).

Відповідь:_____

Завдання 37. Поясніть, чому небезпечно використовувати один і той самий пароль для різних онлайн-сервісів. Наведіть сценарій можливих наслідків такої практики.

Відповідь:_____

Завдання 38. Що таке менеджер паролів і які переваги надає його використання? Назвіть принаймні три переваги.

Відповідь:_____

Завдання 39. Опишіть, як працює двофакторна автентифікація (2FA) та чому вона є ефективнішою за звичайний пароль. Наведіть приклади різних типів другого фактора автентифікації.

Відповідь:_____

Завдання 40. Ваш друг звернувся до вас із проханням допомогти, оскільки він підозрює, що хтось отримав несанкціонований доступ до його облікового запису електронної пошти. Опишіть покроковий алгоритм дій, які йому слід виконати для відновлення безпеки свого облікового запису.

Відповідь:_____

Критерії оцінювання відкритих завдань (36-40)

3 бали – повна, вичерпна відповідь, що демонструє глибоке розуміння питання, містить конкретні приклади та деталі.

2 бали – правильна відповідь, але неповна або без конкретних прикладів.

1 бал – частково правильна відповідь, фрагментарні знання.

0 балів – неправильна відповідь або відсутність відповіді.

Шкала оцінювання

Високий рівень: 48–60 балів (80–100%).

Середній рівень: 30–47 балів (50–79%).

Початковий рівень: 0–29 балів (0–49%).

Додаток В

КОМПЛЕКС ПРАКТИЧНИХ СИТУАЦІЙНИХ ЗАВДАНЬ

Загальна інформація

Кількість завдань: 7.
Час виконання: 90 хвилин.
Максимальна кількість балів: 35 (по 5 балів за кожне завдання).
Форма виконання: індивідуальна робота в комп'ютерному класі.

Шкала оцінювання

Високий рівень: 28–35 балів (80–100%).
Середній рівень: 18–27 балів (51–79%).
Початковий рівень: 0–17 балів (0–50%).

Завдання 1. Встановлення та налаштування антивірусного ПЗ

Час виконання: 12 хвилин

Опис ситуації

На віртуальній машині з операційною системою Windows 10 відсутнє антивірусне програмне забезпечення. Вам необхідно забезпечити базовий захист системи.

Завдання

1. Завантажте та встановіть безкоштовну версію антивірусного ПЗ (Avast Free Antivirus або AVG AntiVirus Free) з офіційного сайту.
2. Виконайте початкове налаштування програми:
– увімкніть захист у реальному часі;
– активуйте захист веб–браузера;
– налаштуйте розклад автоматичного сканування (щоденно о 22:00).
3. Виконайте повне сканування системи.
4. Інтерпретуйте результати сканування та зафіксуйте їх у звіті.

Що потрібно здати

1. Скриншот встановленого та налаштованого антивірусу.
2. Скриншот результатів сканування.
3. Короткий звіт (3–5 речень) з інтерпретацією результатів: чи виявлено загрози, які файли викликають підозру, які дії рекомендуються.

Критерії оцінювання:

– 5 балів: ПЗ встановлено правильно, всі налаштування виконано відповідно до вимог, сканування проведено, результати проінтерпретовано коректно та детально;
– 4 бали: ПЗ встановлено, налаштування виконано з незначними недоліками (наприклад, пропущено один параметр), результати інтерпретовано загалом правильно;

– 3 бали: ПЗ встановлено, але налаштування виконано частково або з помилками, інтерпретація результатів поверхнева;

– 2 бали: ПЗ встановлено, але налаштування не виконано або виконано неправильно, результати не проінтерпретовано;

– 1 бал: завдання не виконано або виконано з критичними помилками (ПЗ завантажено з неофіційного джерела).

Завдання 2. Налаштування приватності в соціальній мережі

Час виконання: 15 хвилин

Опис ситуації

Ви створили новий обліковий запис у Facebook і хочете захистити свою особисту інформацію від несанкціонованого доступу.

Завдання

Налаштуйте параметри приватності відповідно до наступних вимог.

1. Видимість профілю:

– зробіть профіль видимим лише для друзів;

– обмежте можливість пошуку профілю за електронною адресою та номером телефону.

2. Особиста інформація:

– приховайте дату народження (видимість: «Тільки я»);

– приховайте номер телефону та електронну адресу;

– приховайте місце проживання від незнайомців.

3. Публікації:

– налаштуйте видимість майбутніх публікацій: «Друзі»;

– обмежте видимість старих публікацій: «Друзі»;

– налаштуйте перевірку публікацій, в яких вас позначають.

4. Друзі:

– приховайте список друзів (видимість: «Тільки я»);

– налаштуйте, хто може надсилати запити на дружбу: «Друзі друзів».

5. Додаткові налаштування:

– увімкніть двофакторну автентифікацію;

– перегляньте активні сеанси та завершіть підозрілі.

Що потрібно здати:

– скриншоти кожного розділу налаштувань приватності з виконаними змінами (мінімум 5 скріншотів);

– скриншот налаштованої двофакторної автентифікації;

– короткий опис (2–3 речення), чому ці налаштування важливі для захисту приватності.

Критерії оцінювання:

– 5 балів: всі вимоги виконано правильно, двофакторна автентифікація налаштована, наданий змістовний опис важливості налаштувань;

– 4 бали: більшість вимог виконано, пропущено 1–2 налаштування,

двофакторна автентифікація налаштована;

– 3 бали: виконано близько половини вимог, є суттєві прогалини в налаштуваннях;

– 2 бали: виконано лише базові налаштування, відсутня двофакторна автентифікація;

– 1 бал: завдання практично не виконано або виконано з критичними помилками.

Завдання 3. Створення надійних паролів та налаштування менеджера паролів

Час виконання: 12 хвилин

Опис ситуації

Вам потрібно створити облікові записи для п’яти різних сервісів і забезпечити надійний захист доступу до них.

Завдання

Частина 1. Створення паролів.

Створіть п’ять надійних паролів для наступних сервісів:

1. Електронна пошта (Gmail).
2. Онлайн-банкінг.
3. Соціальна мережа (Facebook).
4. Хмарне сховище (Google Drive).
5. Інтернет–магазин (Amazon).

Вимоги до кожного пароля:

– мінімум 12 символів;

– містить великі та малі літери;

– містить цифри;

– містить спеціальні символи (!@#$%^&);

– не містить словникових слів;

– усі паролі різні.

Частина 2. Налаштування менеджера паролів.

1. Встановіть один з менеджерів паролів (LastPass, Bitwarden або KeePass).
2. Створіть майстер-пароль за всіма вимогами надійності.
3. Збережіть всі п’ять створених паролів у менеджері з відповідними назвами сервісів та логінами.
4. Встановіть розширення для браузера (якщо доступне).

Що потрібно здати

– документ Word або текстовий файл з п’ятьма створеними паролями та поясненням структури кожного (наприклад: «Пароль 1 складається з 14 символів: перші 4 – випадкові літери, наступні 4 – цифри, останні 6 – комбінація літер і символів»);

– скриншот встановленого менеджера паролів із збереженими обліковими записами (паролі мають бути приховані);

– скриншот розширення браузера для менеджера паролів.

Критерії оцінювання:

– 5 балів: всі 5 паролів відповідають вимогам надійності, менеджер паролів встановлено та налаштовано правильно, всі паролі збережено, надано змістовне пояснення структури;

– 4 бали: 4–5 паролів відповідають вимогам, менеджер налаштовано з незначними недоліками;

– 3 бали: 3 паролі відповідають вимогам або всі паролі частково відповідають вимогам, менеджер встановлено, але налаштовано не повністю;

– 2 бали: створено паролі низької надійності, менеджер встановлено, але не налаштовано;

– 1 бал: паролі не відповідають вимогам безпеки або завдання не виконано.

Завдання 4. Розпізнавання фішингових повідомлень

Час виконання: 15 хвилин

Опис ситуації

Ви отримали 10 електронних листів. Серед них є як легітимні, так і фішингові повідомлення.

Набір електронних листів

Лист 1

Від: support@paypa1-security.com
Тема: Термінове підтвердження облікового запису
Шановний користувач!
Ми виявили підозрілу активність у вашому обліковому записі PayPal.
Для підтвердження вашої особи перейдіть за посиланням:
http://paypal-verify.tk/confirm
У вас є 24 години, інакше обліковий запис буде заблоковано.
З повагою, Команда PayPal

Лист 2

Від: noreply@google.com
Тема: Новий вхід у ваш обліковий запис Google
Шановний Іване Петренко,
Ми виявили новий вхід у ваш обліковий запис Google.
Пристрій: iPhone 12
Місцезнаходження: Київ, Україна
Час: 15 листопада 2024, 14:23
Якщо це були не ви, захистіть свій обліковий запис:
https://myaccount.google.com/security

Лист 3

Від: no-reply@bank-alert.net
Тема: УВАГА!!! Ваша картка заблокована!!!

ШАНОВНИЙ КЛІЄНТ!

Ваша банківська картка 4532 ЗАБЛОКОВАНА через підозрілу операцію.

Для розблокування ТЕРМНОВО введіть дані картки за посиланням:

http://bit.ly/bank-unlock-2024

ПІН-код, CVV, термін дії.

УВАГА! У ВАС Є ЛИШЕ 3 ГОДИНИ!!!

Лист 4

Від: invoice@amazon.com

Тема: Ваше замовлення #125-7834562-9834561

Доброго дня,

Дякуємо за замовлення на Amazon.com

Товар: Ноутбук Lenovo IdeaPad 3

Ціна: $549.99

Адреса доставки: вул. Хрещатик, 22, Київ

Очікувана дата доставки: 20–22 листопада 2024

Переглянути деталі: https://www.amazon.com/orders

Лист 5

Від: winner@lottery-international.biz

Тема: Вітаємо! Ви виграли $500,000!

ВІТАЄМО!!!

Ваша електронна адреса виграла $500,000 у міжнародній лотереї!

Для отримання виграшу надішліть:

- Копію паспорта
- Номер банківського рахунку
- Адресу проживання
- $250 для оплати податків

Відповідайте протягом 48 годин!

Лист 6

Від: security@facebook.com

Тема: Підтвердьте свою особу

Привіт,

Ми отримали запит на скидання пароля для вашого облікового запису Facebook.

Якщо це були ви, використайте цей код: 847392

Якщо ви не робили такого запиту, проігноруйте це повідомлення.

Посилання дійсне протягом 24 годин.

Лист 7

Від: ceo@yourcompany-hr.com

Тема: Терміново! Оновлення кадрової політики

Шановні співробітники!

Через зміни в трудовому законодавстві просимо всіх ТЕРМІНОВО заповнити

форму з особистими даними: http://tinyurl.com/hr-update-form

Вкажіть ПІБ, ІПН, номер паспорта, банківські реквізити.
УВАГА! Хто не заповнить до кінця дня – буде звільнений!
Генеральний директор

Лист 8

Від: notifications@linkedin.com
Тема: Запрошення від Марії Коваленко
Привіт,
Марія Коваленко запрошує вас приєднатися до її мережі на LinkedIn.
Марія Коваленко
Менеджер проектів у TechCorp
Прийняти запрошення: https://www.linkedin.com/invitations

Лист 9

Від: support@microsoft-security-team.net
Тема: Вірус виявлено на вашому комп’ютері
УВАГА! ЗАГРОЗА БЕЗПЕЦІ!
Наша система виявила 12 вірусів на вашому комп’ютері Windows.
Завантажте наш інструмент очищення ЗАРАЗ:
http://windows-fix.download/cleaner.exe
Якщо не очистите протягом години, ваші файли будуть зашифровані!
Microsoft Security Team

Лист 10

Від: no-reply@netflix.com
Тема: Проблема з оплатою вашої підписки
Привіт,
На жаль, нам не вдалося обробити ваш останній платіж.
Щоб продовжити користуватися Netflix, оновіть платіжну інформацію
у налаштуваннях облікового запису протягом 3 днів.
Оновити платіжну інформацію: https://www.netflix.com/YourAccount

Завдання

1. Проаналізуйте кожен з 10 листів.
2. Визначте, які листи є фішинговими (мінімум 4, максимум 6).
3. Для кожного фішингового листа вкажіть конкретні ознаки фішингу (мінімум 3 ознаки для кожного листа).
4. Поясніть, які дії слід вжити при отриманні фішингових листів.

Що потрібно здати

Таблицю у форматі:

№ листа	Фішинг (Так/Ні)	Ознаки фішингу (якщо так)
1	Так	1. Підозріла адреса відправника (paypa1 замість paypal)

№ листа	Фішинг (Так/Ні)	Ознаки фішингу (якщо так)
		2. Доменне ім’я .tk (безкоштовний домен) 3. Вимога термінових дій та залякування 4. Запит переходу за підозрілим посиланням
2	Ні	Легітимний лист від Google
...	...	...

Критерії оцінювання:

– 5 балів: правильно ідентифіковано всі або майже всі фішингові листи (5–6 з 6), для кожного вказано мінімум 3 конкретні ознаки, надано чіткі рекомендації щодо дій;

– 4 бали: правильно ідентифіковано 4 фішингові листи, ознаки вказано, але не для всіх або не всі ознаки конкретні;

– 3 бали: правильно ідентифіковано 3 фішингові листи, ознаки вказано поверхнево;

– 2 бали: ідентифіковано 1–2 фішингові листи або багато помилкових спрацьовувань;

– 1 бал: завдання не виконано або виконано з грубими помилками.

Підказка: Фішингові листи: 1, 3, 5, 7, 9 (разом 5 листів).

Завдання 5. Оцінка надійності інтернет-магазину

Час виконання: 12 хвилин

Опис ситуації

Ви плануєте придбати ноутбук в інтернеті та знайшли три варіанти інтернет-магазинів. Потрібно оцінити їх надійність перед здійсненням покупки.

Інтернет–магазини для аналізу

Магазин А:

URL: https://laptop–sale–ukraine.com.ua
Ціна ноутбука: На 40% нижче ринкової
SSL–сертифікат: Присутній (замок у браузері)
Контактна інформація: Тільки форма зворотного зв’язку
Відгуки: На сайті тільки 5-зіркові відгуки
Способи оплати: Тільки передоплата на картку ФОП
Про компанію: Немає інформації про юридичну особу

Магазин Б:

URL: http://super–tehnics.online
Ціна ноутбука: На 50% нижче ринкової
SSL–сертифікат: Відсутній
Контактна інформація: Телефон, адреса офісу
Відгуки: Немає відгуків на незалежних платформах
Способи оплати: Готівка при отриманні або передоплата

Про компанію: Є реквізити, але при перевірці в реєстрі – не знайдено

Магазин В:

URL: https://www.rozetka.com.ua

Ціна ноутбука: Ринкова ціна

SSL–сертифікат: Присутній, валідний

Контактна інформація: Телефони, email, адреси магазинів, онлайн–чат

Відгуки: Тисячі відгуків на Google, Trustpilot (середня оцінка 4.2/5)

Способи оплати: Картою онлайн, готівка, безготівковий розрахунок, оплата частинами

Про компанію: Повна юридична інформація, ліцензії, сертифікати

Завдання

1. Перевірте наявність SSL–сертифікату:

– перейдіть на кожен сайт (або проаналізуйте надану інформацію);

– перевірте наявність та валідність SSL–сертифікату;

– поясніть, чому це важливо.

2. Оцініть надійність кожного магазину за наступними критеріями (кожен критерій оцініть від 1 до 5):

– наявність HTTPS та валідного SSL–сертифікату;

– адекватність цін (чи не занадто низькі);

– повнота контактної інформації;

– наявність та якість відгуків на незалежних платформах;

– різноманітність та безпечність способів оплати;

– наявність юридичної інформації про компанію.

3. Визначте найбезпечніший магазин та обґрунтуйте свій вибір.

4. Оберіть безпечний спосіб оплати для обраного магазину та поясніть чому.

Що потрібно здати

Звіт, який містить:

1. Таблицю оцінки кожного магазину за всіма критеріями.

2. Загальну оцінку надійності кожного магазину (сума балів).

3. Обґрунтований висновок: який магазин обрати і чому.

4. Рекомендований спосіб оплати.

5. Перелік «червоних прапорців» (ознак ненадійності), виявлених у магазинах А та Б.

Критерії оцінювання:

– 5 балів: проведено детальний аналіз усіх трьох магазинів за всіма критеріями, правильно визначено найбезпечніший варіант, обґрунтовано вибір способу оплати, виявлено всі основні «червоні прапорці»;

– 4 бали: проведено аналіз за більшістю критеріїв, висновки загалом правильні, виявлено більшість ознак ненадійності;

– 3 бали: проведено поверхневий аналіз, висновки частково обґрунтовані,

виявлено деякі ознаки ненадійності;

– 2 бали: аналіз фрагментарний, висновки недостатньо обґрунтовані;

– 1 бал: завдання не виконано або виконано з грубими помилками (наприклад, обрано ненадійний магазин).

Завдання 6. Створення резервних копій

Час виконання: 12 хвилин

Опис ситуації

У вас є набір важливих файлів (документи курсової роботи, фотографії, важливі таблиці), які необхідно захистити від можливої втрати.

Завдання

Частина 1. Підготовка файлів.

Створіть тестовий набір файлів для резервного копіювання:

– 1 документ Word (будь–який текст, мінімум 1 сторінка);

– 1 таблиця Excel (будь–які дані);

– 2–3 зображення (можна завантажити будь–які);

– 1 текстовий файл зі списком паролів (вигаданих).

Створіть папку «Важливі документи» та помістіть туди всі ці файли.

Частина 2. Локальне резервне копіювання.

1. Підключіть USB–флешку або створіть окрему папку на диску D:\ (імітація зовнішнього носія).

2. Створіть повну копію папки «Важливі документи».

3. Перевірте цілісність копії (переконайтеся, що всі файли скопійовано правильно).

Частина 3. Резервне копіювання у хмарне сховище.

1. Виберіть одне з хмарних сховищ (Google Drive, OneDrive, Dropbox).

2. Створіть окрему папку «Backup_[дата]» у хмарному сховищі.

3. Завантажте всі файли з папки «Важливі документи» у хмару.

4. Переконайтеся, що файли синхронізовано.

Частина 4. Налаштування автоматичного резервного копіювання.

Налаштуйте автоматичне резервне копіювання одним зі способів:

– варіант А: налаштуйте автоматичну синхронізацію папки з хмарним сховищем;

– варіант Б: створіть bat–файл або використайте вбудовані засоби Windows для планування автоматичного копіювання.

Частина 5. Тестування відновлення.

1. Видаліть один файл з оригінальної папки.

2. Відновіть його з резервної копії (локальної або хмарної).

3. Задокументуйте процес відновлення.

Що потрібно здати

1. Скриншот оригінальної папки «Важливі документи» з усіма файлами.

2. Скриншот локальної резервної копії.

3. Скриншот файлів у хмарному сховищі.

4. Скриншот налаштувань автоматичного резервного копіювання.

5. Короткий опис (5–7 речень):

– чому важливо мати як локальні, так і хмарні резервні копії;

– як часто слід створювати резервні копії;

– які файли потребують найчастішого резервного копіювання;

Критерії оцінювання

– 5 балів: створено як локальну, так і хмарну резервну копію, налаштовано автоматичне копіювання, успішно протестовано відновлення, наданий змістовний опис;

– 4 бали: створено обидва типи копій, автоматичне копіювання налаштовано частково, відновлення протестовано;

– 3 бали: створено лише один тип резервної копії (локальну або хмарну), автоматичне копіювання не налаштовано або налаштовано неправильно;

– 2 бали: резервна копія створена, але з помилками, відновлення не протестовано;

– 1 бал: завдання не виконано або виконано з критичними помилками.

Завдання 7. Реагування на інцидент інформаційної безпеки

Час виконання: 12 хвилин

Опис ситуації

Під час роботи ви помітили наступні підозрілі ознаки на комп’ютері:

– комп’ютер працює повільніше, ніж зазвичай;

– антивірус видав кілька попереджень, які ви випадково закрили;

– відкриваються вікна браузера з рекламою, яких ви не запускали;

– при перевірці диспетчера завдань виявлено незнайомий процес svchost32.exe, який споживає багато ресурсів;

– з’явився новий значок на робочому столі для програми, яку ви не встановлювали.

Завдання:

Розробіть та виконайте план дій для вирішення цього інциденту безпеки.

Покроковий план повинен включати:

1. Негайні дії (перші 5 хвилин): що треба зробити одразу для запобігання поширенню загрози?

2. Діагностика (наступні 10–15 хвилин):

– як визначити, чи дійсно комп’ютер заражений?

– які інструменти використати для діагностики?

3. Ізоляція (якщо підтверджено зараження): які кроки вжити, щоб запобігти поширенню на інші пристрої?

4. Очищення системи:

– якими методами видалити шкідливе ПЗ?

– які програми або інструменти використати?

5. Відновлення:

– як переконатися, що система очищена?

– які налаштування потрібно змінити після очищення?

6. Профілактика: що зробити, щоб запобігти подібним інцидентам у майбутньому?

Практична частина

1. Виконайте діагностику системи:

– перевірте диспетчер завдань на наявність підозрілих процесів;

– проведіть швидке сканування антивірусом;

– перевірте список встановлених програм.

2. Задокументуйте виявлені проблеми.

3. Виконайте базові кроки з очищення (якщо виявлено загрози).

Що потрібно здати

1. Детальний план дій (покроковий алгоритм) у форматі документа Word або PDF.

2. Скриншоти:

– диспетчера задач з процесами;

– результатів сканування антивірусом;

– списку встановлених програм;

– виконаних дій з очищення (якщо можливо).

3. Звіт про інцидент (10–15 речень), який включає:

– опис виявлених проблем;

– виконані дії;

– результат (чи вдалося усунути проблему);

– рекомендації щодо профілактики.

Критерії оцінювання:

– 5 балів: розроблено повний та логічний план дій з усіма етапами, виконано діагностику, задокументовано всі кроки, звіт детальний та професійний, надано конкретні рекомендації щодо профілактики;

– 4 бали: план містить більшість необхідних етапів, діагностика виконана, документація достатня, рекомендації загальні;

– 3 бали: план неповний або частково логічний, діагностика виконана поверхнево, документація мінімальна;

– 2 бали: план фрагментарний, діагностика виконана з помилками або не виконана, відсутні важливі кроки;

– 1 бал: завдання не виконано або виконано з критичними помилками (наприклад, рекомендовано дії, які можуть завдати шкоди системі).

Додаток Д

АНКЕТА

Шановний студенте!

Просимо Вас взяти участь у дослідженні, присвяченому вивченню ставлення до питань інформаційної безпеки. Анкета є анонімною, тому просимо відповідати щиро. Ваші відповіді будуть використані виключно в узагальненому вигляді для наукових цілей.

Інструкція: Уважно прочитайте кожне твердження та оцініть ступінь своєї згоди з ним, обравши один варіант відповіді:

5 – повністю згоден/згодна
4 – скоріше згоден/згодна
3 – важко відповісти
2 – скоріше не згоден/не згодна
1 – повністю не згоден/не згодна

Немає правильних чи неправильних відповідей. Важлива саме Ваша особиста думка.

Час заповнення: 15-20 хвилин

Блок 1. Усвідомлення особистої відповідальності за безпеку інформації

№	Твердження	1	2	3	4	5
1	Я відчуваю особисту відповідальність за захист своїх персональних даних в Інтернеті	☐	☐	☐	☐	☐
2	Я розумію, що моя необережність в онлайн-середовищі може завдати шкоди не лише мені, а й іншим людям	☐	☐	☐	☐	☐
3	Захист інформації – це передусім моя власна відповідальність, а не обов'язок адміністраторів систем	☐	☐	☐	☐	☐
4	Я усвідомлюю наслідки можливої втрати або компрометації моїх персональних даних	☐	☐	☐	☐	☐

Блок 2. Розуміння цінності конфіденційності та приватності

№	Твердження	1	2	3	4	5
5	Конфіденційність моїх особистих даних є важливою цінністю для мене	☐	☐	☐	☐	☐
6	Я вважаю, що маю право контролювати, хто і яку інформацію про мене може отримати	☐	☐	☐	☐	☐
7	Приватність в онлайн-середовищі так само важлива, як і в реальному житті	☐	☐	☐	☐	☐
8	Захист моєї особистої інформації від несанкціонованого доступу є пріоритетом для мене	☐	☐	☐	☐	☐

Блок 3. Інтерес до вивчення питань інформаційної безпеки

№	Твердження	1	2	3	4	5
9	Мені цікаво дізнаватися про нові загрози в цифровому середовищі та способи захисту від них	☐	☐	☐	☐	☐
10	Я слідкую за новинами у сфері інформаційної безпеки	☐	☐	☐	☐	☐
11	Я готовий/готова витрачати час на вивчення інструментів та методів захисту інформації	☐	☐	☐	☐	☐
12	*Питання інформаційної безпеки надто складні та нудні для мене*	☐	☐	☐	☐	☐

Блок 4. Готовність витрачати зусилля на забезпечення безпеки

№	Твердження	1	2	3	4	5
13	Я готовий/готова витратити додаткові 5-10 хвилин на налаштування параметрів приватності нового додатку	☐	☐	☐	☐	☐
14	Я вважаю виправданим використання складних паролів, навіть якщо їх важче запам'ятати	☐	☐	☐	☐	☐
15	Створення резервних копій важливих файлів варте витрачених зусиль	☐	☐	☐	☐	☐
16	*Я не бачу сенсу витрачати час на налаштування параметрів приватності*	☐	☐	☐	☐	☐

Блок 5. Дотримання етичних норм

№	Твердження	1	2	3	4	5
17	Я ніколи не використовую чужі паролі або облікові записи без дозволу	☐	☐	☐	☐	☐
18	Я поважаю приватність інших людей в онлайн-середовищі	☐	☐	☐	☐	☐
19	Я вважаю неприйнятним поширення особистої інформації інших людей без їхньої згоди	☐	☐	☐	☐	☐
20	*Якщо я знаю чужий пароль, я можу ним скористатися, якщо це мені потрібно*	☐	☐	☐	☐	☐

Блок 6. Бажання допомагати іншим

№	Твердження	1	2	3	4	5
21	Я готовий/готова допомогти друзям чи родичам у питаннях інформаційної безпеки	☐	☐	☐	☐	☐
22	Я вважаю важливим поширювати знання про безпечну поведінку в Інтернеті серед свого оточення	☐	☐	☐	☐	☐
23	*Інформаційна безпека – це особиста справа кожного, тому я не втручаюся в цифрову поведінку інших*	☐	☐	☐	☐	☐
24	*Мені байдуже, якщо мої знайомі не дотримуються правил безпеки в Інтернеті*	☐	☐	☐	☐	☐

Примітка: *Курсивом виділені твердження з негативним формулюванням*

Ключ для обробки результатів

Твердження з прямим формулюванням (оцінюються за стандартною шкалою 1-5): пункти: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 13, 14, 15, 17, 18, 19, 21, 22

Твердження з негативним формулюванням (оцінки інвертуються: 5→1, 4→2, 3→3, 2→4, 1→5): пункти: 12, 16, 20, 23, 24

Інверсія балів для негативних тверджень

Отримана оцінка	Бал для підрахунку
5 (повністю згоден)	1
4 (скоріше згоден)	2
3 (важко відповісти)	3
2 (скоріше не згоден)	4
1 (повністю не згоден)	5

Підрахунок результатів

Крок 1: Підрахуйте суму балів за твердження 1-11, 13-15, 17-19, 21-22 (пряме формулювання).

Крок 2: Підрахуйте інвертовані бали за твердження 12, 16, 20, 23, 24 (негативне формулювання).

Крок 3: Підсумуйте результати кроків 1 і 2.

Загальна сума балів: _____ (максимум 120 балів).

Інтерпретація результатів

Загальний рівень сформованості ціннісно-мотиваційного компоненту:

Високий рівень: 96-120 балів (80-100%)

Здобувач демонструє високу мотивацію до забезпечення інформаційної безпеки

– Усвідомлює особисту відповідальність за захист інформації.
– Високо цінує приватність та конфіденційність.
– Виявляє активний інтерес до вивчення питань інформаційної безпеки.
– Готовий витрачати час та зусилля на забезпечення безпеки.
– Дотримується етичних норм у цифровому середовищі.
– Прагне допомагати іншим у питаннях інформаційної безпеки.

Середній рівень: 60-95 балів (50-79%)

– Здобувач загалом розуміє важливість інформаційної безпеки.
– Частково усвідомлює особисту відповідальність.
– Цінує приватність, але не завжди готовий витрачати зусилля на її захист.
– Інтерес до вивчення питань інформаційної безпеки є епізодичним.
– Готовність дотримуватися правил безпеки залежить від ситуації.
– Загалом дотримується етичних норм.
– Не завжди виявляє бажання допомагати іншим.

Початковий рівень: 0-59 балів (0-49%)

– Здобувач не усвідомлює важливості інформаційної безпеки.
– Не відчуває особистої відповідальності за захист інформації.
– Не цінує приватність та конфіденційність або вважає їх другорядними.
– Відсутній інтерес до вивчення питань інформаційної безпеки.
– Не готовий витрачати час та зусилля на забезпечення безпеки.
– Можливі прояви неетичної поведінки в цифровому середовищі.
– Не виявляє бажання допомагати іншим або поширювати знання про безпеку.

Детальний аналіз за блоками

Для більш детального аналізу можна підрахувати суми балів окремо за кожним блоком:

Блок	Пункти	Максимум балів	Отримано балів %
1. Усвідомлення відповідальності	1-4	20	
2. Цінність конфіденційності	5-8	20	
3. Інтерес до вивчення	9-12*	20	
4. Готовність витрачати зусилля	13-16*	20	
5. Дотримання етичних норм	17-20*	20	
6. Бажання допомагати	21-24*	20	
ЗАГАЛОМ	**1-24**	**120**	

*Блоки містять твердження з негативним формулюванням, що вимагають інверсії балів

Бланк відповідей для здобувача

ПІБ (за бажанням, анкета анонімна): _____
Група: _____ Дата заповнення: _____
Стать: ☐ Чоловіча ☐ Жіноча **Вік: _____**

№	Оцінка	№	Оцінка	№	Оцінка	№	Оцінка
1		7		13		19	
2		8		14		20	
3		9		15		21	
4		10		16		22	
5		11		17		23	
6		12		18		24	

Загальна сума балів: _____ / 120
Рівень: ☐ Високий ☐ Середній ☐ Початковий

Дякуємо за участь у дослідженні!
Ваші відповіді допоможуть удосконалити методику формування навичок інформаційної безпеки у здобувачів фахової передвищої освіти.

Додаток Е

КОМПЛЕКС КЕЙСІВ

Загальна інформація:
Кількість кейсів: 5
Час виконання: 60 хвилин
Максимальна кількість балів: 100 (по 20 балів за кожен кейс)
Форма виконання: індивідуальна письмова робота

Шкала оцінювання:
Високий рівень: 80-100 балів (80-100%)
Середній рівень: 50-79 балів (50-79%)
Початковий рівень: 0-49 балів (0-49%)

Кейс 1. Підозрілий застосунок

Рекомендований час: 10 хвилин

Опис ситуації

Ви отримали повідомлення у месенджері Telegram від свого друга Олексія, з яким навчаєтесь разом:

Олексій, 14:23
Привіт! 👋
Дивись який крутий застосунок знайшов!
Показує, хто переглядає твій профіль в Instagram! 😎
Я вже встановив, реально працює!
Ось посилання: insta-view-tracker.apk
Швидше качай, поки безкоштовно! 🔥

Ви знаєте, що офіційно Instagram не надає такої функції. Застосунок потрібно завантажити з посилання (не з Google Play або App Store). При спробі відкрити посилання ваш антивірус видає попередження про потенційну загрозу, але дозволяє продовжити завантаження на власний ризик.

Ваш друг наполегливо радить спробувати і каже, що у нього все працює нормально. Крім того, ви бачите, що декілька інших ваших знайомих також поширюють це посилання у своїх сторіс.

Завдання

1. Проаналізуйте ситуацію (0-5 балів):

– Які елементи цієї ситуації викликають підозру?

– Чому офіційно Instagram не надає функції перегляду відвідувачів профілю?

– Які мотиви можуть бути у розробників цього застосунку?

– Як могло статися, що ваш друг і знайомі поширюють це посилання?

2. Оцініть можливі ризики (0-5 балів):

– Які конкретні загрози може нести встановлення цього застосунку?

– Які дані можуть бути скомпрометовані?

– Які можливі наслідки для вашого пристрою та облікових записів?

– Чи може це вплинути на інших користувачів (друзів, контакти)?

3. Визначте ознаки потенційної загрози та прийміть рішення (0-5 балів):

– Перелічіть всі ознаки, що свідчать про можливу загрозу

– Яке рішення ви приймете: встановлювати чи не встановлювати застосунок?

– Що ви відповісте другу?

– Які дії потрібно порадити вжити тим, хто вже встановив застосунок?

4. Спрогнозуйте можливі наслідки різних варіантів дій (0-5 балів):

– Що може статися, якщо ви встановите застосунок?

– Що може статися, якщо ви проігноруєте повідомлення?

– Що може статися, якщо ви попередите інших користувачів про небезпеку?

– Які довгострокові наслідки поширення такого застосунку?

Бланк для відповіді

1. Аналіз ситуації

_____
_____
_____
_____

2. Оцінка ризиків

_____
_____
_____
_____

3. Ознаки загрози та рішення

_____
_____
_____
_____

4. Прогноз наслідків

_____
_____
_____
_____

Кейс 2. Публічний Wi-Fi

Рекомендований час: 12 хвилин

Опис ситуації

Ви сидите в кав’ярні біля коледжу і готуєтесь до заліку. Раптом вам приходить повідомлення про необхідність терміново оплатити онлайн-курс, якщо ви хочете зберегти знижку 50%. До кінця акції залишилося 2 години. Вартість курсу зі знижкою – 500 грн, без знижки – 1000 грн. Цей курс дуже важливий для вашого фахового розвитку, і ви довго відкладали гроші на його придбання.

Поточна ситуація:

– Ви підключені до відкритої мережі Wi-Fi кав’ярні CoffeeTime_Free.

– Мобільний інтернет на вашому телефоні закінчився (пакет вичерпано).

– Вдома є стабільний захищений Wi-Fi, але дорога додому займе 1,5 години.

– У вас є банківська картка та можливість оплатити курс прямо зараз.

– На курсі потрібно створити обліковий запис з електронною поштою та паролем.

Додаткова інформація:

– У кав’ярні крім вас сидить ще близько 15 осіб з ноутбуками.

– Офіційне підтвердження акції прийшло на вашу електронну пошту від платформи Udemy.

– У вас встановлено базовий антивірус, але немає VPN.

– Ви використовуєте цю ж електронну пошту та паролі для кількох інших сервісів.

Завдання

1. Проаналізуйте ситуацію (0-5 балів):

– Які фактори створюють ризик у даній ситуації?

– Які фактори створюють тиск для прийняття швидкого рішення?

– Наскільки критичною є терміновість оплати?

– Які технічні можливості у вас є для забезпечення безпеки?

2. Оцініть ризики використання публічної мережі (0-5 балів):

– Які конкретні загрози пов'язані з використанням відкритого Wi-Fi?

– Які дані можуть бути перехоплені під час транзакції?

– Який рівень ризику для ваших фінансових даних?

– Які додаткові облікові записи можуть опинитися під загрозою?

3. Запропонуйте та обґрунтуйте оптимальне рішення (0-5 балів):

– Які альтернативні варіанти дій у вас є?

– Оцініть кожен варіант з точки зору безпеки та зручності

– Яке рішення ви приймете і чому?

– Які додаткові заходи безпеки можна застосувати?

– Як збалансувати економію 500 грн і потенційні ризики?

4. Спрогнозуйте наслідки (0-5 балів):

– Що може статися в найгіршому сценарії при оплаті через публічний Wi-Fi?

– Які наслідки відмови від термінової оплати?

– Які довгострокові наслідки компрометації ваших облікових даних?

– Які превентивні заходи варто вжити після прийняття рішення?

Бланк для відповіді

1. Аналіз ситуації

_____

_____

_____

_____

2. Оцінка ризиків

_____

_____

_____

_____

3. Варіанти рішень та обґрунтування

_____

_____

_____

_____

_____

4. Прогноз наслідків

_____

_____

_____

_____

Кейс 3. Повідомлення від банку

Рекомендований час: 12 хвилин

Опис ситуації

О 22:35 вам на електронну пошту приходить наступний лист:

Від: security-alert@privatbank-secure.com

Тема: ⚠ ТЕРМІНОВЕ ПОВІДОМЛЕННЯ: Підозріла активність на вашому рахунку

Шановний клієнте ПриватБанку!

Наша система безпеки виявила ПІДОЗРІЛУ АКТИВНІСТЬ на вашому рахунку:

Спроба входу з IP-адреси: 185.34.xxx.xxx (Польща)
Спроба переказу коштів на суму 15,000 грн
Зміна контактного номера телефону

ДЛЯ ВАШОЇ БЕЗПЕКИ МИ ТИМЧАСОВО ЗАБЛОКУВАЛИ ВАШ РАХУНОК!

Для підтвердження, що це не ви здійснювали ці операції, та розблокування рахунку, будь ласка, ТЕРМІНОВО пройдіть верифікацію особи:

[ПІДТВЕРДИТИ ОСОБУ](http://privatbank-verification.web.app/confirm)

У ВАС Є ЛИШЕ 3 ГОДИНИ, інакше рахунок буде остаточно заблоковано і для розблокування потрібно буде особисто відвідувати відділення банку.

Для верифікації вам знадобиться:
- Номер картки
- CVV-код
- SMS-код підтвердження
- Дата народження

З повагою,
Служба безпеки ПриватБанк
Цілодобова підтримка: 3700

✉@ Не відповідайте на цей email, він генерується автоматично.

Додаткова інформація:

– Ви дійсно є клієнтом ПриватБанку.
– У вас на картці є сума близько 8,000 грн.
– Сьогодні ввечері ви справді здійснювали покупку онлайн.
– Ви не здійснювали жодних спроб входу з-за кордону.
– Ви не змінювали номер телефону.
– Офіційний email ПриватБанку зазвичай виглядає як noreply@privatbank.ua.
– Офіційна підтримка ПриватБанку – 3700 (це правда).

Завдання

1. Критично проаналізуйте повідомлення (0-5 балів):
– Які елементи повідомлення виглядають легітимно?
– Які елементи викликають підозру?
– Проаналізуйте email відправника.
– Проаналізуйте URL посилання (не переходячи за ним).
– Які психологічні прийоми використані для маніпуляції?

2. Виявіть ознаки фішингу або підтвердьте автентичність (0-5 балів):
– Перелічіть усі ознаки фішингу, які ви виявили.
– Які стандартні практики банків порушено в цьому листі?
– Чи може це бути справжнім повідомленням від банку?
– Як банки зазвичай повідомляють про підозрілу активність?
3. Оцініть можливі наслідки різних варіантів дій (0-5 балів):
– Що станеться, якщо ви перейдете за посиланням і введете дані?
– Що станеться, якщо ви проігноруєте повідомлення?
– Які можуть бути фінансові наслідки помилкових дій?
– Які можуть бути наслідки для ваших інших облікових записів?
4. Прийміть виважене рішення (0-5 балів):
– Покроково опишіть, що ви зробите у відповідь на це повідомлення
– Як ви перевірите справжність повідомлення?
– Кому і як ви повідомите про це повідомлення?
– Які превентивні заходи варто вжити на майбутнє?

Бланк для відповіді

1. Аналіз повідомлення

_____
_____
_____
_____
_____

2. Ознаки фішингу/автентичності

_____
_____
_____
_____

3. Оцінка наслідків

_____
_____
_____
_____

4. План дій

_____
_____
_____
_____

Кейс 4. Робочі документи на особистому пристрої

Рекомендований час: 13 хвилин

Опис ситуації

Ви навчаєтесь у коледжі і паралельно працюєте за сумісництвом в ІТ-компанії на посаді молодшого фахівця з технічної підтримки. Робота дистанційна, і ви виконуєте її на своєму особистому ноутбуці вдома.

Робоча інформація на вашому ноутбуці:

– База даних клієнтів компанії (імена, email, номери телефонів, історія звернень) – файл Excel на 500+ записів.

– Документи з паролями доступу до корпоративних систем (Google Docs).

– Конфіденційні технічні інструкції та внутрішні регламенти компанії (PDF-файли).

– Листування з клієнтами в робочій електронній пошті (Gmail).

– Скріншоти екранів клієнтів з технічними проблемами (можуть містити чутливу інформацію).

Домашня ситуація:

– Ноутбуком також користується ваш молодший брат (14 років) для ігор та навчання.

– Іноді батьки просять ноутбук для онлайн-покупок та перегляду фільмів.

– На ноутбуці один обліковий запис Windows без пароля.

– Всі файли зберігаються на робочому столі та в папці «Документи» без шифрування.

– Резервні копії не створюються.

– Антивірус встановлено, але часто вимкнений для кращої продуктивності в іграх.

– Брат іноді встановлює різні програми і ігри, завантажені з торрент-трекерів.

Додаткова інформація:

– У трудовому договорі є пункт про нерозголошення конфіденційної інформації клієнтів.

– За витік даних передбачена дисциплінарна та можлива юридична відповідальність.

– Компанія не надала вам робочий ноутбук, очікуючи, що ви використаєте власний.

– У компанії немає чітких інструкцій щодо захисту інформації на особистих пристроях.

– Ви не повідомляли керівництво, що ноутбуком користуються інші члени родини.

Завдання

1. Проаналізуйте потенційні ризики (0-5 балів):

– Які конкретні загрози існують для конфіденційності даних?

– Які вразливості присутні в поточній ситуації?

– Хто може отримати несанкціонований доступ до інформації?
– Які технічні та організаційні проблеми ви виявили?
2. Оцініть можливі наслідки компрометації інформації (0-5 балів):
– Які наслідки для клієнтів компанії?
– Які наслідки для компанії?
– Які особисті наслідки для вас (юридичні, професійні, фінансові)?
– Які репутаційні ризики?
– Оцініть ймовірність реалізації кожного ризику
3. Розробіть стратегію безпечного зберігання та використання робочих даних (0-5 балів):
– Які технічні заходи захисту необхідно впровадити?
– Як організувати розділення робочого та особистого використання?
– Які організаційні заходи потрібно вжити?
– Як залучити родину до дотримання правил безпеки?
– Що потрібно узгодити з роботодавцем?
4. Спрогнозуйте наслідки впровадження/невпровадження заходів безпеки (0-5 балів):
– Що зміниться після впровадження заходів безпеки?
– Які переваги та незручності створять ці заходи?
– Що може статися, якщо залишити все як є?
– Який реалістичний сценарій інциденту безпеки в поточній ситуації?
– Які довгострокові наслідки для вашої професійної кар'єри?

Бланк для відповіді

1. Аналіз ризиків

_____
_____
_____
_____
_____

2. Оцінка наслідків

_____
_____
_____
_____
_____

3. Стратегія безпечного зберігання

_____
_____
_____
_____
_____
_____

4. Прогноз наслідків

_____
_____
_____
_____
_____

Кейс 5. Інцидент витоку даних

Рекомендований час: 13 хвилин

Опис ситуації

Сьогодні вранці ви побачили у стрічці новин шокуючу інформацію: популярна платформа для онлайн-навчання EduPlatform, якою ви користуєтесь вже 3 роки, зазнала масштабного витоку даних. За попередньою інформацією, хакери отримали доступ до бази даних з 5 мільйонами облікових записів користувачів.

Офіційне повідомлення EduPlatform:

З глибоким жалем повідомляємо про інцидент безпеки, який стався 10 листопада 2024 року. Несанкціонований доступ до нашої бази даних призвів до витоку наступної інформації:

✅ Електронні адреси (100% користувачів)

✅ Хеші паролів (85% користувачів)

✅ Імена та прізвища (100% користувачів)

✅ Номери телефонів (70% користувачів)

✅ Збережені дані банківських карток (25% користувачів, які обрали опцію збереження)

✅ Історія покупок та переглядів курсів

⚠ Паспортні дані студентів, які отримували сертифікати (15% користувачів)

Ми вже повідомили правоохоронні органи та працюємо над розслідуванням. Всім користувачам рекомендуємо змінити паролі.

Ваша ситуація:

– Ви активний користувач платформи з 2023 року.

– У вас 15 придбаних курсів, загальна вартість яких становила близько 8,000 грн.

– Ви обрали опцію «Зберегти картку для швидших покупок».

– Ваша картка все ще активна, на ній зараз 12,000 грн.

– Ви використовуєте той самий пароль на EduPlatform, як і на: Gmail (основна електронна пошта); Facebook; Instagram; Приват24 (онлайн-банкінг); Amazon; Netflix.

– Ви отримували електронні сертифікати з курсів, для чого надавали скан

паспорта.

– Ваш номер телефону зареєстрований у платформі.

– Останній раз заходили на платформу 2 дні тому.

Додаткова інформація з новин:

– Хакери вже виклали частину бази даних на хакерському форумі.

– Зафіксовані випадки шахрайських дзвінків користувачам від імені підтримки платформи.

– Кіберполіція попереджає про можливу хвилю фішингу на адреси скомпрометованих користувачів.

– Юристи прогнозують можливі колективні позови до платформи.

– Деякі банки вже почали превентивно блокувати картки постраждалих користувачів.

Завдання

1. Проаналізуйте масштаб проблеми (0–5 балів):

– Які ваші конкретні дані потрапили в руки зловмисників?

– Наскільки критичною є ситуація саме для вас?

– Які ваші облікові записи опинилися під загрозою?

– Які фінансові ризики ви маєте?

– Хто ще може постраждати (родина, друзі, роботодавець)?

2. Оцініть персональні ризики (0–5 балів):

– Ризик несанкціонованого доступу до банківського рахунку

– Ризик компрометації інших онлайн–сервісів

– Ризик фішингу та соціальної інженерії

– Ризик крадіжки особи (identity theft)

– Ризик шантажу чи інших злочинних дій

– Оцініть ймовірність та потенційну шкоду кожного ризику

3. Спрогнозуйте можливі наслідки (0–5 балів):

– Короткострокові наслідки (найближчі дні/тижні)

– Середньострокові наслідки (місяці)

– Довгострокові наслідки (роки)

– Фінансові наслідки

– Емоційні та психологічні наслідки

– Юридичні аспекти

4. Розробіть детальний план дій (0–5 балів):

А) Негайні дії (перші 24 години):

– Покроковий план захисту банківських коштів

– План зміни паролів (у якій послідовності?)

– Дії щодо моніторингу рахунків

Б) Короткострокові заходи (тиждень):

– Захист інших облікових записів

– Моніторинг підозрілої активності

– Комунікація з банком та сервісами

В) Довгострокова стратегія:
– Превентивні заходи на майбутнє
– Зміна практик безпеки
– Документування для можливих юридичних дій

Бланк для відповіді

1. Аналіз масштабу проблеми

_____
_____
_____
_____
_____

2. Оцінка персональних ризиків

_____
_____
_____
_____
_____
_____

3. Прогноз наслідків

Короткострокові:

_____
_____

Середньострокові:

_____
_____

Довгострокові:

_____
_____

4. Детальний план дій

А) Негайні дії (24 години):

_____
_____
_____
_____

Б) Короткострокові заходи (тиждень):

_____
_____
_____
_____

В) Довгострокова стратегія:

_____

_____
_____
_____

Критерії оцінювання відповідей на кейси

Загальні критерії для кожного кейсу (максимум 20 балів)

1. Повнота та глибина аналізу ситуації (0-5 балів)

5 балів:
– Виявлено всі ключові аспекти ситуації
– Проаналізовано як очевидні, так і приховані фактори
– Продемонстровано системне розуміння проблеми
– Враховано контекст та супутні обставини
– Аналіз структурований та логічний

4 бали:
– Виявлено більшість ключових аспектів
– Аналіз достатньо глибокий, але упущено деякі деталі
– Загалом системний підхід присутній
– Логіка аналізу зрозуміла

3 бали:
– Виявлено основні, найбільш очевидні аспекти
– Аналіз поверхневий
– Упущено важливі деталі
– Системність відсутня

2 бали:
– Виявлено лише окремі аспекти
– Аналіз фрагментарний та непослідовний
– Багато важливих факторів не враховано

1 бал:
– Аналіз мінімальний або відсутній
– Нерозуміння суті проблеми

0 балів:
– Відповідь відсутня або повністю неправильна

2. Адекватність оцінки ризиків (0–5 балів)

5 балів:
– Ідентифіковано всі релевантні ризики
– Правильно оцінено рівень кожного ризику
– Враховано ймовірність реалізації ризиків
– Оцінено потенційну шкоду
– Визначено пріоритетність ризиків

4 бали:
– Ідентифіковано більшість важливих ризиків

– Оцінка рівня ризиків загалом адекватна
– Деякі ризики можуть бути переоцінені або недооцінені

3 бали:
– Ідентифіковано основні, найбільш очевидні ризики
– Оцінка ризиків частково правильна
– Упущено важливі ризики

2 бали:
– Ідентифіковано лише поодинокі ризики
– Оцінка неадекватна
– Багато ризиків упущено

1 бал:
– Ризики не ідентифіковано або ідентифіковано неправильно
– Нерозуміння концепції ризику

0 балів:
– Відповідь відсутня

3. Обґрунтованість прийнятого рішення (0–5 балів)

5 балів:
– Рішення оптимальне для даної ситуації
– Наведено переконливе обґрунтування
– Враховано баланс між безпекою та практичністю
– Розглянуто альтернативні варіанти
– Рішення реалістичне та практично здійсненне

4 бали:
– Рішення правильне, але не обов'язково оптимальне
– Обґрунтування присутнє та загалом переконливе
– Баланс врахований частково

3 бали:
– Рішення частково правильне
– Обґрунтування недостатньо переконливе
– Не враховано важливі фактори

2 бали:
– Рішення сумнівне або малоефективне
– Обґрунтування слабке
– Не враховано баланс інтересів

1 бал:
– Рішення неправильне або шкідливе
– Обґрунтування відсутнє або нелогічне

0 балів:
– Відповідь відсутня

4. Здатність прогнозувати наслідки (0–5 балів)

5 балів:
– Спрогнозовано всі ключові наслідки

– Враховано різні сценарії розвитку подій
– Прогнози реалістичні та обґрунтовані
– Визначено як короткострокові, так і довгострокові наслідки
– Продемонстровано розуміння причинно–наслідкових зв'язків
4 бали:
– Спрогнозовано більшість важливих наслідків
– Прогнози загалом реалістичні
– Враховано різні терміни
3 бали:
– Спрогнозовано основні, найбільш очевидні наслідки
– Прогнози поверхневі
– Упущено важливі наслідки
2 бали:
– Спрогнозовано лише окремі наслідки
– Прогнози нереалістичні або необґрунтовані
1 бал:
– Прогноз відсутній або повністю неправильний
– Нерозуміння причинно–наслідкових зв'язків
0 балів:
– Відповідь відсутня

Додаток Ж

ЩОДЕННИК ЦИФРОВОЇ АКТИВНОСТІ
Самооцінювання поведінки в цифровому середовищі з точки зору інформаційної безпеки

ПІБ здобувача: _____
Група: _____
Період ведення щоденника: з _____ по _____ (7 днів)

Інструкція

Протягом одного тижня щодня заповнюйте таблицю, фіксуючи свою цифрову активність та аналізуючи власну поведінку з точки зору інформаційної безпеки. Будьте чесними та критичними до себе – це допоможе виявити вразливості та покращити свою цифрову безпеку.

Що фіксувати:

– Всі використані цифрові сервіси та пристрої.
– Ситуації, коли потрібно було прийняти рішення щодо безпеки.
– Вашу оцінку власних дій (чи були вони безпечними?)
– Виявлені ризики, помилки, небезпечні практики.
– Застосовані заходи захисту.

Щоденні записи

День: _____ (дата)

Розділ	Зміст
1. Використані цифрові сервіси та пристрої	
Пристрої (ноутбук, смартфон, планшет тощо)	
Онлайн-сервіси та додатки (соціальні мережі, месенджери, email, онлайн-покупки, банкінг тощо)	
Мережі Wi-Fi (домашня, публічна, мобільний інтернет)	
2. Ситуації, що потребували рішень щодо інформаційної безпеки	
Опис ситуації 1	
Яке рішення я прийняв/прийняла	
Опис ситуації 2 (за наявності)	
Яке рішення я прийняв/прийняла	
3. Оцінка власних дій з точки зору безпечності	
Які мої дії були безпечними?	
Які мої дії були потенційно небезпечними?	
Чи діяв/діяла я усвідомлено чи автоматично?	
4. Виявлені ризики або помилки	
Які ризики я виявив/виявила?	
Які помилки я допустив/допустила?	
Що могло б статися в найгіршому випадку?	
5. Застосовані заходи захисту	
Які конкретні заходи захисту я використовував/використовувала сьогодні?	

(паролі, VPN, антивірус, двофакторна автентифікація, перевірка посилань тощо)	
Які заходи захисту я НЕ застосував/застосувала, хоча міг/могла?	

Узагальнюючий аналіз (заповнюється наприкінці тижня)

1. Самоаналіз усвідомленості рішень

Наскільки усвідомлено я приймаю рішення щодо інформаційної безпеки?

Аспект	Моя оцінка та обґрунтування
Чи замислююсь я про безпеку перед кожною дією в цифровому середовищі?	
Чи дію я за звичкою/автоматично, чи свідомо оцінюю ризики?	
У яких ситуаціях я був/була найбільш/найменш усвідомленим/усвідомленою?	
Що найчастіше заважає мені приймати усвідомлені рішення? (поспіх, незручність, незнання тощо)	
Загальна оцінка рівня усвідомленості (низький / середній / високий) та чому	

2. Виявлені небезпечні звички

Які небезпечні звички в цифровому середовищі я виявив/виявила у себе?

№	Небезпечна звичка	Як часто це трапляється?	Чому я так роблю?	Який ризик це створює?
1.		☐ Постійно ☐ Часто ☐ Іноді ☐ Зрідка		
2.		☐ Постійно ☐ Часто ☐ Іноді ☐ Зрідка		
3.		☐ Постійно ☐ Часто ☐ Іноді ☐ Зрідка		
4.		☐ Постійно ☐ Часто ☐ Іноді ☐ Зрідка		
5.		☐ Постійно ☐ Часто ☐ Іноді ☐ Зрідка		

3. План змін у цифровій поведінці

Що я планую змінити у своїй цифровій поведінці?

№	Що саме я планую змінити?	Чому це важливо?	Конкретні кроки	Коли почну?	Як буду контролювати виконання?
1.				☐ Негайно ☐ Цього тижня ☐ Цього місяця	
2.				☐ Негайно ☐ Цього тижня ☐ Цього місяця	
3.				☐ Негайно ☐ Цього тижня ☐ Цього місяця	
4.				☐ Негайно ☐ Цього тижня ☐ Цього місяця	
5.				☐ Негайно ☐ Цього тижня ☐ Цього місяця	

4. Систематичність застосування заходів захисту

Наскільки систематично я застосовую заходи захисту інформації?

Захід безпеки	Частота використання	Коментар
Використання надійних паролів	☐ Завжди ☐ Часто ☐ Іноді ☐ Зрідка ☐ Ніколи	
Різні паролі для різних сервісів	☐ Завжди ☐ Часто ☐ Іноді ☐ Зрідка ☐ Ніколи	
Двофакторна автентифікація	☐ Завжди ☐ Часто ☐ Іноді ☐ Зрідка ☐ Ніколи	
Перевірка посилань перед переходом	☐ Завжди ☐ Часто ☐ Іноді	

	☐ Зрідка ☐ Ніколи	
Уважне читання повідомлень/листів	☐ Завжди ☐ Часто ☐ Іноді ☐ Зрідка ☐ Ніколи	
Використання VPN у публічних мережах	☐ Завжди ☐ Часто ☐ Іноді ☐ Зрідка ☐ Ніколи	
Оновлення ПЗ та антивірусу	☐ Завжди ☐ Часто ☐ Іноді ☐ Зрідка ☐ Ніколи	
Перевірка параметрів приватності	☐ Завжди ☐ Часто ☐ Іноді ☐ Зрідка ☐ Ніколи	

Загальний висновок про систематичність:

_____
_____
_____

5. Ключові інсайти

Найважливіші усвідомлення, які я отримав/отримала за цей тиждень:

№	Інсайт
1.	
2.	
3.	

Найбільший ризик, який я виявив/виявила у своїй поведінці:

_____
_____

Найбільша зміна, яку я готовий/готова впровадити:

_____
_____

КРИТЕРІЇ ОЦІНЮВАННЯ ЩОДЕННИКА

Для експерта/викладача:

Параметр оцінювання	Бали	Коментар експерта
1. Повнота та систематичність ведення записів (0-10 балів)	___/10	
Заповнені всі 7 днів		
Всі розділи заповнені кожного дня		
Записи детальні та змістовні		
2. Глибина аналізу власної поведінки (0-10 балів)	___/10	
Аналіз не поверхневий, а глибокий		
Виявлено причини поведінки		
Проаналізовано контекст ситуацій		
3. Здатність виявляти ризики та помилки (0-10 балів)	___/10	
Виявлено реальні ризики		
Виявлено власні помилки		
Оцінено потенційні наслідки		
4. Критичність самооцінки (0-10 балів)	___/10	
Чесна самооцінка без прикрашання		
Визнання проблем та слабких місць		
Об'єктивність оцінок		
5. Конструктивність висновків та планів (0-10 балів)	___/10	
Висновки конкретні та обґрунтовані		
План змін реалістичний та детальний		
Визначено терміни та способи контролю		
ЗАГАЛЬНА ОЦІНКА	**___/50**	

Рівень сформованості рефлексивних навичок:

☐ Високий рівень (40-50 балів / 80-100%)

☐ Середній рівень (25-39 балів / 50-79%)

☐ Початковий рівень (0-24 бали / 0-49%)

Дякуємо за сумлінне ведення щоденника!

Цей досвід допоможе вам краще усвідомити свою поведінку в цифровому середовищі та покращити навички з інформаційної безпеки.