МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВОЛИНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЛЕСІ УКРАЇНКИ

Кафедра загальної математики та методики навчання інформатики

На правах рукопису

КОНОТОПЧИК ДМИТРО ОЛЕКСАНДРОВИЧ

МЕТОДИКА НАВЧАННЯ УЧНІВ ОСНОВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА МЕДІАГРАМОТНОСТІ

Спеціальність: 014 «Середня освіта (Інформатика)»
Освітньо-професійна програма «Середня освіта. Інформатика»
Робота на здобуття освітнього ступеня «Магістр»

Науковий керівник:
РОЙКО ЛАРИСА ЛЕОНІДІВНА,
кандидат педагогічних наук, доцент
кафедри загальної математики та
методики навчання інформатики

РЕКОМЕНДОВАНО ДО ЗАХИСТУ
Протокол № ____
засідання кафедри загальної математики
та методи навчання інформатики
від _____ 2024 року
Завідувач кафедри:

_____ _____
(підпис) ПІБ

ЛУЦЬК – 2024

Анотація

Конотопчик Д. О. Методика навчання учнів основ інформаційної безпеки та медіаграмотності – Рукопис

Кваліфікаційна робота за спеціальністю 014 Середня освіта (Інформатика). – Волинський національний університет імені Лесі Українки. Луцьк, 2024.

У кваліфікаційній роботі на основі теоретичного аналізу наукової, навчально-методичної, психолого-педагогічної літератури досліджено поняття інформаційної безпеки та медіаграмотності, проаналізовано їх історичний розвиток, сучасні виклики та потреби інтеграції в освітній процес.

Розглянуто моделі формування медіаграмотності та інформаційної безпеки, окреслено принципи і методи їх реалізації у навчальному процесі. Проаналізовано переваги й недоліки використання цифрових технологій у формуванні цих компетенцій, а також розроблено дидактичні матеріали для інтерактивного навчання з акцентом на медіаграмотність і інформаційну безпеку.

Розроблено інтерактивну платформу для контролю й оцінювання рівня успішності учнів з питань інформаційної безпеки та медіаграмотності. Сформульовано основні принципи її роботи, спроєктовано структуру та реалізовано функціональні можливості платформи. Особливу увагу приділено її адаптації для умов дистанційного та змішаного навчання.

Експериментально перевірено ефективність запропонованої платформи та її вплив на рівень сформованості медіаграмотності та інформаційної безпеки учнів. Сформульовано рекомендації щодо впровадження запропонованих рішень у шкільну практику.

Ключові слова: медіаграмотність, інформаційна безпека, інтерактивне навчання, цифрові технології, освітній процес, освітня платформа, критичне мислення, навчальні ресурси.

Abstract

Konotopchyk D. O. Methodology for teaching students the basics of information security and media literacy – Manuscript

Master's thesis in the specialty 014 Secondary education (Informatics). – Lesya Ukrainka Volyn National University. Lutsk, 2024.

This study, based on theoretical analysis of scientific, educational-methodological, psychological, and pedagogical literature, examines the concepts of information security and media literacy. It analyzes their historical development, contemporary challenges, and the need for integration into the educational process, highlighting their role in preparing future informatics teachers.

Models for forming media literacy and information security are explored, along with the principles and methods for implementing them in the educational process. The advantages and disadvantages of using digital technologies in fostering these competencies are analyzed, and didactic materials for interactive teaching focusing on media literacy and information security are developed.

An interactive platform is proposed to monitor and assess students' proficiency in information security and media literacy. The key principles of its operation are formulated, its structure is designed, and functional capabilities are implemented, with particular attention to its adaptation for distance and blended learning conditions.

The effectiveness of the developed platform and its impact on the level of students' media literacy and information security were experimentally verified. Recommendations for integrating the proposed solutions into school practice are provided.

Keywords: media literacy, information security, interactive learning, digital technologies, educational process, educational platform, critical thinking, teaching resources.

ЗМІСТ

ВСТУП

Актуальність теми. У сучасному світі, що характеризується стрімким розвитком цифрових технологій, інформаційна безпека та медіаграмотність набувають надзвичайної важливості. З кожним днем збільшується обсяг інформації, яка поширюється через різноманітні медіа-канали, що створює, як нові можливості, так і серйозні загрози для суспільства. Учні, які активно користуються цифровими пристроями та мережевими ресурсами, потребують спеціальних знань та навичок для захисту своєї особистої інформації, критичного оцінювання інформаційних джерел, а також протистояння маніпуляціям та кіберзагрозам.

В умовах зростаючої кількості кібератак, дезінформації та впливу на свідомість молоді через соціальні мережі навчання основ інформаційної безпеки та медіаграмотності стає одним із ключових завдань сучасної освіти. Це забезпечує формування свідомих, компетентних і відповідальних громадян, здатних орієнтуватися в інформаційному просторі та захищати свої права в цифровому середовищі. Водночас медіаграмотність допомагає розвивати критичне мислення, сприяє розумінню механізмів створення та поширення інформації, формує здатність до усвідомленого споживання та аналізу інформаційного контенту.

У новій редакції Концепції впровадження медіаосвіти в Україні наводиться наступне визначення: «Медіаграмотність – складова медіакультури, яка торкається вміння користуватися інформаційно-комунікативною технікою, виражати себе та спілкуватися за допомогою медіазасобів, успішно здобувати необхідну інформацію, свідомо сприймати та критично тлумачити інформацію, отриману з різних медіа, відділяти реальність від її віртуальної симуляції, тобто розуміти реальність, сконструйовану медіаджерелами, осмислювати владні стосунки, міфи й типи контролю, які вони культивують» [24].

На уроках інформатики інформаційна безпека і медіаграмотність формуються паралельно із засвоєнням інформаційних технологій. Інтеграція цих знань сприяє формуванню цифрової компетентності, яка є невід’ємною

частиною освіти XXI століття. Це забезпечує не лише технічні навички, а й свідоме ставлення до інформаційного простору.

Таким чином, актуальність теми зумовлена необхідністю формування в учнів навичок безпечної поведінки у цифровому середовищі та критичного ставлення до медіаконтенту, як одного з важливих чинників успішної адаптації в умовах сучасного інформаційного суспільства.

Мета дослідження полягає у розробці та впровадженні методики навчання учнів старших класів основам інформаційної безпеки та медіаграмотності з використанням розробленої інтерактивної платфоми.

Відповідно до теми та мети визначено **завдання дослідження**:

- проаналізувати теоретичні основи інформаційної безпеки та медіаграмотності, їх значення у сучасній освіті на основі опрацювання наукової, навчально-методичної, психолого-педагогічної літератури;

- проаналізувати нормативно-правову базу, навчальні програми та рекомендації щодо формування навичок інформаційної безпеки та медіаграмотності учнів;

- дослідити сучасні підходи, методи, засоби та методику навчання інформаційної безпеки та медіаграмотності школярів у процесі вивчення інформатики;

- споєктувати та розробити інтерактивну платформу для навчання основам інформаційної безпеки та медіаграмотності учнів старших класів;

- провести перевірку ефективності використання програмного засобу у формуванні компетентностей з інформаційної безпеки та медіаграмотності у процесі вивчення інформатики;

- розробити навчальні матеріали та завдання для інтеграції цих тем у навчальний процес;

- сформулювати рекомендації для практичного впровадження та використання програмного продукту.

Об’єкт дослідження – процес навчання школярів основам інформаційної безпеки та медіаграмотності в освітньому середовищі.

Предмет дослідження – технології проєктування, засоби створення та методичні особливості змістового наповнення інтерактивної платфоми з формування основ інформаційної безпеки та медіаграмотності учнів старших класів.

Практичне значення: розроблену інтерактивну платформу «Основи інформаційної безпеки та медіаграмотності» можна використовувати на уроках інформатики з метою розвитку та поглиблення практичних навичок з основ інформаційної безпеки та медіаграмотності учнів старших класів. Матеріали, розміщені на платформі, сприяють формуванню критичного мислення, навичок безпечного користування інформаційними ресурсами та протидії маніпулятивним технікам у медіапросторі. Платформа адаптована до сучасних вимог цифрового навчання і може використовуватись також у дистанційній та змішаній форматах навчання.

Наукова новизна: зміст навчального матеріалу інтерактивної платформи сприяє розвитку інтелектуальних та творчих здібностей, розвитку вміння орієнтуватися у сучасному медіапросторі, використовувати цифрові технології для задоволення власних навчальних потреб, поширювати створений власноруч медіаконтент. Впровадження інтерактивної платформи у навчальний процес сприятиме формуванню компетентностей у сфері інформаційної безпеки та медіаграмотності.

Методологічна база дослідження. Відповідно до визначених завдань застосовувалися наступні **методи дослідження:**

- теоретичні: аналіз наукової, навчально-методичної, психолого-педагогічної літератури, нормативно-законодавчої документації і періодичних навчальних видань з проблеми дослідження;

- емпіричні: анкетування, систематизація, узагальнення; аналіз програмного забезпечення.

База дослідження: заклад загальної середньої освіти «Великоглушанський ліцей» Камінь-Каширської міської ради Волинської області.

Апробація результатів дослідження. Результати дослідження були представлені на XIII Міжнародній науково-практичній конференції «Математика. Інформаційні технології. Освіта» (тези); XLIII Міжнародній науково-практичній конференції «Сучасні виклики та досягнення наукової спільноти XXI століття» (тези); електронному мультидисциплінарному науковому часописі «Нотатки сучасної науки».

1. Конотопчик Д. О., Ройко Л. Л. Безпечна поведінка школярів у цифровому середовищі. *Математика. Інформаційні технології. Освіта* : збірник тез доп. XIII міжнар. наук.-практ. конф. (м. Луцьк, 31 травн.-2 червн. 2024 р.). Луцьк, 2024. С. 225-227 [20].

2. Конотопчик Д. О., Ройко Л. Л. Розвиток інформаційно-цифрової компетентності учителів інформатики у процесі дистанційного навчання. *Modern Challenges and Achievements of the Scientific Community of the 21st century :* XLIII International scientific and practical conference (October 16-18, 2024). Narva, Estonia. International Scientific Unity, 2024. С.154-156 [21].

3. Конотопчик Д. О., Ройко Л. Л. Формування інформаційної безпеки та медіаграмотності майбутніх вчителів інформатики. *Нотатки сучасної науки: електронний мультидисциплінарний науковий часопис*. Харків: СГ НТМ «Новий курс», 2024. № 19. С.5 [22].

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА МЕДІАГРАМОТНОСТІ

1.1. Медіаграмотність як суспільне, наукове та освітнє явище

Згідно з Концепцією впровадження медіаосвіти в Україні на період до 2025 року визначено і охарактеризовано її складники: медіаосвіта дошкільна, шкільна, позашкільна, вища школа, батьківська, медіаосвіта дорослих, медіаосвіта засобами медіа (неформальна). Окрім цього визначено завдання, принципи, напрями, форми та основні етапи впровадження медіаосвіти в Україні. Концепція спрямована на підвищення рівня медіаграмотності, що є важливим в умовах інформаційного суспільства, де люди постійно стикаються з великою кількістю інформаційних потоків, у тому числі недостовірних або маніпулятивних [24].

Медіаграмотність – це сукупність знань, навичок і умінь, які дозволяють усвідомлено сприймати, аналізувати та оцінювати інформацію, що поширюється через різноманітні медіа. В епоху інформаційних технологій медіаграмотність стала необхідною умовою успішної соціалізації та повноцінного функціонування у суспільстві. Вона не обмежується лише вмінням споживати контент, але й включає здатність розуміти, яким чином цей контент може впливати на думки, поведінку та соціальні відносини. Збільшення кількості фейкових новин, маніпуляцій, пропаганди і дезінформації вимагає від громадян нових навичок і знань для протистояння таким загрозам.

Медіаграмотність забезпечує суспільству механізми протидії таким негативним явищам, як інформаційні атаки, політична маніпуляція через медіа, мова ворожнечі та інші форми шкідливого впливу інформаційного середовища. Вона також відіграє ключову роль у збереженні інформаційної безпеки та стійкості суспільства перед зовнішніми і внутрішніми інформаційними загрозами [10].

З наукової точки зору, медіаграмотність є предметом дослідження у багатьох дисциплінах, таких як соціологія, філологія, психологія, педагогіка, інформаційні технології. Вона охоплює вивчення різних аспектів взаємодії людини з медіа: від особливостей сприйняття інформації до аналізу механізмів впливу медіа на свідомість людини.

Аналіз науково-педагогічної літератури [25, 39, 47, 49, 50, 57] дає можливість стверджувати, що наукові дослідження у галузі медіаграмотності зосереджуються у кількох напрямах:

- вивчення медіа-впливу: дослідження того, як медіа впливають на формування суспільних настроїв, політичних поглядів та культурних цінностей (вивчаються, зокрема, механізми пропаганди, маніпуляції свідомістю, а також ефекти дезінформації та фейкових новин);

- розвиток критичного мислення: науковці вивчають, яким чином медіаграмотність сприяє розвитку критичного мислення у споживачів медіа та які дидактичні методи найкраще сприяють розвитку цієї навички;

- медіа-екологія: науковий підхід, що досліджує взаємодію людей із медіа середовищем, оцінюючи, як інформаційні потоки впливають на культуру та поведінку. Зокрема, вивчаються наслідки інтенсивного використання цифрових медіа та соціальних мереж на психічне здоров’я та соціальні взаємодії;

- психологія медіа: зосереджується на тому, як люди сприймають та обробляють медіаконтент; досліджує емоційні та когнітивні реакції на інформаційні потоки, вплив візуальних та аудіальних елементів, а також мотиваційні аспекти споживання медіа;

- дослідження освітніх практик: науковці розробляють і тестують методики навчання медіаграмотності, оцінюючи їх ефективність та вплив на різні вікові групи.

В освітній сфері медіаграмотність виступає важливим інструментом для підготовки учнів до життя у сучасному інформаційному суспільстві. З розвитком цифрових технологій традиційні підходи до освіти доповнюються новими формами навчання, спрямованими на розвиток у молодого покоління навичок

критичного мислення та аналізу інформації.

Основні завдання освітньої діяльності з розвитку медіаграмотності включають [9]:

1. Навчання розумінню медіаконтенту: учні повинні вміти ідентифікувати джерела інформації, аналізувати їхню достовірність, виявляти пропагандистські прийоми та фейкові новини. Особлива увага приділяється навичкам перевірки фактів і критичного осмислення отриманої інформації.

2. Розвиток навичок створення медіаконтенту: медіаграмотність передбачає не лише вміння аналізувати медіа, але й створювати власний контент, використовуючи етичні норми та технічні можливості сучасних медіаресурсів, що допомагає учням глибше розуміти механізми створення та поширення інформації.

3. Формування відповідального споживання медіа: освіта у сфері медіаграмотності сприяє формуванню усвідомленого підходу до споживання медіапродукції, вихованню етичних норм користування інформаційними ресурсами та медіаресурсами.

4. Захист від інформаційних загроз: одним із завдань освітніх програм з медіаграмотності є підготовка учнів до розпізнавання та протидії інформаційним загрозам, таким як фейки, кібербулінг, шахрайство в мережі та інші негативні явища інформаційного простору.

Формування інформаційної безпеки та медіаграмотності вимагає систематичного, багаторівневого підходу до навчання, який охоплює як теоретичні знання, так і практичні навички. Це означає, що в освітній процес повинні бути інтегровані навчальні матеріали та методи, які допоможуть школярам зрозуміти основні принципи роботи з інформацією, навчити їх виявляти та уникати інформаційних загроз, а також формувати відповідальне ставлення до використання медіа ресурсів.

Особливу увагу слід приділяти різноманітним типам загроз: від фейкових новин і маніпуляцій до кібербулінгу і крадіжки персональних даних. У цьому контексті важливо забезпечити учнів не тільки знаннями про можливі небезпеки,

але й навичками запобігання та захисту від них.

Одним із ефективних способів формування інформаційної безпеки та медіаграмотності є інтегровані уроки, які дозволяють систематично включати в освітній процес питання, пов’язані з критичним аналізом інформації, кібербезпекою та етикою використання медіа ресурсів.

Наприклад, під час вивчення історії можна аналізувати історичні приклади пропаганди та дезінформації, що дозволить учням краще розуміти механізми маніпуляції інформацією. На уроках інформатики важливо навчати основам кібербезпеки, включаючи захист особистих даних та вміння користуватися антивірусними програмами.

Сучасна освіта надає можливості для впровадження різноманітних інтерактивних методик, які сприяють ефективному засвоєнню знань з інформаційної безпеки та медіаграмотності. Це можуть бути такі методи, як групові дискусії, проєктне навчання, ігрові методики та кейс-методи.

Одним із важливих елементів формування критичного мислення на тему медіа впливу та інформаційних загроз є дискусії. Учні можуть обговорювати реальні випадки маніпуляцій через медіа, аналізувати фейкові новини або приклади пропаганди. Такі дискусії дозволяють не тільки краще розуміти, як працює медіасередовище, але й навчитися аргументувати власну думку та відстоювати її.

Проєктне навчання – це ефективна методика, яка допомагає школярам не лише освоїти теоретичні знання, а й застосувати їх на практиці. Наприклад, учні можуть створювати власні проєкти з аналізу медіа-контенту, розробляти кампанії щодо підвищення обізнаності про кібербезпеку або моделювати інформаційні атаки та шляхи їхнього запобігання.

Ігрові методики є чудовим інструментом для засвоєння знань у ненав’язливій, інтерактивній формі. Сьогодні існують різні дидактичні ігри, спрямовані на розвиток медіаграмотності та інформаційної безпеки, які допомагають учням на практиці вивчати, як уникати кіберзагроз, захищати свої особисті дані, або розпізнавати фейкові новини.

Аналіз реальних кейсів із медіа або прикладів кіберзагроз дозволяє учням глибше зрозуміти, як працюють інформаційні загрози на практиці. Наприклад, школярі можуть розглянути конкретні приклади кібератак, що мали місце у світі, та обговорити, як можна було б захиститися від подібних ситуацій.

Важливою ланкою у процесі формування медіаграмотності є педагог, який повинен не тільки володіти необхідними знаннями та компетенціями у сфері медіа-освіти, але й бути готовим застосовувати інноваційні методики, що відповідають викликам цифрового суспільства; добре обізнаним про загрози інформаційного середовища та методи їхньої нейтралізації. Це вимагає регулярного підвищення кваліфікації, навчання новим методикам викладання, а також доступу до сучасних навчальних матеріалів та технологій.

Педагоги повинні використовувати інтерактивні методики, що включають активну участь учнів у процесі навчання. Це можуть бути майстер-класи, семінари, онлайн-курси та вебінари, де учні зможуть отримувати практичні знання та застосовувати їх на практиці. Таким чином школярі матимуть можливість експериментувати з медіаресурсами, створювати власні інформаційні продукти (наприклад, відео, блоги, новинні випуски), що сприяє не тільки розвитку технічних навичок, але й усвідомленню етичних аспектів медіа-культури.

Ключовим аспектом формування медіаграмотності та інформаційної безпеки є розвиток у школярів критичного мислення, яке є основою для ефективної взаємодії з інформаційним середовищем, оскільки дозволяє учням не тільки сприймати інформацію, але й аналізувати її, виявляти маніпуляції та оцінювати ризики [8].

Особлива увага повинна приділятися формуванню в учнів навичок самостійного аналізу інформаційних загроз, таких як фейки, кібербулінг, фішинг та інші небезпеки, які вони можуть зустріти в цифровому середовищі. Завдяки інтеграції цих тем у навчальний процес, учні будуть краще підготовлені до самостійного прийняття рішень в інформаційній сфері [4].

Формування інформаційної безпеки та медіаграмотності у школярів є

важливим завданням сучасної освіти, яке потребує системного підходу та використання різноманітних методик. Інтеграція цих тем у навчальний процес, використання інтерактивних методик і підвищення кваліфікації педагогів сприяють розвитку у школярів критичного мислення та навичок безпечної взаємодії з інформаційним середовищем.

Таким чином, медіаграмотність як освітнє явище сприяє формуванню сучасних навичок роботи з інформацією у школярів, що дозволяє їм адаптуватися до викликів цифрового світу. Вона є фундаментом для розвитку інформаційної безпеки, критичного мислення та громадянської відповідальності. Для успішного розвитку медіаграмотності необхідна спільна робота освітян, науковців, медіа та усього суспільства.

Зупинимось на понятті медіа-інформаційної грамотності, як основі інформаційної безпеки.

Медіа-інформаційна грамотність (МІГ) – це комплексна концепція, що об’єднує знання, навички та компетенції, необхідні для ефективної роботи з інформацією та медіаконтентом. Вона забезпечує здатність не тільки отримувати доступ до різноманітних джерел інформації, але й критично оцінювати її, відрізняти надійну інформацію від маніпулятивної або хибної. З розвитком технологій зростає не тільки кількість інформації, а й різноманітність каналів її поширення: соціальні мережі, блог-платформи, новинні портали, стрімінгові сервіси та інші. В умовах цієї різноманітності навички критичного аналізу інформаційного контенту є не просто важливими, а необхідними для забезпечення інформаційної безпеки як особистої, так і суспільної [32].

У сучасній освіті формування МІГ – це не лише питання технічних знань про пошук інформації, а й питання розвитку етичних принципів її використання. Студенти і школярі повинні розуміти, як поширюється інформація, як працюють алгоритми соціальних мереж, як інформація може бути використана з метою маніпуляції або дезінформації. Ці знання допомагають уникати пасток пропаганди та інформаційних загроз.

Медіа-інформаційна грамотність передбачає наступні аспекти [34]:

- критичне мислення та аналіз інформації: школярі навчаються аналізувати джерела інформації, перевіряти їх на достовірність і об’єктивність, а також розуміти, які інтереси можуть стояти за тим чи іншим контентом (навичка є важливою для розпізнавання фейкових новин, пропаганди та маніпуляцій);

- оцінка інформаційної безпеки: уміння працювати з інформацією включає розуміння можливих ризиків, пов’язаних із використанням онлайн-ресурсів: крадіжка даних, шкідливе програмне забезпечення, кібербулінг, фішинг тощо (дозволяє учням безпечно використовувати інформаційні ресурси, зберігаючи конфіденційність своїх даних та захищаючи особисту інформацію);

- етичне використання медіа та інформації, що охоплює аспекти етичної поведінки в інформаційному середовищі: відповідальність за створення і поширення контенту, повага до авторських прав та особистої інформації інших користувачів; включає розуміння правил поведінки в Інтернеті, таких як уникнення мовленнєвої агресії та зловживання свободою слова;

- розвиток навичок створення контенту: власні інформаційні контент-тексти, відео, мультимедійні проєкти – з дотриманням етичних та юридичних норм (розвиває креативність та відповідальність у взаємодії з медіа).

Освіта є ключовим інструментом для формування медіа-інформаційної грамотності серед молодого покоління. У світі, де інформаційні технології швидко розвиваються, освітні програми повинні бути адаптовані до сучасних викликів, що виникають через інформаційну перенасиченість.

Впровадження медіа-інформаційної грамотності у навчальні програми сприяє:

- адаптації до інформаційного суспільства;
- формуванню критичного мислення;
- формуванню комунікативних навичок;
- відповідальному використанню інформаційних ресурсів.

Навчання медіа-інформаційній грамотності дозволяє школярам ефективно взаємодіяти з цифровими технологіями та інформаційними ресурсами, правильно використовувати пошукові системи, формувати навички оцінки

надійності джерел, а також здатності обробляти великі обсяги інформації.

Одним із основних завдань медіа-освіти є розвиток у молоді вміння мислити критично, що дозволяє їм не тільки сприймати інформацію, але й аналізувати її з позиції різних точок зору, виявляючи маніпуляції та фейки.

МІГ сприяє розвитку навичок ефективної комунікації через різні медіаканали, включаючи письмові тексти, аудіовізуальні медіа та інтернет. Це важливо не тільки для особистого розвитку, але й для професійного становлення в умовах сучасного інформаційного ринку. Навчання МІГ допомагає школярам формувати відповідальне ставлення до інформаційних ресурсів: вони повинні розуміти, як інформація може впливати на інших людей, усвідомлювати, що дезінформація та маніпуляції можуть мати серйозні наслідки для суспільства.

Незважаючи на очевидні переваги, впровадження медіа-інформаційної грамотності у систему освіти стикається з низкою викликів:

1. Підготовка педагогічних кадрів. Для ефективного навчання медіаграмотності необхідно підготувати викладачів, які б мали відповідні навички та знання. Це вимагає оновлення програм підготовки вчителів і регулярного підвищення їхньої кваліфікації.

2. Забезпечення доступу до сучасних ресурсів. У багатьох школах і навчальних закладах відчувається брак технологічного забезпечення для навчання медіа-інформаційної грамотності. Учні потребують доступу до сучасних комп’ютерів, Інтернету та навчальних програм, які б відповідали потребам цифрової епохи.

3. Оновлення навчальних програм. Зміни в інформаційному середовищі відбуваються дуже швидко, тому навчальні програми повинні постійно оновлюватися, аби залишатися актуальними. Це вимагає систематичного перегляду змісту освітніх курсів з урахуванням нових медіа та інформаційних загроз.

4. Мотивація учнів. Школярі не завжди сприймають медіа-інформаційну грамотність як необхідний навик. Тому важливо забезпечити мотивацію до навчання, показуючи реальні приклади того, як МІГ допомагає в повсякденному

житті та професійній діяльності.

Медіа-інформаційна грамотність є невід'ємною частиною сучасної освіти, що готує школярів до життя в інформаційному суспільстві. Вона сприяє формуванню критичного мислення, розвитку комунікативних навичок і забезпечує безпечну взаємодію з інформаційним середовищем.

1.2. Актуальні загрози інформаційній безпеці в умовах цифровізації

З розвитком цифрових технологій та їх широким проникненням у всі сфери життя, постали нові виклики, пов'язані з інформаційною безпекою. Цифровізація, яка покликана спростити доступ до інформації та вдосконалити процеси обміну даними, одночасно створює сприятливі умови для виникнення нових загроз. Огляд актуальних загроз інформаційній безпеці дозволить глибше усвідомити їх природу та запропонувати ефективні шляхи протидії.

Основні загрози інформаційної безпеки представлені на рисунку 1.1.

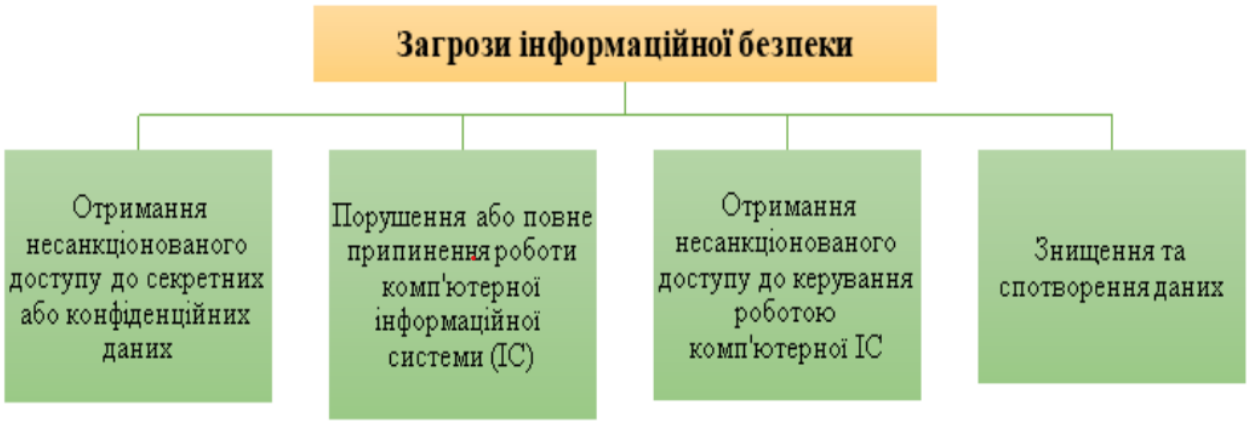


Рисунок 1.1. Загрози інформаційної безпеки

Однією з найсерйозніших загроз в умовах цифровізації є кіберзлочинність, що охоплює широкий спектр шкідливої діяльності, яка здійснюється за допомогою інформаційно-комунікаційних технологій. Серед основних проявів кіберзлочинності можна виділити такі явища, як:

- Фішинг – шахрайські методи отримання конфіденційної інформації (паролів, банківських реквізитів) через підроблені електронні листи або веб-сайти. Небезпека цього виду атак полягає в їхньому масовому характері та складності для пересічних користувачів розпізнати загрозу.

- Шкідливе програмне забезпечення (Malware) – це широкий клас програм, які призначені для пошкодження або викрадення даних. У цю категорію входять віруси, трояни, шпигунські програми, які можуть бути використані як для викрадення інформації, так і для виведення з ладу комп'ютерних систем.

- Ransomware (вимагальне програмне забезпечення) – особливий тип атак, де злочинці шифрують дані користувача і вимагають викуп за відновлення доступу до них. Відсутність гарантій повернення даних після оплати викупу робить ці атаки особливо небезпечними для компаній та індивідуальних користувачів.

Витоки даних є ще однією ключовою загрозою в умовах цифровізації. Вони можуть бути наслідком як технічних недоліків, так і несанкціонованих дій або помилок користувачів. Часто витоки даних відбуваються через неправильну конфігурацію систем безпеки, що призводить до несанкціонованого доступу до конфіденційної інформації. Особливу небезпеку становлять випадки, коли великі обсяги персональних даних стають доступними для третіх осіб через помилки у налаштуваннях баз даних або хмарних сервісів. Помилки людського фактору, коли працівники ненавмисно сприяють витокам інформації через некоректне поводження з конфіденційними даними або порушення процедур безпеки. Така загроза потребує підвищення рівня обізнаності персоналу щодо правил кібербезпеки.

Проблема кібербулінгу, особливо серед молоді, є новим викликом, який виник у цифрову епоху. Відсутність фізичної присутності в цифровому просторі та можливість анонімної взаємодії часто сприяють агресивній поведінці, яка може мати серйозні наслідки для психічного здоров'я. Зокрема, постраждалі від кібербулінгу можуть відчувати тривожність, депресію, а в найгірших випадках навіть наражатися на ризик самогубства.

Умови цифровізації сприяли появі феномена масового поширення дезінформації та фейкових новин. Соціальні мережі стали потужним інструментом маніпуляції суспільною свідомістю, коли неправдиві або навмисно викривлені дані можуть швидко поширюватися серед користувачів, впливаючи на їхні думки, емоції та рішення. Роль медіаграмотності у цьому контексті стає ключовою, оскільки вона формує критичне мислення та здатність розпізнавати дезінформацію.

Загрози приватності набули особливого значення в умовах активного використання інтернет-ресурсів та соціальних мереж. Користувачі часто не розуміють повною мірою, як їхні персональні дані збираються, зберігаються та використовуються третіми сторонами. Недостатній рівень усвідомлення цієї проблеми створює ризики несанкціонованого доступу до персональної інформації та її використання у комерційних або навіть шкідливих цілях.

Цифровізація відкриває нові перспективні можливості для розвитку суспільства, але водночас породжує серйозні загрози інформаційній безпеці. Найбільш небезпечними з них є кіберзлочинність, витоки даних, кібербулінг, дезінформація та порушення приватності [44]. Для мінімізації цих ризиків необхідно формувати в учнів комплекс навичок, які дозволять їм безпечно користуватися цифровими технологіями, розпізнавати загрози та критично оцінювати інформаційні потоки. Ефективна система освіти у галузі інформаційної безпеки та медіаграмотності має стати основою для підготовки молодого покоління до викликів сучасного інформаційного середовища.

1.3. Методика формування основ інформаційної безпеки та медіаграмотності у процесі навчання школярів

Формування інформаційної безпеки та медіаграмотності у школярів є важливим завданням сучасної системи освіти, оскільки діти стають активними користувачами цифрових технологій вже з раннього віку. Питання полягає не тільки у тому, щоб навчити школярів використовувати технології, але й у тому,

щоб зробити їх обізнаними щодо можливих загроз та маніпуляцій, з якими вони можуть зіткнутися в Інтернеті. Виховання критичного мислення та інформаційної культури сприяє запобіганню ризикам, пов’язаним з кіберзлочинністю, маніпуляцією інформацією, фейковими новинами та кібербулінгом.

Основні аспекти формування інформаційної безпеки за джерелом [14]:

1. Захист персональних даних. Учнів необхідно навчати розпізнавати загрози, пов’язані з передачею приватної інформації через Інтернет. Це включає пояснення важливості складних паролів, небезпеки фішингових атак та виявлення підозрілих повідомлень.

2. Безпечна поведінка в Інтернеті. Школярі повинні знати правила безпечного використання соціальних мереж та електронної пошти, а також розуміти наслідки своїх дій в онлайн-просторі. Під час уроків важливо розвивати навички розпізнавання шкідливих програм, кібербулінгу та методів самооборони в разі загроз.

3. Кіберетика. Важливо виховувати в учнів не тільки технічні навички, а й етичні норми поведінки в Інтернеті, які охоплюють повагу до інших користувачів, запобігання булінгу та неправомірному використанню чужих матеріалів.

Медіаграмотність передбачає вміння аналізувати, критично оцінювати та інтерпретувати інформацію, яка надходить з різних джерел: телебачення, радіо, друкованих медіа та особливо Інтернету. На уроках інформатики важливо привертати увагу до того, як інформація може бути спотворена або маніпулюватися з певною метою. Учні повинні навчитися аналізувати джерела інформації, розуміти, як виявляти фейкові новини, відрізняти факти від думок і як уникати дезінформації.

Окрім споживання інформації, школярі мають навчитися створювати власний контент, як наприклад блоги, відео чи пости у соціальних мережах. Це допомагає краще зрозуміти відповідальність за якість та правдивість поданої інформації.

1.3.1. Питання медіаграмотності та інформаційної безпеки у навчальних програмах з інформатики

Поділяємо думку науковців О. Грицюк, Л. Максимової, А. Опришко, що «медіаграмотність працівника закладу загальної середньої освіти включає [9]:

- уміння аналізувати, критично осмислювати й створювати медіа тексти;
- здатність ідентифікувати джерело медіа тексту, його політичні, соціальні, комерційні та культурні інтереси і відповідний контекст;
- навички добору відповідних медіа для створення та поширення власних медіа текстів і залучення зацікавленої в них аудиторії;
- вільний доступ до медіа для споживання та виробництва власної медіа продукції;
- розуміння важливості міжособистісного професійного спілкування для успішності будь-якої трудової діяльності;
- прагнення до підвищення рівня комунікаційної та медіакомпетентності;
- уміння спілкуватися з використанням для цього телекомунікаційних каналів зв’язку» [9].

При вивченні шкільної інформатики основи медіграмотності формуються паралельно із вивченням і засвоєнням інформаційних технологій, оскільки:

- на уроках інформатики школярі вчаться працювати з різноманітними програмними засобами для створення, редагування та розповсюдження медіаконтенту;
- пошук, перевірка вірогідності та відбір релевантної інформації з мережі Інтернет для підготовки проєктів та досліджень сприяє розвитку вмінь критично оцінювати медіаресурси, виявляти маніпуляції та упередженість;
- вивчаючи правові аспекти використання інформаційних ресурсів, учні усвідомлюють важливість дотримання авторського права у медіасфері, навчаються коректно цитувати та посилатися на джерела;
- на заняттях розглядаються питання захисту персональних даних, протидії кібербулінгу, шахрайству та іншим онлайн-загрозам, що розвиває

навички безпечної медіаповедінки;

- створення учнями власних мультимедійних проєктів (вебсайтів, блогів, відео та ін.) інтегрує різні медіанавички – від виробництва контенту до його промоції та поширення;

- робота з медіаресурсами на уроках інформатики може поєднуватися з аналізом медіатекстів на уроках мови, літератури, історії тощо, комплексно розвиваючи медіаграмотність.

Курс інформатики у 10-11 класах є обов'язково-вибірковим з великою варіативною складовою. Згідно навчальної програми з інформатики для старшої школи (10-11 класи) рівень стандарту «Інформаційна безпека» вивчається вибірковим модулем (17 год.), включаючи основи безпеки інформаційних технологій (базові принципи збереження даних, робота з паролями, основи криптографії); забезпечення безпеки інформаційних технологій (практичні прийоми захисту даних, встановлення антивірусного та антишпигунського програмного забезпечення); забезпечення безпеки комп'ютерних систем і мереж (розгляд механізмів захисту від несанкціонованого доступу, принципи роботи брандмауерів, загальні підходи до захисту локальних і глобальних мереж). Стосовно базового модуля, то питання проблем інформаційної безпеки, загрози при роботі в Інтернеті і їх уникнення вивчаються у межах теми «Інформаційні технології в суспільстві» [16].

На рівні профільного навчання питання інформаційної безпеки, рівні та протоколи інформаційної безпеки, керування ризиками в інформаційних системах вивчаються у межах теми «Сучасні інформаційні технології» [17].

1.3.2. Форми, методи і засоби формування основ медіаграмотності у процесі позакласної та виховної діяльності

Позакласна та виховна діяльність є важливими складовими загальноосвітнього процесу, де можна більш творчо підходити до формування основ медіаграмотності. Вони дають можливість поглиблювати знання учнів та

сприяти їхньому критично-аналітичному мисленню у невимушеній обстановці. Залучення учнів до різноманітних форм діяльності дозволяє зробити процес навчання більш цікавим, інтерактивним і гнучким.

До форм позакласної діяльності, що сприяють формуванню медіаграмотності можна віднести:

- гуртки, факультативні курси – школярі мають можливість обговорювати різні медіа-матеріали (новини, фільми, відео з Інтернету) і вчитися аналізувати їх критично; така діяльність стимулює їх спільно шукати рішення щодо реальних медіа-проблем і розвивати навички самостійної роботи з інформацією;

- тренінги та воркшопи з медіаграмотності – школярі отримують практичні поради щодо безпеки в Інтернеті, розпізнавання фейкових новин та основних методів маніпуляції інформацією.

Методи формування медіаграмотності:

- *Метод кейсів.* Робота з конкретними прикладами (кейсами) допомагає учням практично застосовувати знання і навички, пов’язані з критичним аналізом інформації. Використання реальних або вигаданих новин, відео або постів у соціальних мережах допомагає навчити школярів розпізнавати маніпуляції та дезінформацію.

- *Ігрові методи*. Гейміфікація у навчанні може бути ефективною для учнів різного віку. Використання дидактичних ігор допомагає візуалізувати наслідки неправильного поводження з інформацією або порушення правил інформаційної безпеки. Це робить процес навчання цікавішим і залучає учнів до активної участі.

- *Метод дискусій.* Дискусії у невимушеній обстановці дозволяють учням висловлювати свої думки, ставити під сумнів медіа-джерела, а також аналізувати різні точки зору. Це сприяє розвитку навичок критичного мислення та вмінню аргументувати свою точку зору.

- *Проєктний метод*. Дає учням можливість самостійно або в групах досліджувати певні аспекти медіаграмотності (наприклад, розробка власних медіа-проєктів, таких як створення блогів, відео чи подкастів, що дозволяє їм розвивати практичні навички роботи з медіа і краще розуміти структуру медіа-

простору). Даний метод зміцнює навички командної роботи та самопрезентації.

Засоби формування медіаграмотності:

- інтерактивні платформи: для позакласної діяльності можуть бути використані різноманітні інтерактивні онлайн-платформи та додатки для аналізу та створення медіа-контенту (наприклад, платформи для створення відео, інфографіки або інтерактивних презентацій, які допомагають учням на практиці опановувати навички роботи з медіа);

- соціальні мережі та блоги: ефективним інструментом для формування медіаграмотності є використання популярних серед учнів платформ (Instagram, YouTube, TikTok), де учні можуть самостійно створювати або аналізувати контент, вчитися знаходити маніпуляції або фейки;

- медіаресурси: важливо навчити школярів працювати з різними типами медіа та вміти знаходити якісну, надійну інформацію використання різних джерел інформації – новини, репортажі, документальні фільми – є важливим засобом для навчання медіаграмотності.

Таким чином, позакласна та виховна діяльність створює широкі можливості для розвитку основ медіаграмотності, формуючи у школярів вміння критично ставитися до інформації, створювати якісний контент і відповідально використовувати медіаресурси. Використання цифрових ресурсів для навчання, розваг та спілкування є необхідністю, але разом з цим виникають ризики, пов’язані з використанням Інтернету та медіа. Усвідомлене володіння медіа інструментами стає ключовим для особистісного розвитку молодого покоління.

Під час проходження педагогічної практики здобувачем освіти Конотопчиком Д. О. у закладі загальної середньої освіти «Великоглушанський ліцей» Камінь-Каширської міської ради Волинської області з учнями 10 класу був проведений виховний захід «Безпека в Інтернеті та соціальних мережах» (Додаток В).

1.3.3. Особливості формування основ інформаційної безпеки та медіаграмотності в умовах дистанційного та змішаного навчання

Дистанційне та змішане навчання вимагають особливих підходів до формування навичок інформаційної безпеки та медіаграмотності, оскільки учні значно більше часу проводять в онлайн-середовищі. Це робить їх більш вразливими до кіберзагроз і медіаманіпуляцій. Важливо навчити школярів правильно організовувати роботу з онлайн-ресурсами, уникати перевантаження інформацією та відповідально використовувати цифровий контент, дотримуючись правил безпеки та етики.

Під час дистанційного та змішаного навчання учні працюють на різних платформах та з різними програмами, тому важливо навчати їх захищати особисту інформацію, налаштовувати приватність акаунтів, використовувати двофакторну аутентифікацію та розпізнавати кіберзагрози, як-от фішинг або злом акаунтів.

Використання онлайн-платформ для навчальних відеоконференцій також вимагають знань про захист. Школярі повинні вміти правильно налаштовувати доступ до онлайн-занять, щоб уникати загроз, як-от «Zoom-бомбардування» (неналежні втручання в онлайн-уроки). Безпека у віртуальних класах – це комплекс заходів, спрямованих на захист персональних даних, забезпечення конфіденційності, а також створення комфортного і безпечного середовища для всіх учасників освітнього процесу. У віртуальних класах використовуються цифрові платформи, які відкривають можливості для навчання, але також супроводжуються потенційними ризиками.

До основних ризиків віртуальних класів можна віднести:

- несанкціонований доступ (випадкове чи навмисне проникнення сторонніх осіб у відеоконференції);
- кібератаки (використання шкідливих програм для крадіжки даних чи доступу до облікових записів);
- витік персональних даних (збирання та несанкціоноване використання

інформації про учасників навчання (імена, адреси, зображення тощо));

- поширення шкідливого контенту (випадки, коли учасники або сторонні особи розміщують неприйнятні матеріали в чатах чи на екранах);

- недотримання конфіденційності (використання записів занять без дозволу учасників).

До заходів безпеки у віртуальних класах відносимо:

- використання захищених платформ (обирати перевірені платформи з функціями шифрування даних (Zoom, Google Meet, Microsoft Teams); регулярно оновлювати програмне забезпечення для уникнення вразливостей);

- контроль доступу (використовувати паролі для входу в заняття; налаштовувати функцію «зал очікування» для перевірки учасників перед їх допуском; використовувати індивідуальні посилання для кожного заняття);

- управління ролями учасників (вчителі повинні мати адміністративний контроль над функціями, як-от вмикання/вимикання мікрофонів і камер учнів; обмежувати можливість демонстрації екрана тільки для вчителя).

- захист персональних даних (мінімізувати обмін персональною інформацією у відкритих чатах; забороняти запис занять без дозволу всіх учасників; вказувати правила конфіденційності перед початком використання платформи);

- навчання кібергігієни (проводити інструктажі для учнів і вчителів щодо базових принципів інформаційної безпеки (створення надійних паролів, розпізнавання фішингових атак, уникнення підозрілих посилань);

- моніторинг і реагування (постійно стежити за активністю в класі; мати план дій у разі порушення безпеки (видалення небажаних учасників, звернення до служби підтримки платформи).

При дистанційному та змішаному навчанні школярі часто самостійно шукають ресурси для навчання, тому важливо, щоб вони могли розпізнавати шахрайські сайти, шкідливі додатки, які можуть загрожувати їхнім пристроям і особистим даним. Однією з ключових навичок при таких формах навчання є вміння самостійно шукати, аналізувати та обробляти інформацію.

Ознаки фейкових сайтів:

- домен схожий на оригінальний, але з помилками (наприклад, *g00gle.com* замість *google.com*);
- використання незвичних доменів (.xyz, .top, .info) для обману;
- відсутність HTTPS (замок у адресному рядку), що свідчить про незахищене з'єднання;
- неякісний дизайн, орфографічні або граматичні помилки у текстах;
- неправильно працюючі посилання чи кнопки;
- надмірна кількість спливаючих вікон, банерів або посилань, які ведуть на сторонні сайти;
- пропозиції ввести паролі, дані банківських карток чи іншу конфіденційну інформацію без вагомих причин;
- використання логотипів відомих компаній із низькою якістю зображення;
- відсутність офіційних контактних даних компанії.

Ознаки фейкових додатків:

- завантаження не з офіційних магазинів (Google Play, App Store), а зі сторонніх сайтів;
- підроблені сторінки завантаження, схожі на офіційні;
- мала кількість завантажень або негативні відгуки про програму;
- нереально позитивні відгуки, створені ботами;
- додаток просить доступ до камери, мікрофона, контактів або повідомлень без очевидної необхідності;
- імітація дизайну відомих додатків, але від іншого розробника;
- наявність однакових або схожих назв, але з дрібними відмінностями;
- аномальне споживання батареї, пам'яті або інтернет-трафіку.

Учні мають розуміти, як оцінювати надійність джерел в Інтернеті, аналізувати авторитетність вебсайтів та виявляти маніпулятивні техніки. До методів розпізнавання фейкових сайтів і додатків можна віднести:

- перевірка URL (завжди перевіряйте, чи співпадає адреса з офіційним

сайтом; використовуйте інструменти, як-от *Google Safe Browsing*, для перевірки безпечності сайту);

- аналіз дозволів додатків (встановлюйте лише додатки з офіційних магазинів; читайте, які дозволи запитує додаток, і відмовляйтеся від встановлення, якщо вимоги викликають сумнів);

- використання антивірусів та блокувальників реклами (антивірусні програми допоможуть розпізнати шкідливі сайти або додатки);

- фактчекінг (перевіряйте відгуки та оцінки додатків; знаходьте офіційний сайт розробника або компанії);

- використання онлайн-ресурсів для перевірки (використовуйте сервіси для сканування сайтів).

Отже, формування інформаційної безпеки та медіаграмотності в умовах онлайн-навчання є важливим завданням у зв'язку з активним використанням цифрових платформ та інтернет-ресурсів. Дотримання простих правил та використання доступних технологічних інструментів допоможе усім учасникам освітнього процесу мінімізувати ризики.

1.4. Використання інноваційних технологій у навчанні інформаційної безпеки та медіаграмотності

Використання інтерактивних вправ є одним з найефективніших методів формування практичних навичок в області інформаційної безпеки. Такі вправи дозволяють учням не лише вивчати теоретичні питання, але й застосовувати ці знання в реальних або змодельованих ситуаціях, що імітують цифрові загрози.

Переваги інтерактивних вправ для навчання інформаційній безпеці:

1. *Реалістичні сценарії.* Інтерактивні вправи відтворюють типові загрози інформаційної безпеки, з якими учні можуть стикатися у реальному житті, такі як фішингові атаки, витоки даних, шахрайство або несанкціоновані спроби доступу до персональної інформації. Це дозволяє учням опанувати техніки протидії в умовах, наближених до реальних.

2. *Активне залучення учнів.* На відміну від пасивного споживання інформації, інтерактивні вправи стимулюють активну участь школярів у навчальному процесі. Їм потрібно приймати рішення, що вимагає критичного мислення, аналізу ситуації та застосування раніше отриманих знань.

3. *Зворотний зв'язок у реальному часі.* Платформа надає миттєвий зворотний зв'язок після виконання кожної вправи, що дозволяє учням побачити свої помилки, отримати роз'яснення та поради щодо правильних дій. Це сприяє покращенню розуміння та коригуванню поведінки під час наступних завдань.

Приклади інтерактивних вправ для формування навичок інформаційної безпеки [44]:

1. *Фішингові атаки.* Учні отримують змодельовані електронні листи, серед яких є справжні і фішингові. Їм потрібно проаналізувати листи та вирішити, які з них є спробами фішингу. Вправа допомагає школярам навчитися розпізнавати небезпечні повідомлення та уникати на них відповідей або завантаження шкідливих файлів.

2. *Налаштування конфіденційності у соціальних мережах.* У вправі учням пропонується пройти через процес налаштування конфіденційності профілю в популярних соціальних мережах. Вони вивчають, як обмежувати доступ до особистої інформації, як керувати налаштуваннями безпеки та як захищати свій акаунт від зловмисників.

3. *Аналіз даних надійності джерел.* Вправа вчить учнів оцінювати інформацію, отриману з інтернету або соціальних медіа. Учням надаються новини або статті, і вони мають визначити, чи є ці матеріали надійними, звертаючи увагу на джерело, авторство, стилістику та використані докази. Це також сприяє формуванню навичок критичного мислення.

4. *Захист від зловмисних програм.* Учням пропонується змодельоване робоче середовище, у якому вони повинні розпізнати та усунути загрози зловмисного програмного забезпечення (вірусів, троянів, шпигунських програм). Вправа може включати імітацію використання антивірусних програм та інших засобів захисту.

5. *Витік персональних даних.* У цьому сценарії школярам демонструються наслідки неналежного захисту персональних даних, і вони мають виявити джерела витоку та запропонувати ефективні рішення для запобігання подібним ситуаціям у майбутньому. Така вправа допомагає усвідомити важливість збереження конфіденційності та практичні методи захисту даних.

Алгоритм проведення інтерактивних вправ:

1. *Постановка завдання.* Учням пропонується реалістичний сценарій або ситуація, в якій потрібно вирішити проблему, пов’язану з інформаційною безпекою.

2. *Аналіз і прийняття рішення.* На цьому етапі учні аналізують ситуацію, використовують знання з інформаційної безпеки та приймають рішення щодо дій (наприклад, визначають, яке з повідомлень є фішинговим або як захистити акаунт).

3. *Виконання дій і зворотний зв’язок.* Після прийняття рішення учень отримує зворотний зв’язок: чи було рішення правильним, і які помилки були зроблені, якщо такі були.

4. *Рефлексія*. Учні мають можливість обговорити результати вправи, виявити складнощі та отримати додаткові пояснення від вчителя. Це дозволяє закріпити отримані знання та вміння.

При розробці інтерактивних завдань вчителю на допомогу можуть прийти платформи LearningApps, Kahoot!, Edmodo, Classcraft, MineTest, Wordwall, Baamboozle, які дозволяють створювати ігрові сценарії для вивчення медіаграмотності та інформаційної безпеки, що сприяє активній взаємодії учнів і вчителя та підвищує мотивацію до навчання.

Використання інноваційних технологій у вигляді інтерактивних завдань, не лише покращує якість знань, але й сприяє формуванню навичок критичного мислення, цифрової грамотності, етичного медіаспоживання, практичного застосування знань. Інтерактивні завдання для уроків інформатики на тему інформаційної безпеки та медіаграмотності подані у додатку Б.

РОЗДІЛ 2
ПРОЄКТУВАННЯ ТА РОЗРОБКА ІНТЕРАКТИВНОЇ ПЛАТФОРМИ ДЛЯ НАВЧАННЯ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ТА МЕДІАГРАМОТНОСТІ

2.1. Постановка задачі та формулювання вимог до програмного засобу

Основним завданням кваліфікаційної роботи – є розробка інтерактивної платформи, для навчання інформаційній безпеці та медіаграмотності, враховуючи зростаючі кіберзагрози та необхідність критичного сприйняття інформації. Дана платформа зможе допомогти школярам краще розуміти основи інформаційної безпеки, захисту даних, уникнення дезінформації та навчитися використовувати медіа-ресурси розумно та відповідально. Доступ до матеріалів і тестування допоможе вчителям інтегрувати навички безпечного поводження з інформацією у навчальний процес.

Веб-система проєктується та розроблюється таким чином, щоб її можна було легко використовувати різним категоріям користувачів: учням, вчителям та адміністраторам. Програмний продукт включатиме весь необхідний функціонал і буде доступним на різних пристроях, зокрема смартфонах, планшетах і комп’ютерах. Інтерфейс системи має бути адаптивним, що дозволить користувачам працювати з платформою на різних розмірах екранів.

Для створення даної інтерактивної платформи виділяються наступні етапи розробки:

- аналіз вимог (визначення освітніх потреб та вимог до інформаційної безпеки);
- проєктування концепції (розробка концептуальних рішень платформи та підготовка технічної документації);
- технічне завдання (формулювання специфікацій та затвердження функціональних вимог);
- створення прототипів (підготовка попередніх ескізів інтерфейсу);
- технічний проєкт (розробка остаточних функцій і логіки платформи);

- введення в експлуатацію (тестування, впровадження та підтримка платформи).

Вимоги до функціональності платформи:

- весь інтерфейс поділяється на основні розділи: головна сторінка з інформацією про курс, вкладки з темами лекцій, тести та контрольні завдання;
- платформа повинна швидко реагувати на дії користувача, забезпечуючи плавну і надійну взаємодію;
- система має захищати конфіденційні дані користувачів, обмежуючи доступ до особистої інформації.

Функціональні характеристики програмного продукту:

- адаптивний веб-дизайн, що підлаштовується під різні екрани;
- можливість доступу до інтерактивних лекцій, тестів та мультимедійних матеріалів з інформаційної безпеки та медіаграмотності;
- система тестування для оцінки знань учнів, а також інтегровані аудіо- та відеоматеріали.

Надійність програмного забезпечення забезпечується такими засобами:

- постійне резервне копіювання даних;
- контроль достовірності введених даних;
- відновлення системи після можливих збоїв;
- виконання вимог щодо захисту даних та конфіденційності.

Для повноцінної роботи платформи необхідний пристрій з веб-браузером і підключення до Інтернету. Підтримку платформи має забезпечувати адміністратор, який відповідає за оновлення контенту та надання технічної підтримки.

Склад документації включає:

- технічне завдання;
- інструкції для користувача та адміністратора платформи.

Розроблена інтерактивна платформа може слугувати важливим інструментом для навчання, формуючи критичне мислення та навички безпечного поводження з інформацією у цифровому середовищі. А також

повинна забезпечити глибоке розуміння ключових принципів безпеки в цифровому середовищі, а також навчити учнів розпізнавати та ефективно реагувати на загрози, які можуть виникати в інформаційному просторі. Особливий акцент робиться на підвищенні рівня критичного мислення при споживанні медіа та розвитку практичних навичок захисту персональних даних.

Завдання створення інтерактивної платформи включають:

1. Розробку навчальних модулів з основ інформаційної безпеки та медіаграмотності. Модулі повинні містити як теоретичні, так і практичні аспекти, що сприяють формуванню цілісного уявлення про інформаційні загрози та способи їх уникнення.

2. Інтерактивні вправи та симуляції, які допоможуть учням на практиці застосовувати отримані знання. Це можуть бути симуляції фішингових атак, перевірки правдивості новин, налаштування конфіденційності в соціальних мережах.

3. Розробку автоматизованої системи тестування, яка дозволить учням перевіряти рівень засвоєних знань через інтерактивні вікторини та тести. Результати тестування повинні відображати рівень медіаграмотності та знань про інформаційну безпеку учня.

4. Запровадження системи сертифікації, що дасть можливість учням отримувати сертифікати після успішного проходження всіх навчальних модулів і тестів. Це додасть мотивації до навчання та підтвердить досягнутий рівень знань.

5. Адаптація платформи для використання в дистанційному та змішаному навчанні, що дозволить школам впроваджувати її в рамках різних форм навчання. Це особливо важливо в умовах сучасної цифровізації освіти.

6. Забезпечення зручного користувацького інтерфейсу, який буде інтуїтивно зрозумілим для учнів та викладачів, сприяючи ефективному використанню платформи в навчальному процесі.

Навчальна платформа орієнтована на учнів старших класів і вчителів, які можуть використовувати її у рамках навчальних занять або самостійної роботи.

Її функціональні можливості включають:

1. *Навчальні модулі,* кожен з яких присвячений окремому аспекту інформаційної безпеки та медіаграмотності і містить:

- теоретичні матеріали у вигляді текстів, відеоуроків або інтерактивних презентацій;
- практичні вправи, які дозволяють учням застосувати знання на практиці;
- контрольні запитання для самоперевірки.

2. *Інтерактивні вправи та симуляції*. Платформа включає в себе низку інтерактивних симуляцій, які моделюють різні загрози в інформаційному середовищі, наприклад:

- симуляція фішингових атак, де учням пропонується визначити, які електронні листи є фішинговими;
- перевірка правдивості новин, де учні повинні оцінити джерело інформації та вирішити, чи є воно надійним;
- налаштування конфіденційності в соцмережах, де учні вивчають, як захистити свої дані в різних платформах.

3. *Тести та автоматизована система оцінювання.* Після завершення кожного модуля учні мають можливість пройти тестування. Система оцінює результати автоматично та надає зворотний зв’язок з роз’ясненням помилок. Це дозволяє школярам коригувати свої знання та повторювати матеріал за необхідності.

4. *Система сертифікації.* Учні, які успішно пройшли всі модулі та завершили тести, отримують електронний сертифікат про засвоєння курсу. Сертифікат підтверджує рівень знань у сфері інформаційної безпеки та медіаграмотності і може бути використаний для подальшого навчання або під час прийому на роботу.

5. *Адміністративна панель для вчителів.* Викладачі отримують доступ до адміністративної панелі, яка дозволяє:

- переглядати прогрес учнів у навчанні.
- керувати навчальними групами та призначати додаткові завдання.

- створювати власні тести або додаткові матеріали для учнів.
- оцінювати учнівські досягнення та надавати їм зворотний зв’язок.

6. *Форум та обговорення.* Платформа надає можливість для спілкування та обміну думками між учнями та вчителями. Форум дозволяє обговорювати питання, пов’язані з навчанням, ділитися ресурсами або задавати питання щодо матеріалів курсів.

Користувацький інтерфейс:

1. *Головна сторінка.* На головній сторінці користувачам надається доступ до основних функцій платформи: перегляд модулів, доступ до тестів та сертифікатів, останні повідомлення та новини курсу.

2. *Меню користувача.* Зручне та інтуїтивне меню дозволяє користувачам швидко переміщатися між навчальними модулями, тестами, сертифікатами та іншими розділами платформи. У кожного учня є персональний кабінет, де відображаються результати навчання.

3. *Адаптивний дизайн.* Платформа має адаптивний дизайн, що дозволяє використовувати її як на комп’ютері, так і на мобільних пристроях. Це особливо важливо для учнів, які можуть займатися як у школі, так і вдома.

4. *Доступність і зручність.* Інтерфейс розроблений таким чином, щоб бути зрозумілим навіть для користувачів з мінімальним досвідом роботи з інформаційними технологіями. Використання простих інструкцій, великі кнопки та логічна структура сприяють легкому навчанню.

2.2 Вибір моделі розробки програмного засобу

Для розробки освітньої інтерактивної платформи з інформаційної безпеки та медіаграмотності було обрано каскадну модель, де процес розробки проходить через наступні послідовні етапи:

1. Визначення та аналіз вимог (збір і документування вимог до платформи, аналіз потреб користувачів і специфікацій).

2. Проєктування (створення структури і функціональної моделі системи,

підготовка технічної документації).

3. Реалізація проєкту (кодування основних модулів платформи, відповідно до затвердженого проєкту).

4. Тестування (перевірка функціональності, виявлення та виправлення помилок, забезпечення відповідності вимогам).

5. Інтеграція та підтримка (впровадження готового продукту, а також підтримка та оновлення системи після запуску).

Основний принцип каскадної моделі полягає у тому, що кожен етап завершується перед початком наступного, що забезпечує систематичний та контрольований процес розробки. Особливістю каскадної моделі є те, що повернення до попередніх етапів є обмеженим, тому вона краще підходить для проєктів зі стабільними, чітко визначеними вимогами, які не змінюються у процесі розробки. Схема каскадної моделі представлена на рисунку 2.1.

Рисунок 2.1. Візуальна схема каскадної моделі розробки

На першому етапі були визначені вимоги до функціональних та

нефункціональних характеристик платформи, що включає адаптивність інтерфейсу, швидкість реакції системи та вимоги безпеки даних.

На етапі «Проєктування» було розроблено план побудови платформи, створено архітектурні рішення та документацію, що описує основні елементи системи і зв’язки між ними.

На етапі реалізації відбулося кодування, під час якого створено модулі курсу, інтерактивні лекційні матеріали та систему тестування.

Етап тестування включав перевірку функціональних можливостей платформи на відповідність технічним вимогам. Було проведено багаторівневе тестування: від модульного тестування кожного компонента до інтеграційного тестування всієї платформи.

Завершальний етап – інтеграція та підтримка, де програмний продукт був введений у дію, надано доступ користувачам, а також розроблені інструкції з експлуатації для адміністраторів та користувачів.

Переваги каскадної моделі:

- простота та зручність – модель легка для розуміння і застосування завдяки послідовності етапів;
- стабільність вимог – дозволяє ретельно опрацювати вимоги перед початком розробки;
- контрольованість процесу – чітка структура дає змогу легко керувати проєктом;
- прогнозованість витрат – визначення бюджету та ресурсів на початковому етапі.

Недоліки каскадної моделі:

- пізнє тестування – перевірка функціональності починається на останніх етапах, що може ускладнити виявлення проблем;
- обмежена гнучкість – замовник бачить кінцевий продукт тільки після завершення розробки, що обмежує можливість внесення змін;
- великий обсяг документації – необхідність у написанні детальної документації може сповільнити процес розробки.

Використання каскадної моделі вимагає детального та структурованого опису вимог на початковому етапі, що є критичним для успішної реалізації проєкту. Цей підхід дозволяє забезпечити стабільний і контрольований процес розробки платформи для контролю знань в області інформаційної безпеки та медіаграмотності.

2.3 Опис проєкту

Перед початком розробки інтерактивної платформи було проведено детальний аналіз і проєктування етапів створення платформи з інтерактивними завданнями з інформаційної безпеки та медіаграмотності. Основна увага зосереджена на визначенні архітектури системи, ключовими компонентами якої є хостинг на GitHub Pages та клієнтська частина.

Серверна частина реалізована через хостинг на GitHub Pages, що забезпечує надійне та безкоштовне розміщення статичного веб-сайту. Цей підхід дозволяє легко оновлювати контент через систему контролю версій Git та забезпечує стабільний доступ до платформи. GitHub Pages також надає SSL-сертифікат для безпечного з’єднання через HTTPS.

Клієнтська частина формуватиме інтерфейс у вигляді веб-сторінок та розроблена з використанням сучасних веб-технологій, таких як HTML5, CSS3 і JavaScript, що забезпечує адаптивний та інтуїтивно зрозумілий інтерфейс.

Для покращення користувацького досвіду застосовано принципи responsive design, що дозволяє комфортно працювати з платформою на різних пристроях – від смартфонів до десктопних комп’ютерів.

Діаграми послідовностей – ілюструють послідовність взаємодій між об’єктами системи, показуючи, як різні компоненти реагують на запити користувачів (рис. 2.2).

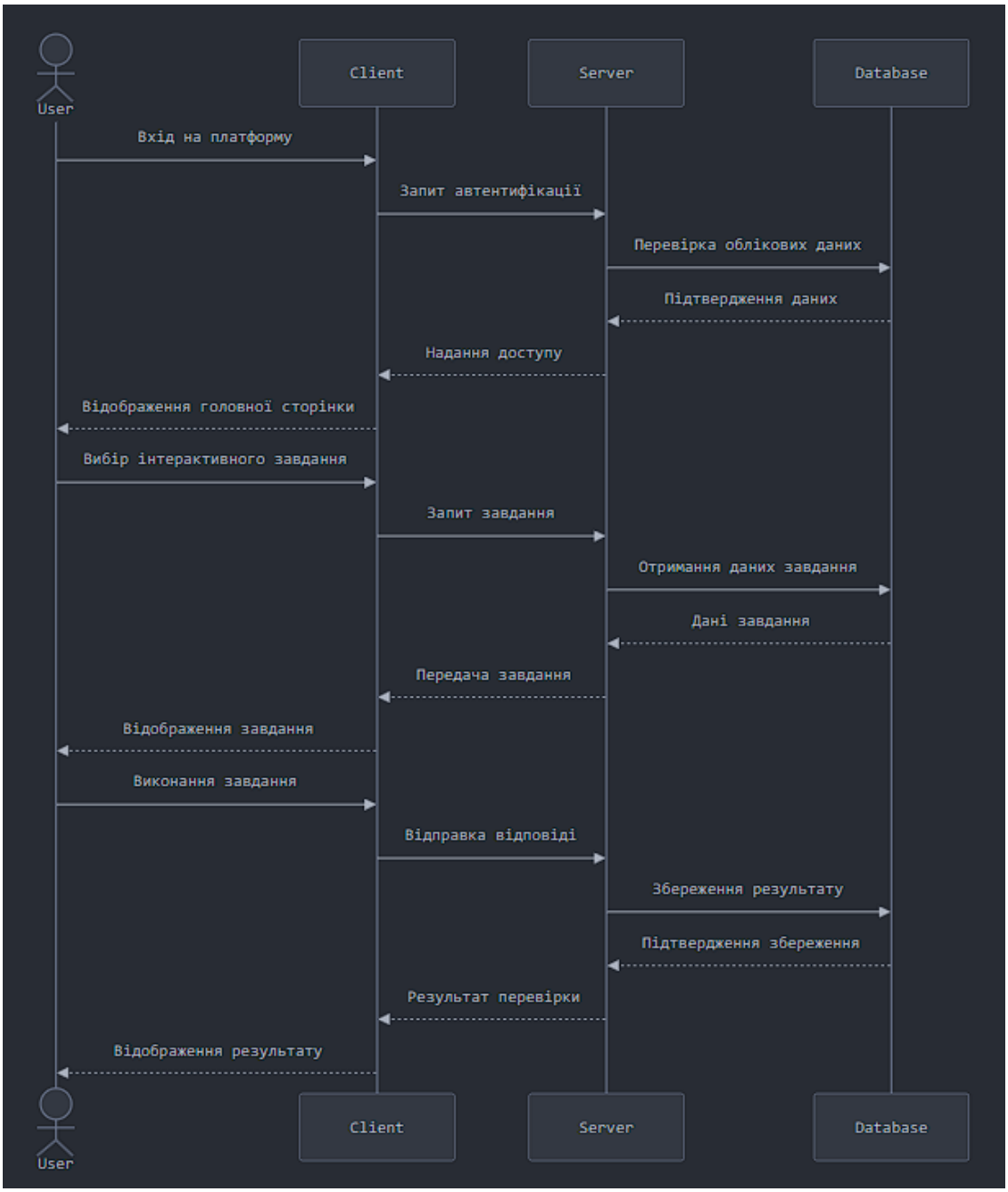


Рисунок 2.2. Діаграма послідовностей

Діаграми варіантів використання – це графічне представлення взаємодії між користувачами (акторами) та системою, яке визначає основні функціональні можливості через демонстрацію доступних операцій без деталізації їх технічної реалізації, що дозволяє спростити розуміння системи для всіх зацікавлених сторін та встановити чіткі межі її функціональності на ранніх етапах розробки. (рис. 2.3).

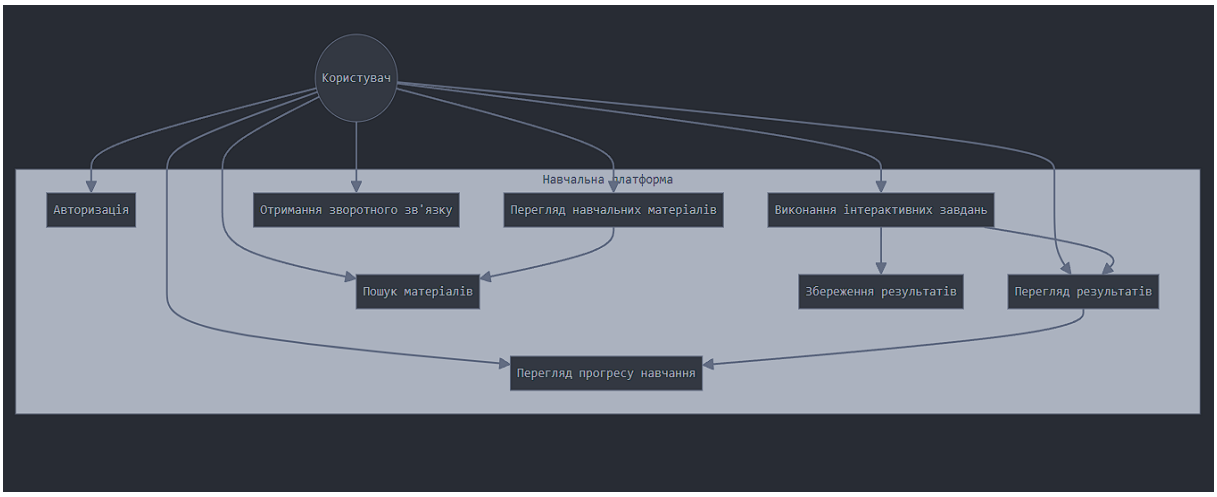


Рисунок 2.3. Діаграми варіантів використання

Обираючи архітектуру, було вирішено використовувати просту та зрозумілу модель клієнт-сервер, яка оптимально підходить для веб-системи. Основною перевагою клієнт-серверної моделі є чітке розділення функцій між клієнтською та серверною частинами, що дозволяє зменшити обчислювальне навантаження.

Клієнтська частина системи складається з веб-сторінок, які забезпечують зручний та інтерактивний інтерфейс для користувачів. Вона буде реалізована з використанням HTML, CSS, JavaScript.

Серверна частина відповідатиме за обробку даних та доступ до бази даних, реалізовуючи бізнес-логіку платформи. Вона буде розроблена таким чином, щоб спрощувати взаємодію з клієнтською частиною і забезпечувати користувачів актуальною інформацією.

Варіанти прецедентів описують можливі сценарії взаємодії між користувачами та системою, допомагаючи досягати конкретних результатів. Для створення якісних варіантів прецедентів використовувалися такі принципи:

- наявність хоча б одного суб’єкта;
- визначення ініціатора процесу;
- досягнення чіткого результату для кожного сценарію.

Користувач, взаємодіє з усіма варіантами прецедентів. Модель також включає асоціації, що відповідають за напрямки передачі інформації між

користувачем та сценаріями використання.

2.4 Обґрунтування вибору засобів розробки програмного засобу

Для реалізації проєкту було обрано класичний стек веб-технологій: HTML, CSS та JavaScript, без використання додаткових фреймворків чи систем керування контентом.

HTML (HyperText Markup Language) використовується, як основна мова розмітки для створення структури веб-сторінок. Це стандартна технологія, яка забезпечує базову структуру контенту та його семантичну організацію. HTML5, остання версія стандарту, надає розширені можливості для створення сучасних веб-інтерфейсів.

CSS (Cascading Style Sheets) відповідає за візуальне оформлення веб-сторінок. За допомогою CSS реалізовано адаптивний дизайн, який забезпечує коректне відображення сайту на різних пристроях.

Використання CSS дозволяє:

- створювати привабливий користувацький інтерфейс;
- забезпечувати адаптивність під різні розміри екранів;
- налаштовувати анімації та переходи;
- підтримувати консистентний стиль across the application.

JavaScript використовується для створення інтерактивної функціональності на стороні клієнта. За допомогою JavaScript реалізовано:

- обробку користувацьких дій;
- валідацію форм;
- динамічне оновлення контенту;
- взаємодію з сервером через AJAX-запити.

Бази даних у даному проєкті не використовувались для забезпечення безпеки та оптимізацій продукту. Всі дії виконуються на стороні користувача. Це зменшує навантаження на сервер і запобігає збору будь якої інформацій про користувачів даного сайту (що забезпечує користувачам безпечне користування

та анонімність).

Переваги обраного підходу:

- повний контроль над кодом та архітектурою;
- відсутність зайвих залежностей та overhead від фреймворків;
- висока продуктивність завдяки оптимізованому коду;
- простота розгортання та обслуговування;
- легкість внесення змін та масштабування.

Архітектура проєкту побудована за принципом розділення відповідальності:

- HTML відповідає за структуру контенту;
- CSS керує відображенням;
- JavaScript забезпечує інтерактивність.

Запропонована архітектура дозволяє ефективно розробляти та підтримувати проєкт, забезпечуючи при цьому високу продуктивність та хороший користувацький досвід.

Для розробки було обрано саме такий підхід, оскільки проєкт не потребує складної функціональності, яку надають фреймворки. Натомість, важливими були такі фактори:

- швидкість завантаження сторінок;
- простота підтримки;
- мінімальні системні вимоги;
- легкість розгортання;
- прозорість роботи усіх компонентів.

Цей вибір дозволив створити легкий та ефективний веб-ресурс, який повністю відповідає поставленим вимогам та забезпечує необхідну функціональність для навчальної інтерактивної платформи.

2.5 Програмна реалізація та її особливості

Для реалізації навчальної платформи було розроблено власний веб-сайт, який не використовує готові фреймворки чи системи керування вмістом. Натомість, застосовано класичний підхід на основі HTML, CSS та JavaScript.

Загальна структура сайту складається з таких основних компонентів:

HTML структура: для розмітки сторінок використовується семантичний HTML5, який забезпечує чітку організацію контенту. Наприклад, для створення головної сторінки застосовується наступна структура:

– <!DOCTYPE html>
– <html lang=«uk»>
– <head>
– <meta charset=«UTF-8»>
– <meta name=«viewport» content=«width=device-width, initial-scale=1.0»>
– <title>Навчальна платформа</title>
– <link rel=«stylesheet» href=«styles.css»>
– </head>
– <body>
– <header>
–
– <h1>Ласкаво просимо на навчальну платформу</h1>
– Отримайте знання з медіаграмотності та інформаційної безпеки
–
– <nav>
–
Головна
Курс
Контакти
–
– </nav>

– </header>

– <main>

– <h2>Про платформу</h2>

– <section id=«about»>

– Наша платформа надає можливість учням оволодіти важливими навичками в галузі інформаційної безпеки та медіаграмотності. Ці навички є невід’ємною частиною сучасної освіти та допомагають учням ефективно орієнтуватися у світі інформаційних технологій, забезпечуючи їх захист від можливих загроз і розвиток критичного мислення.

– Ми пропонуємо інтерактивні курси, тести та навчальні матеріали, які дозволяють засвоїти знання у зручному та доступному форматі. Долучайтеся до нас, щоб стати компетентними користувачами цифрових технологій!

– </section>

– </main>

– <footer id=«contact»>

– <h2>Контакти</h2>

– Email: dimakonotop0000@gmail.com

– <b> >>>>>>>>>_Telegram_<<<<<<<<<

– © 2024 Навчальна платформа

– </footer>

– <script>

– // Видалення даних з локального сховища після входу

– if (localStorage) {

– localStorage.clear(); // Очищає все дані в локальному сховищі

– console.log(«Дані локального сховища видалено.»);

– }

– </script>

– </body>

– </html>

CSS стилізація: Візуальне оформлення сайту реалізовано за допомогою каскадних таблиць стилів. Наприклад, для створення адаптивного та загального дизайну сторінки застосовано CSS-змінні та медіа-запити:

– /* Основні стилі */

– *{ margin: 0; padding: 0; box-sizing: border-box; }

– html, body {

– height: 100%; font-family: Arial, sans-serif; background: #f4f4f4; color: #333; min-width: 100%; position: relative;

– display: flex; flex-direction: column; justify-content: space-between;}

– header, footer {

– padding: 15px 0; color: white; text-align: center; flex-shrink: 0;}

– header { background: #4CAF50; font-size: 1.5rem; }

– footer { background: #333; font-size: 1rem; }

– main {

– padding: 20px; max-width: 1200px; margin: 0 auto; flex-grow: 1; display: flex; flex-direction: column; align-items: center; justify-content: center;}

– /* Навігація */

– nav ul {

– list-style: none; display: flex; flex-wrap: wrap; justify-content: center; padding: 0; line-height: 1.9;}

– nav ul li { margin: 5px 10px; }

– nav ul li a {

– color: white; background: #333; padding: 1px 10px; border-radius: 10px; text-decoration: none;}

– nav ul li a:hover { background: #555; }

– /* Контент */

– h1, h2, h3 { text-align: center; margin: 10px 0 20px; }

– .section { margin: 0 10% 1%; cursor: pointer; }

– .container { width: 90%; max-width: 90%; margin: auto; padding: 20px; }

– p { margin: 0; text-indent: 3ch; }

– p.pilcrow { text-indent: 0; display: inline; }

– p.pilcrow + p.pilcrow::before { content: « ¶ «; }

– /* Кнопки */

– .btn, .prev-button, .next-button {

– padding: 10px 20px; background: #4CAF50; color: white; border: none; border-radius: 5px; text-align: center; text-decoration: none; cursor: pointer;}

– .btn:hover, .prev-button:hover, .next-button:hover { background: #45a049; }

– .header-content .btn, .registration-container button { background: #007bff; }

– .header-content .btn:hover, .registration-container button:hover { background: #0056b3; }

– /* Курси */

– #courses {

– display: grid; grid-template-columns: repeat(auto-fit, minmax(250px, 1fr)); gap: 20px; width: 100%;}

– .course {

– background: white; padding: 15px; border-radius: 5px; box-shadow: 0 0 5px rgba(0, 0, 0, 0.1); transition: transform 0.2s; text-align: center;}

– .course:hover { transform: scale(1.05); }

– /* Контейнер реєстрації */

– .registration-container, .course-container {

– width: 90%; max-width: 300px; text-align: center; padding: 20px; background: #fff; border-radius: 8px; box-shadow: 0 4px 8px rgba(0, 0, 0, 0.1);}

– .registration-container input[type=«text»] {

– padding: 10px; width: 100%; margin-top: 10px; font-size: 16px; border: 1px solid #ced4da; border-radius: 4px;}

– /* Відео */

– #video-container { display: flex; justify-content: center; width: 100%; max-width: 1200px; margin: auto; }

– .video-frame { width: 100%; height: 500px; display: flex; justify-content: center;}

```
– /* Адаптивність */
– @media (max-width: 375px) {
– header { font-size: 1.1rem; }
– .header-content h1 { font-size: 1.5rem; }
– .btn { padding: 8px 15px; font-size: 0.9rem; }
– .registration-container, .course-container { width: 95%; }
– nav ul li a { padding: 8px 15px; font-size: 0.9rem; }
– .section { margin: 0 1%; }}
– @media (max-width: 768px) {
– nav ul { flex-direction: column; align-items: center; }
– nav ul li { margin-bottom: 10px; }
– #courses { grid-template-columns: 1fr; }
– .video-frame { height: 300px; }}
– @media (min-width: 769px) {
– #courses { grid-template-columns: repeat(2, 1fr); gap: 20px; }}
```

JavaScript інтерактивність: Динамічна функціональність сайту забезпечується за допомогою JavaScript. Наприклад, реалізація обробки результатів тестування:

```
– <script>
– function submitQuiz() {
–     const answers = {
– question1: «B», question2: «A», question3: «B», question4: «B»,
– question5: «B», question6: «B»,  question7: «B», question8: «B»,
– question9: «B», question10: «A», question11: «B», question12: «B»,
– question13: «B»,
– question13: «B», question14: «B»,question15: «B»,question16: «B»,
– question17: «C», question18: «B», question19: «B», question20: «B»,};
–  let score = 0;
–  let allAnswered = true;
–  for (const question in answers) {
```

– const selectedOption = document.querySelector(`input[name=«${question}»]:checked`);

– if (selectedOption) {

– if (selectedOption.value === answers[question]) {

– score += 1;

– } }

– else { allAnswered = false;

– alert(`Будь ласка, виберіть відповідь на питання ${question.slice(-1)}.`);

– break;

– }}

– if (allAnswered) {

– // Зберігаємо бали для тесту в окремій комірці

– localStorage.setItem('testScore', score.toString());

– // Показуємо повідомлення про успішне збереження

– alert(«Ваші бали збережено: « + score + «!»);

– // Перевіряємо, чи бали більше або дорівнюють 10

– if (score >= 10) {

– // Перенаправляємо на іншу сторінку, якщо бали достатні

– window.location.href = «./sertef.html»;}

– else {

– alert(«Вам потрібно набрати 10 або більше балів, щоб пройти тест.»);

– // Перенаправляємо на сторінку з результатами тесту

– window.location.href = «../course-details.html»; // Замість «./fail.html» використайте правильну URL

– }}}

– </script>використайте правильну URL

– }}

Особливості реалізації:

- висока продуктивність: завдяки відсутності додаткових залежностей від

фреймворків та оптимізованому коду, сайт характеризується швидким завантаженням сторінок та миттєвою реакцією на дії користувача;

- гнучкість та масштабованість: власна реалізація на базових веб-технологіях спрощує внесення змін, додавання нового функціоналу та масштабування системи у разі зростання навантаження (наприклад, нові навчальні матеріали можуть бути легко додані шляхом оновлення HTML-розмітки);

- прозорість архітектури: чітке розділення обов'язків між HTML, CSS та JavaScript забезпечує високу прозорість роботи всіх компонентів системи, що полегшує розробку, налагодження та підтримку проєкту;

- мінімальні системні вимоги: відсутність важких фреймворків та бібліотек дозволяє розгортати платформу навіть на обмежених апаратних ресурсах, що розширює коло потенційних користувачів.

Таким чином, обраний підхід до реалізації інтерактивної платформи, заснований на базових веб-технологіях, забезпечує високу продуктивність, гнучкість та легкість обслуговування системи, що відповідає поставленим вимогам до проєкту.

2.6. Тестування та налагодження програмного засобу

На кожному етапі розробки програмного засобу можуть виникати помилки. Їх причинами можуть бути: неправильне розуміння вимог, неякісно складені специфікації, недоліки у проєктуванні, помилки у коді або неточності у логіці роботи. Найбільше впливають помилки на початкових етапах, тому тестування та налагодження програми є критично важливими для забезпечення її працездатності.

Тестування та налагодження – це ретельний процес, у ході якого перевіряється робота кожного модуля та передача управління між ними. Для цього застосовується структуроване програмування із чітко визначеними контролюючими структурами та структурами даних. Кожен модуль тестується

окремо для перевірки відповідності специфікаціям, а також перевіряються всі можливі інформаційні потоки та операції для забезпечення коректності виконання алгоритмів.

Під час тестування програмного забезпечення було виконано наступні кроки:

Тест на точність – перевірка відповідності функціоналу програмного засобу вимогам замовника, зазначеним у специфікаціях.

Перевірка конфігурації – забезпечення коректного створення та структурування всіх елементів програмного засобу для підтримки його впродовж життєвого циклу.

Тест на відновлення – перевірка здатності відновлення програмного забезпечення після збою або кібератаки.

Стрес-тести – тестування стійкості системи до нештатних дій користувачів.

Тест на продуктивність – оцінка швидкодії та ефективності роботи програмного забезпечення.

Для підвищення зручності користування було проведено тестування юзабіліті (Usability Testing), яке включало:

- функціональне тестування;
- тестування посилань;
- навігаційне тестування;
- тестування контенту;
- тестування інтерфейсу користувача;
- тестування сумісності;
- кросплатформенне тестування;
- кросбраузерне тестування;
- оптимізацію зображень;
- бета-тестування.

Налагодження є завершальним етапом, який забезпечує стабільну та безперебійну роботу програмного засобу.

2.7. Особливості використання та впровадження програмного засобу

Після того, як програмне забезпечення успішно пройшло всі етапи тестування, воно повністю готове до використання.

На головній сторінці користувачам надається доступ до основних функцій платформи. У верхній частині розташоване меню навігації, яке забезпечує швидкий перехід між розділами. Центральна частина сторінки містить короткий опис платформи, її можливості та переваги, а також інформацію про автора проєкту.

Інтерфейс розроблено з акцентом на простоту та зручність, що робить його інтуїтивно зрозумілим для учнів та вчителів.

Веб дизайн враховує потреби різних пристроїв, включаючи смартфони, планшети та комп’ютери, забезпечуючи адаптивне відображення. Це сприяє ефективному доступу до ресурсу та його використанню у навчальному процесі. (рис. 2.4).

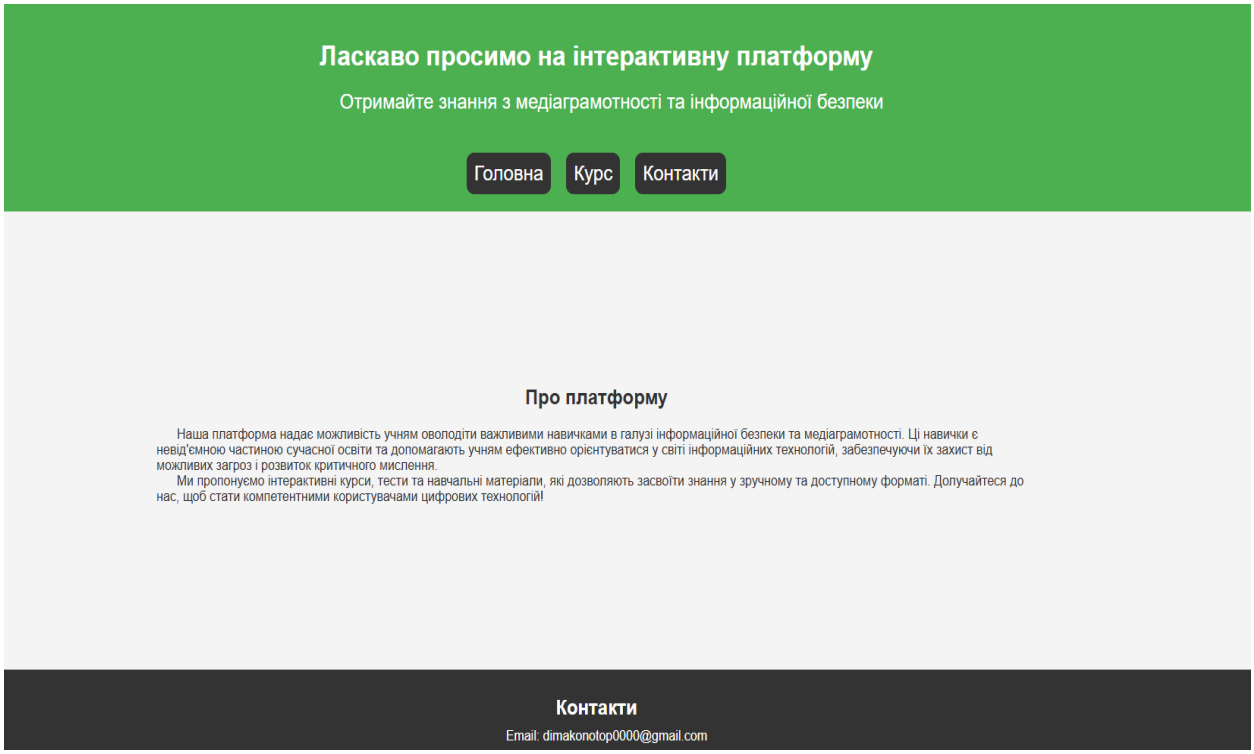


Рисунок 2.4. Головна сторінка розробленої інтерактивної платформи

Натиснувши вкладку «Курс» користувачі мають змогу познайомитись з особливостями проходження курсу, його цілями, модулями та форматом (рис. 2.5).

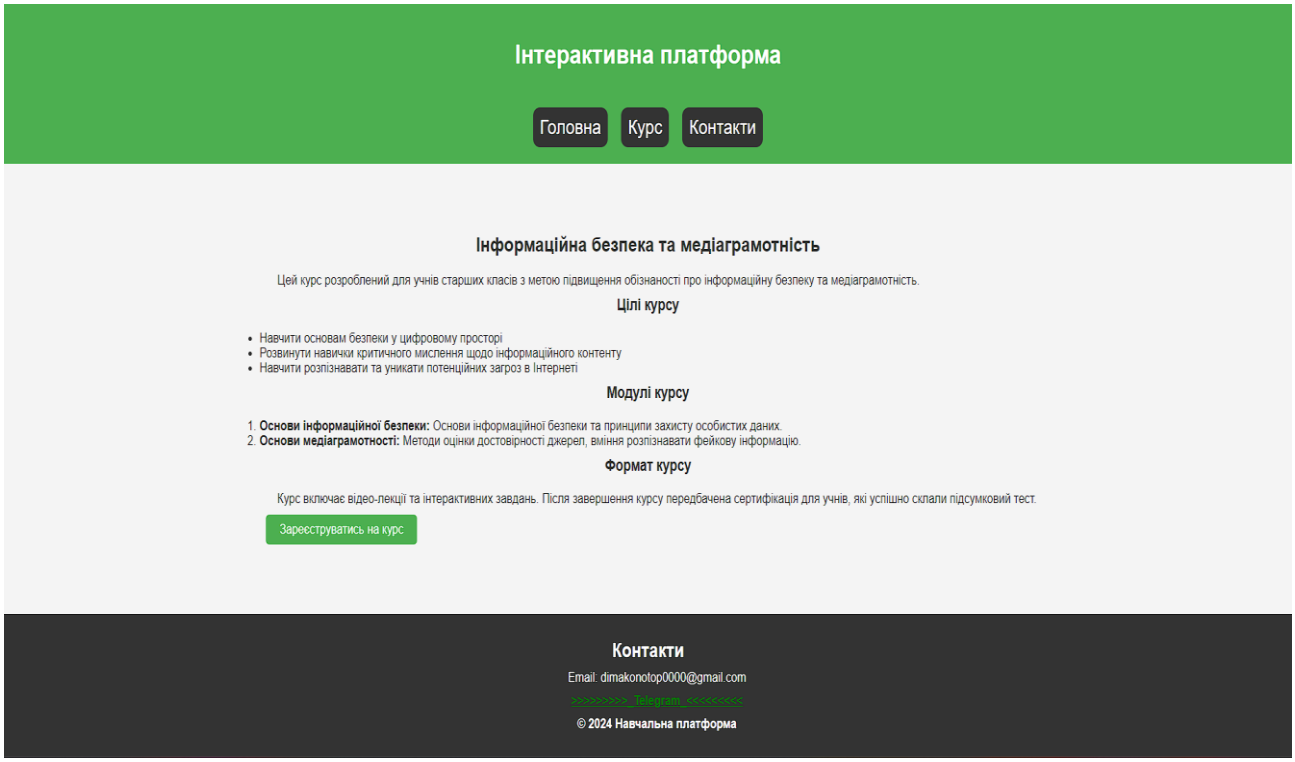


Рисунок 2.5. Інформаційна сторінка розробленої інтерактивної платформи

На сторінці реєстрації на курс пропонується ввести ім’я, яке буде використано у сертифікаті. Поле для введення імені забезпечує правильність форматування, зокрема автоматичне виправлення першої літери на велику.

Простий та зрозумілий інтерфейс форми гарантує, що користувачі не витрачатимуть зайвого часу на заповнення.

Після введення імені, користувач переходить до наступного кроку реєстрації, підтверджуючи готовність до навчання. Уся інформація обробляється конфіденційно, забезпечуючи захист персональних даних відповідно до вимог безпеки (рис. 2.6).

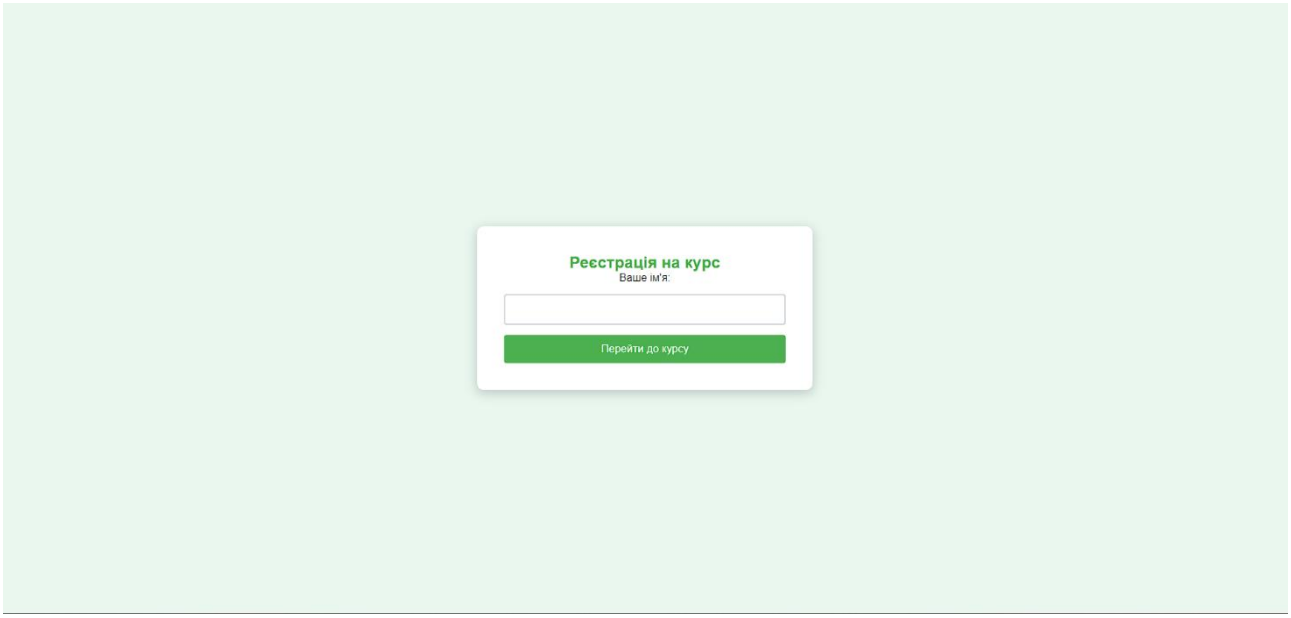


Рисунок 2.6. Сторінка реєстрації на курс

Сторінка курсу, яка використовується для навігацій, включає вкладки проходження теоретичного матеріалу, інтерактивних завдань та фінальний заліковий тест (рис. 2.7).

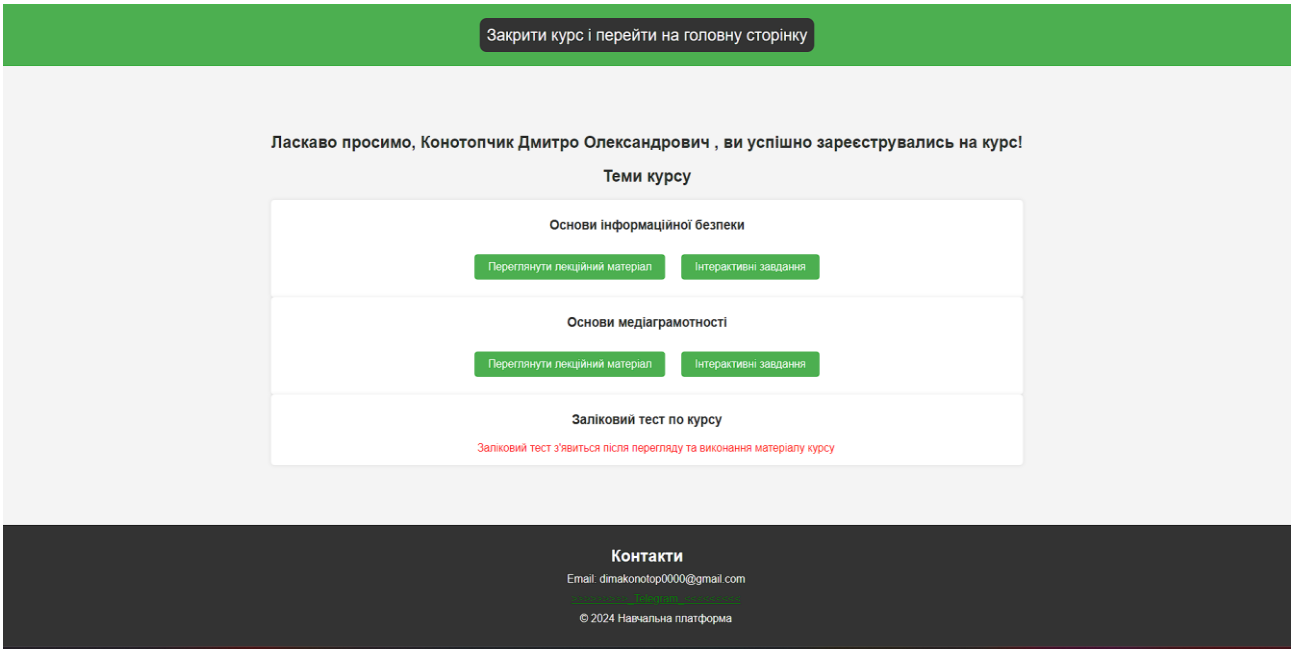
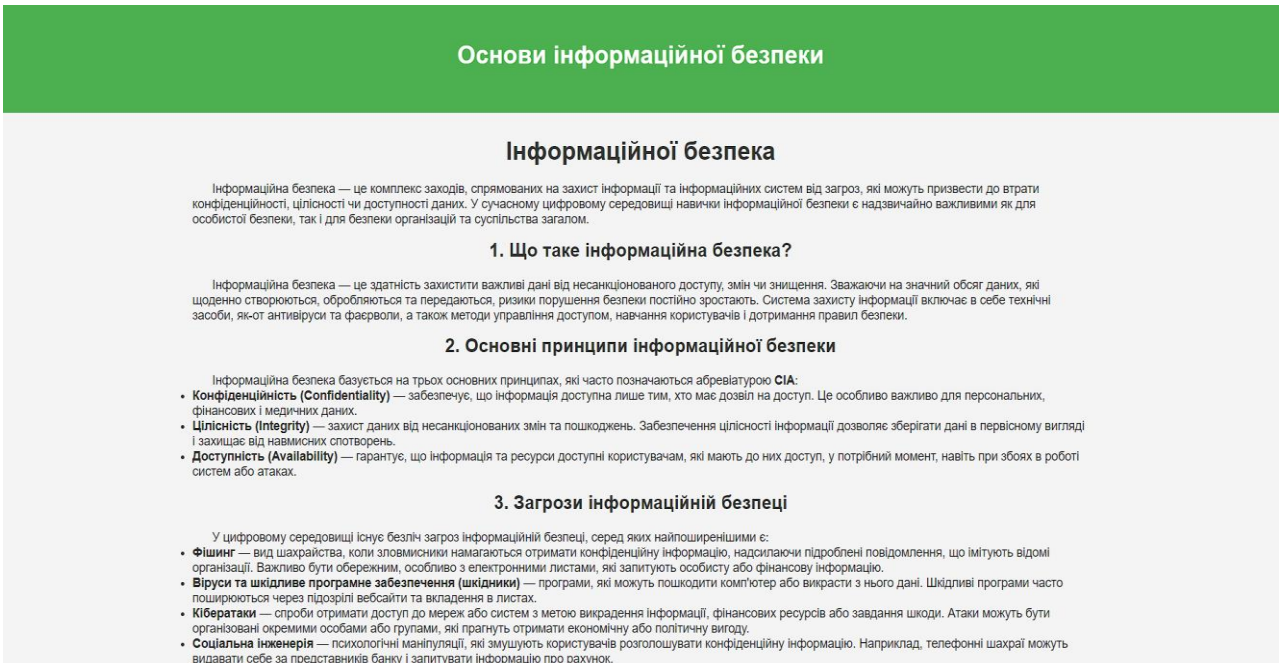


Рисунок 2.7. Сторінка курсу

Сторінка теоретичних матеріалів складається з короткого опису курсу та відеороликів. На рисунках 2.8 і 2.9 показано опис курсів «Основи інформаційної

безпеки» і «Медіаграмотність».



Основи інформаційної безпеки

Інформаційної безпека

Інформаційна безпека — це комплекс заходів, спрямованих на захист інформації та інформаційних систем від загроз, які можуть призвести до втрати конфіденційності, цілісності чи доступності даних. У сучасному цифровому середовищі навички інформаційної безпеки є надзвичайно важливими як для особистої безпеки, так і для безпеки організацій та суспільства загалом.

1. Що таке інформаційна безпека?

Інформаційна безпека — це здатність захистити важливі дані від несанкціонованого доступу, змін чи знищення. Зважаючи на значний обсяг даних, які щоденно створюються, обробляються та передаються, ризики порушення безпеки постійно зростають. Система захисту інформації включає в себе технічні засоби, як-от антивіруси та фаєрволи, а також методи управління доступом, навчання користувачів і дотримання правил безпеки.

2. Основні принципи інформаційної безпеки

Інформаційна безпека базується на трьох основних принципах, які часто позначаються абревіатурою **CIA**:

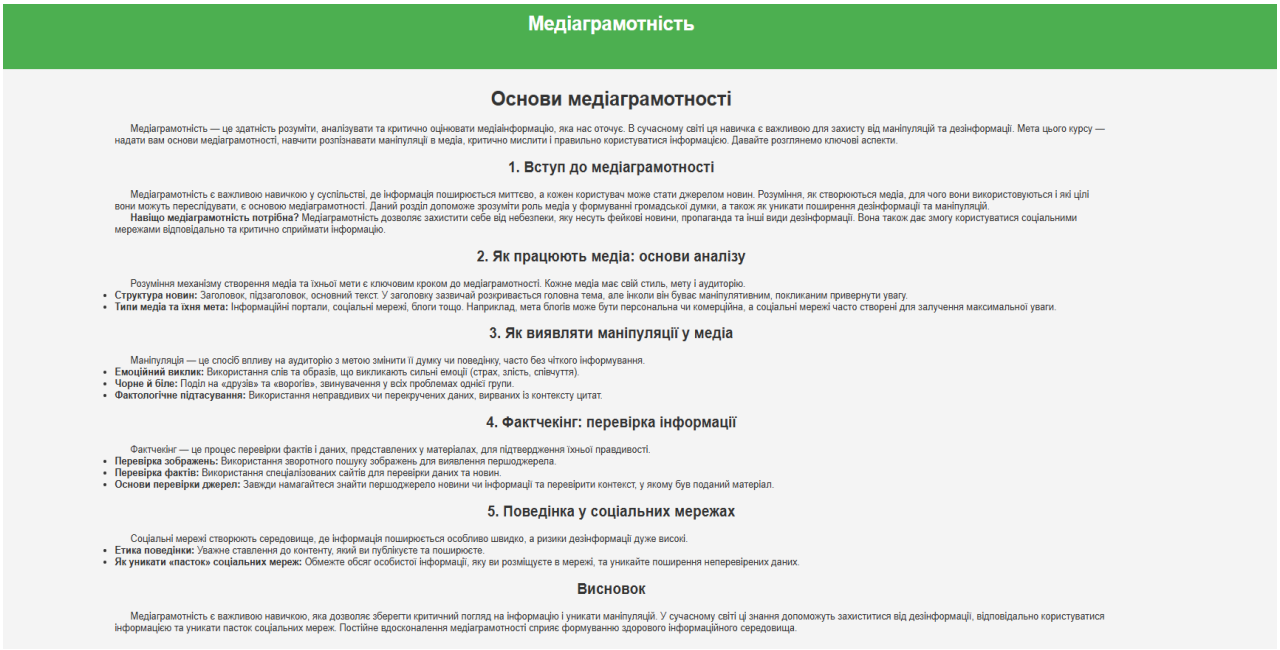
- **Конфіденційність (Confidentiality)** — забезпечує, що інформація доступна лише тим, хто має дозвіл на доступ. Це особливо важливо для персональних, фінансових і медичних даних.
- **Цілісність (Integrity)** — захист даних від несанкціонованих змін та пошкоджень. Забезпечення цілісності інформації дозволяє зберігати дані в первісному вигляді і захищає від навмисних спотворень.
- **Доступність (Availability)** — гарантує, що інформація та ресурси доступні користувачам, які мають до них доступ, у потрібний момент, навіть при збоях в роботі систем або атаках.

3. Загрози інформаційній безпеці

У цифровому середовищі існує безліч загроз інформаційній безпеці, серед яких найпоширенішими є:

- **Фішинг** — вид шахрайства, коли зловмисники намагаються отримати конфіденційну інформацію, надсилаючи підроблені повідомлення, що імітують відомі організації. Важливо бути обережним, особливо з електронними листами, які запитують особисту або фінансову інформацію.
- **Віруси та шкідливе програмне забезпечення (шкідники)** — програми, які можуть пошкодити комп'ютер або викрасти з нього дані. Шкідливі програми часто поширюються через підозрілі вебсайти та вкладення в листах.
- **Кібератаки** — спроби отримати доступ до мереж або систем з метою викрадення інформації, фінансових ресурсів або завдання шкоди. Атаки можуть бути організовані окремими особами або групами, які прагнуть отримати економічну або політичну вигоду.
- **Соціальна інженерія** — психологічні маніпуляції, які змушують користувачів розголошувати конфіденційну інформацію. Наприклад, телефонні шахраї можуть видавати себе за представників банку і запитувати інформацію про рахунок.

Рисунок 2.8. Опис курсу «Основи інформаційної безпеки»



Медіаграмотність

Основи медіаграмотності

Медіаграмотність — це здатність розуміти, аналізувати та критично оцінювати медіаінформацію, яка нас оточує. В сучасному світі ця навичка є важливою для захисту від маніпуляцій та дезінформації. Мета цього курсу — надати вам основи медіаграмотності, навчити розпізнавати маніпуляції в медіа, критично мислити і правильно користуватися інформацією. Давайте розглянемо ключові аспекти.

1. Вступ до медіаграмотності

Медіаграмотність є важливою навичкою у суспільстві, де інформація поширюється миттєво, а кожен користувач може стати джерелом новин. Розуміння, як створюються медіа, для чого вони використовуються і які цілі вони можуть переслідувати, є основою медіаграмотності. Даний розділ допоможе зрозуміти роль медіа у формуванні громадської думки, а також як уникати поширення дезінформації та маніпуляцій.

Навіщо медіаграмотність потрібна? Медіаграмотність дозволяє захистити себе від небезпеки, яку несуть фейкові новини, пропаганда та інші види дезінформації. Вона також дає змогу користуватися соціальними мережами відповідально та критично сприймати інформацію.

2. Як працюють медіа: основи аналізу

Розуміння механізму створення медіа та їхньої мети є ключовим кроком до медіаграмотності. Кожне медіа має свій стиль, мету і аудиторію.

- **Структура новин:** Заголовок, підзаголовок, основний текст. У заголовку зазвичай розкривається головна тема, але інколи він буває маніпулятивним, покликаним привернути увагу.
- **Типи медіа та їхня мета:** Інформаційні портали, соціальні мережі, блоги тощо. Наприклад, мета блогів може бути персональна чи комерційна, а соціальні мережі часто створені для залучення максимальної уваги.

3. Як виявляти маніпуляції у медіа

Маніпуляція — це спосіб впливу на аудиторію з метою змінити її думку чи поведінку, часто без чіткого інформування.

- **Емоційний виклик:** Використання слів та образів, що викликають сильні емоції (страх, злість, співчуття).
- **Чорне й біле:** Поділ на «друзів» та «ворогів», звинувачення у всіх проблемах однієї групи.
- **Фактологічне підтасування:** Використання неправдивих чи перекручених даних, вирваних із контексту цитат.

4. Фактчекінг: перевірка інформації

Фактчекінг — це процес перевірки фактів і даних, представлених у матеріалах, для підтвердження їхньої правдивості.

- **Перевірка зображень:** Використання зворотного пошуку зображень для виявлення першоджерела.
- **Перевірка фактів:** Використання спеціалізованих сайтів для перевірки даних та новин.
- **Основи перевірки джерел:** Завжди намагайтеся знайти першоджерело новини чи інформації та перевірити контекст, у якому був поданий матеріал.

5. Поведінка у соціальних мережах

Соціальні мережі створюють середовище, де інформація поширюється особливо швидко, а ризики дезінформації дуже високі.

- **Етика поведінки:** Уважне ставлення до контенту, який ви публікуєте та поширюєте.
- **Як уникати «пасток» соціальних мереж:** Обмежте обсяг особистої інформації, яку ви розміщуєте в мережі, та уникайте поширення неперевірених даних.

Висновок

Медіаграмотність є важливою навичкою, яка дозволяє зберегти критичний погляд на інформацію і уникати маніпуляцій. У сучасному світі ці знання допоможуть захиститися від дезінформації, відповідально користуватися інформацією та уникати пасток соціальних мереж. Постійне вдосконалення медіаграмотності сприяє формуванню здорового інформаційного середовища.

Рисунок 2.9. Опис курсу «Медіаграмотність»

Для проходження курсів і отримання сертифікату користувачі мають можливість переглянути відеоролики з відповідної тематики. На рисунку 2.10 показано сторінку з відеороликом «Основи інформаційної безпеки».

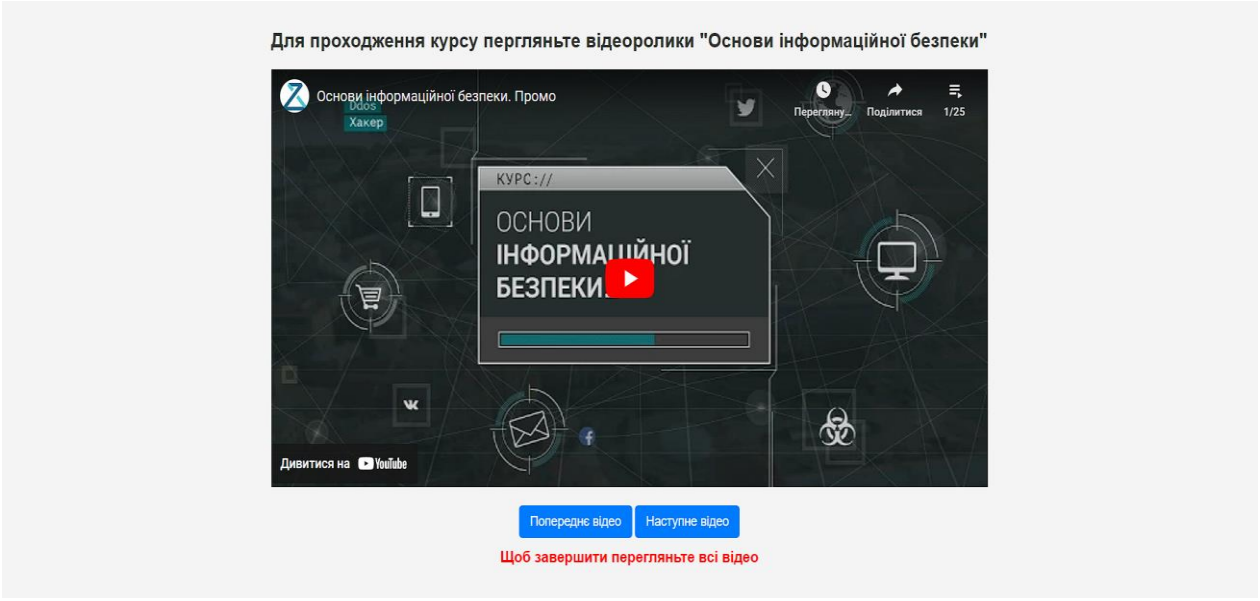


Рисунок 2.10. Сторінка з відеороликом «Основи інформаційної безпеки»

Окрім теоретичного матеріалу користувачі мають можливість виконання інтерактивних завдань, що підвищує їх практичні навички (рис.2.11, рис.2.12). Завдання такого типу перетворюють процес навчання на цікаву гру, яка водночас готує учнів до реальних викликів цифрового світу. Учні краще запам’ятовують інформацію, коли вони залучені до процесу і можуть застосовувати знання на практиці.

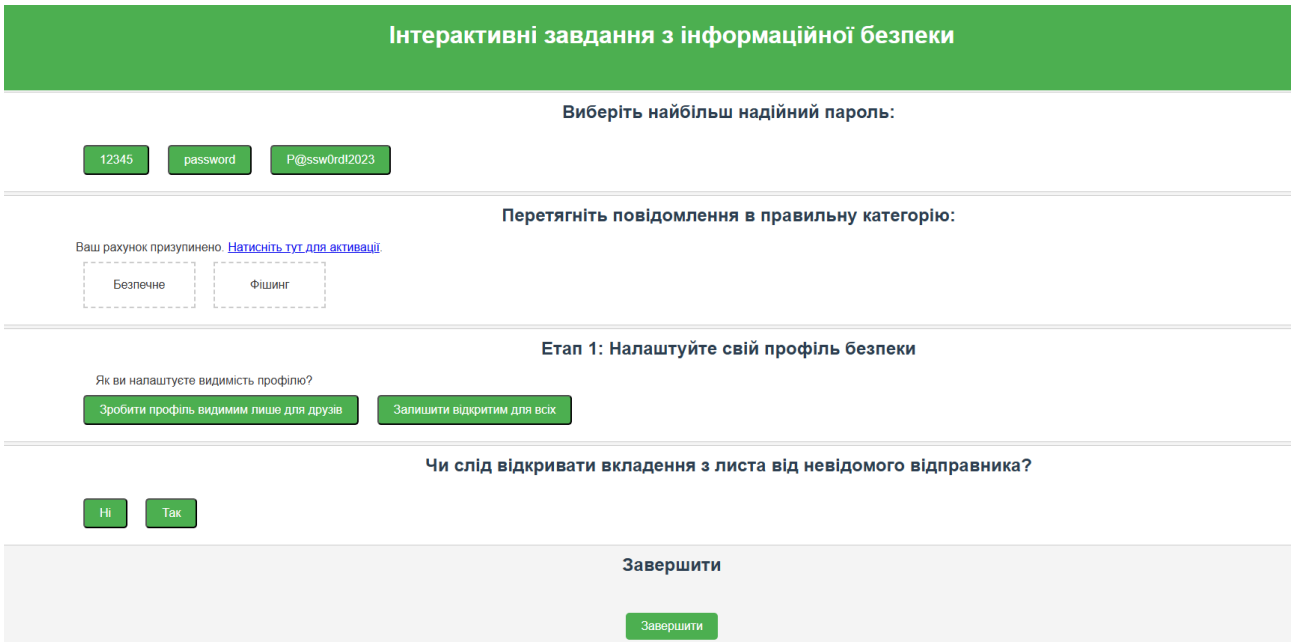


Рисунок 2.11. Сторінка з інтерактивними завданнями «Інформаційна безпека»

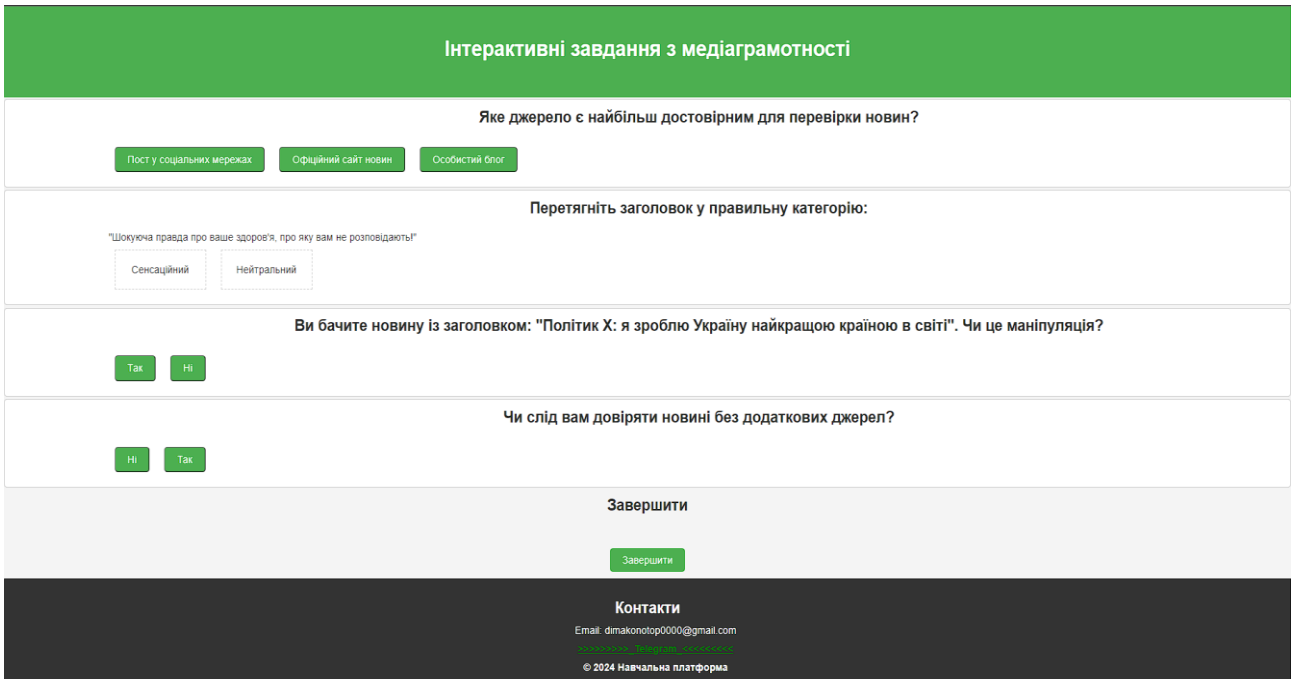


Рисунок 2.12. Сторінка з інтерактивними завданнями «Медіаграмотніть»

Сторінка з контактною інформацією представлена на рисунку 2.11 і містить ключові елементи для забезпечення зручності користувачів: контактну форму для зворотного зв’язку, електронну пошту, номер телефону, а також посилання на соціальні мережі платформи. Дизайн сторінки відповідає загальному стилю платформи, з акцентом на простоту, доступність і адаптивність для різних пристроїв.

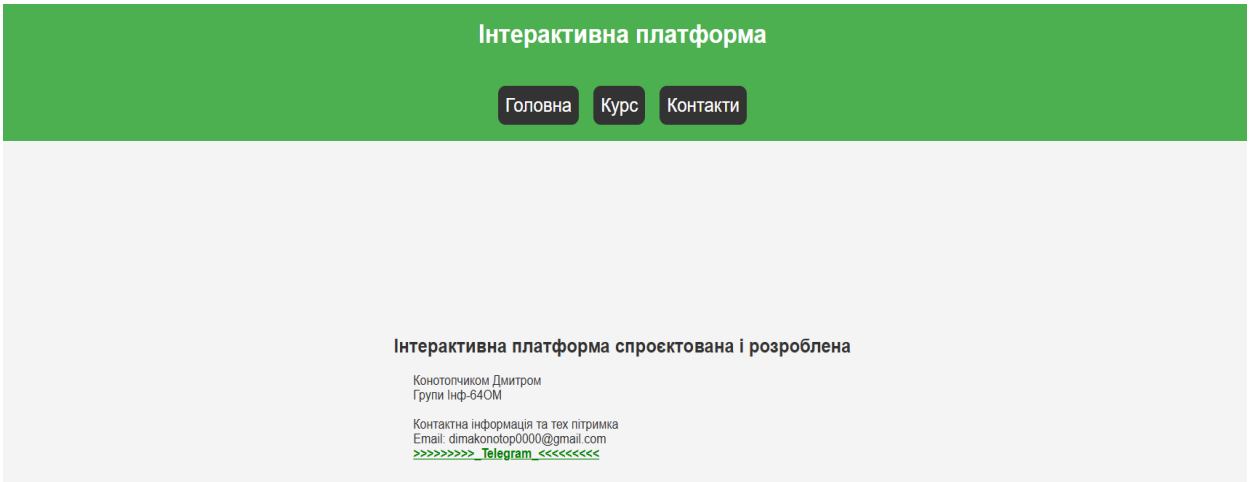


Рисунок 2.11. Сторінка з контактною інформацією

2.8. Рекомендації щодо використання та впровадження програмного засобу

Після успішного тестування та налагодження програмний засіб готовий до використання у навчальному процесі. Основне його призначення – контроль та оцінювання навчальних досягнень школярів через інтерактивні завдання. Оскільки сайт доступний онлайн, усі учасники освітнього процесу можуть ним користуватися.

Для учнів платформа пропонує:

- теоретичні відомості та відеоматеріали;
- інтерактивні вправи для перевірки знань за темою уроку;
- можливість самостійного навчання;

Навчатись учні можуть, перейшовши за посиланням: https://dima16102001.github.io/marister_saite/

або QR-кодом:

Інтерактивні завдання мають творчий характер, що сприяє розвитку пізнавальної діяльності учнів і досягненню позитивних результатів. Поєднання теоретичної частини уроку з інтерактивними ресурсами концентрує увагу на ключових моментах навчального матеріалу.

Цей програмний продукт можна використовувати на всіх етапах занять з інформаційної безпеки та медіаграмотності для перевірки знань та основних

видів контролю навчальних досягнень учнів. Він також буде ефективним у процесі дистанційного та змішаного навчання, забезпечуючи доступ учнів до завдань у зручний для них час.

Основні результати дослідження були представлені на XIII Міжнародній науково-практичній конференції «Математика. Інформаційні технології. Освіта» (тези); XLIII Міжнародній науково-практичній конференції «Сучасні виклики та досягнення наукової спільноти XXI століття» (тези); електронному мультидисциплінарному науковому часописі «Нотатки сучасної науки» (тези).

На платформі Prometheus пройдено та отримано сертифікат з курсу «Медіаграмотність для освітян» (60 годин / 2 кредити ЄКТС). Проходження курсу дало можливість розрізняти психологічні засади медіаграмотності та виокремлювати завдання медіаосвіти у школі, а також використовувати можливості медіа у професійної діяльності педагога. Набуті знання та компетентності були використані при проєктуванні та розробці власної інтерактивної платформи.

Під час проходження педагогічної практики у закладі загальної середньої освіти «Великоглушанський ліцей» Камінь-Каширської міської ради Волинської області з учнями 10 класу був проведений виховний захід «Безпека в Інтернеті та соціальних мережах» (24.04.2024 року); під час проходження педагогічної практики у закладах вищої освіти зі здобувачами факультету інформаційних технологій і математики, група Інф-15О – виховний захід «Інформаційна безпека та медіаграмотність у професійній діяльності майбутніх вчителів інформатики» (24.09.2024 року).

Апробація результатів дослідження пройшла у закладі загальної середньої освіти «Великоглушанський ліцей» Камінь-Каширської міської ради Волинської області у процесі проходження переддипломної практики. Зокрема, зі школярами старших класів було проведено анкетування стосовно ефективності інтерактивної платформи розробленої здобувачем вищої освіти Конотопчиком Д. О. Тридцять п’ять учнів взяли участь в опитуванні, давши відповідь на запитання , що представлені у таблиці 2.1.

Таблиця 2.1

Питання анкети

1. Чи використовуєте ви інтерактивний ресурс Конотопчика Д.О.?
2. Як часто Ви відвідуєте даний ресурс?
3. Чи зручний ресурс у використанні?
4. Наскільки корисним для навчання є даний ресурс?
5. Які функції ресурсу Ви використовуєте найчастіше?
6. Чи порекомендували б Ви цей ресурс учням інших шкіл?

Отримані результати були проаналізовані та занесені до таблиці 2.2.

Таблиця 2.2

Результати анкетування

• Використовують інтерактивний ресурс: 32 особи (91.4%)
• Відвідують ресурс кілька разів на тиждень: 28 осіб (80%)
• Вважають ресурс зручним у використанні: 30 осіб (85.7%)
• Відзначають користь для навчання: 29 осіб (82.9%)
• Активно використовують навчальні матеріали та тести: 27 осіб (77.1%)
• Готові рекомендувати іншим: 33 особи (94.3%)

Результати анкетування відображають загальну задоволеність учнів створеним ресурсом та підкреслюють його важливість при формуванні основ інформаційної безпеки та медіграмотності у школярів.

91% опитаних школярів використовує інтерактивний ресурс. 80% заходить на сайт декілька разів на тиждень. Також за результатами анкетування 86% респондентів відмітили, що ресурс є легким та зручним у використанні. 83% опитаних вважають ресурс корисним для навчання, при цьому 77% активно використовують розміщені навчальні матеріали та тести. 94% схиляються до того, щоб рекомендувати його учням з інших шкіл.

Результати анкетування подані у вигляді діаграми на рисунку 2.12.

Рисунок 2.12. Діаграма результатів анкетування

Таким чином, переважна більшість респондентів позитивно оцінює інтерактивний ресурс Конотопчика Д. О. та активно використовує його для навчання.

ВИСНОВКИ

Кваліфікаційна робота присвячена дослідженню проблеми формування інформаційної безпеки та медіаграмотності школярів старших класів при вивченні інформатики. Вона обґрунтовує необхідність адаптації освітнього процесу до викликів, які постають перед учнями у зв'язку із швидким розвитком інформаційних технологій.

У ході виконання кваліфікаційного дослідження поставлену мету досягнуто, завдання, які ставилися для її досягнення виконано. Отримано наступні результати.

Аналіз наукової, навчально-методичної, психолого-педагогічної літератури показав, що основи інформаційної безпеки та медіаграмотності є важливими для формування у школярів навичок захисту особистої інформації, а також для розвитку здатності до критичного аналізу медіа-контенту. Це сприяє розвитку цифрової грамотності, що є необхідною компетенцією в умовах сучасного інформаційного суспільства. Врахування цих аспектів у навчальному процесі дозволяє підготувати учнів до ефективної роботи з інформацією і засобами масової інформації, а також до захисту своїх прав у цифровому середовищі.

Навчальні програми вимагають включення основ інформаційної безпеки та медіаграмотності у навчальний процес як важливого елементу формування сучасних компетенцій учнів. Рекомендації щодо їх реалізації виявляються важливими для забезпечення цілісного підходу до навчання, враховуючи особливості цифрового середовища і потреби учнів у здобутті практичних навичок безпеки в Інтернеті.

Дослідження сучасних підходів до методики навчання інформаційної безпеки та медіаграмотності дають можливість стверджувати, що дані питання базуються на інтерактивних та практико-орієнтованих методах. Проєктне навчання, аналіз реальних кейсів і використання цифрових інструментів, сприяють розвитку в учнів навичок критичного мислення та практичного

застосування знань в умовах цифрової реальності.

Відповідно до поставлених завдань, було розроблено інтерактивну платформу, яка спрямована на підвищення рівня знань учнів з основ інформаційної безпеки та медіаграмотності. Проєкт інтерактивної платформи базується на комплексному підході, що включає використання сучасних дидактичних принципів, інтеграцію інноваційних методик навчання та залучення учнів до активної взаємодії з цифровими інструментами.

Розроблена платформа пропонує широкий набір інтерактивних завдань, які відповідають зазначеним цілям, і дозволяє здійснювати комплексне оцінювання досягнень учнів.

Практичні результати впровадження платформи підтвердили її ефективність. У ході експериментального тестування учні демонстрували підвищену зацікавленість до навчального матеріалу, покращення розуміння принципів інформаційної безпеки та навичок медіаграмотності. Вони навчалися ідентифікувати фейкову інформацію, аналізувати достовірність джерел та захищати свої персональні дані.

Особливе значення платформа має в умовах змішаного та дистанційного навчання, забезпечуючи інтерактивність і доступність навчального матеріалу.

Сформульовано рекомендації по використанню та впровадженню інтерактивної платформи та методичних матеріалів, що розміщені на ній.

Таким чином, завдання, поставлені у роботі, виконано повною мірою. Розроблений підхід підтвердив свою результативність, а результати дослідження можуть слугувати основою для подальших розробок у галузі інтерактивного навчання основ інформаційної безпеки та медіаграмотності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Антонова О. Навчально-методичний посібник «Нова українська школа: дидактичні основи формування медіаграмотності в учнів початкової школи» для педагогічних працівників. Київ : Генеза, 2020. 96 с

2. Антонченко М. Дефініція поняття «інфомедійна грамотність педагога». *Інфомедійна грамотність – невід'ємна складова навчального процесу закладу вищої освіти* : збірник статей / редкол.: В. Ф. Іванов (голов. ред.) та ін. Київ : Академія української преси, IREX, Центр Вільної преси, 2021. С. 12-21.

3. Батьки, діти та медіа: путівник із батьківського посередництва / О. Волошенюк, О. Мокрогуз; за ред. В. Іванова, О. Волошенюк. Київ : ЦВП, АУП, 2017. 79 с.

4. Бєляєва М. Інформаційна безпека учнів: сучасні виклики та перспективи. Харків : Основа, 2019. 90 с.

5. Бугайчук А. Медіаграмотність у школі. Ключові компетентності, форми та методи роботи. URL: https://osvitaua.com/2020/05/90017/.

6. Бурцева О. Г. Використання медіаосвітніх технологій для підвищення інформаційної компетентності в процесі навчання майбутніх вчителів математики. *Освітологічний дискурс*. 2023. № 1(40). С. 59-75.

7. Волошенюк О., Коваленко П., Мокрогуз О. Навчальна програма для учнів 8 (9) класів «Основи медіаграмотності» (пропедевтичний курс). Київ. 2017. 33 с.

8. Гарматій О. Критичне мислення як ключова компетенція медіаграмотності. *Критичне мислення в епоху токсичного контенту* : збірник статей VIII міжнародної науково-методичної конференції. 2020. С. 11-16.

9. Грицюк О. С., Максимова Л. П., Опришко А. В. Діяльність вчителів інформатики в аспекті розвитку медіакультури та медіаграмотності в Україні та її впровадження у закладах загальної середньої освіти. *Педагогічні науки: теорія та практика.* 2023. №3. С. 20-27.

10. Гуріна А. Медіаграмотність як життєво необхідна навичка в сучасному

соціально-політичному та культурному просторі України. *Нова педагогічна думка.* 2017. №4. С. 24-26

11. Денисенко В. Інформаційна культура та її складові в епоху цифрових медіа. *Культура та суспільство*. 2019. № 7. С. 54-68.

12. Дронова С. Інформаційна безпека в сучасній школі: посібник для педагогів. Київ : Либідь, 2018. 124 с.

13. Захист дітей у цифровому середовищі: рекомендації для батьків та освітян. 2020. URL: http://surl.li/pgbt

14. Зозуля Л. Основи безпеки в цифровому середовищі: рекомендації для школярів. Київ : Логос, 2021. 80 с.

15. Іванова Т. Медіаграмотність та критичне мислення в процесі викладання дисциплін комунікаційного циклу: навчальний посібник / за загал. ред. В. Іванова. Київ : Центр вільної преси. 2024.

16. Інформатика: навчальна програма вибірково-обов'язкового предмету для учнів 10-11 класів загальноосвітніх навчальних закладів (рівень стандарту). URL: https://osvita.ua/school/program/program-10-11/58877/

17. Інформатика для 10-11 класів (профільне навчання). URL:. https://osvita.ua/school/program/program-10-11/58876/

18. Клименко О. Основи інформаційної безпеки для дітей. *Молодь і ринок*. 2020. № 4. С. 112-117.

19. Ковальчук С., Мороз О. Медіаграмотність як сучасний інструмент боротьби з маніпуляторами та фейками. *Маркетинг в Україні.* 2019. № 5. С. 55-64.

20. Конотопчик Д. О., Ройко Л. Л. Безпечна поведінка школярів у цифровому середовищі. *Математика. Інформаційні технології. Освіта* : збірник тез доп. XIII міжнар. наук.-практ. конф. (м. Луцьк, 31 травн.-2 червн. 2024 р.). Луцьк, 2024. С. 225-227

21. Конотопчик Д. О., Ройко Л. Л. Розвиток інформаційно-цифрової компетентності учителів інформатики у процесі дистанційного навчання. *Modern Challenges and Achievements of the Scientific Community of the 21st century*

: XLIII International scientific and practical conference (October 16-18, 2024). Narva, Estonia. International Scientific Unity, 2024. С.154-156

22. Конотопчик Д. О., Ройко Л. Л. Формування інформаційної безпеки та медіаграмотності майбутніх вчителів інформатики. *Нотатки сучасної науки: електронний мультидисциплінарний науковий часопис*. Харків: СГ НТМ «Новий курс», 2024. № 19. С.5

23. Концепція впровадження медіа-освіти в Україні (2016 р.). URL: https://ms.detector.media/ mediaosvita/post/16501/2016–04–27-kontseptsiya-vprovadzhennya-mediaosvity-v-ukraini-novaredaktsiya/

24. Концепція впровадження медіа-освіти в Україні (нова редакція). URL: https://mediaosvita.org.ua/wp-content/uploads/2016/12/концепція-медіаосвіти.pdf

25. Кравець С. Інформаційна безпека і правова культура учнів. Київ: Генеза, 2020. 96 с.

26. Кравченко А. Основи інформаційної безпеки для школярів: методичний посібник для вчителів. Харків : Основа, 2018. 98 с.

27. Кривець М. П. Роль публічних бібліотек у забезпеченні інформаційної безпеки та формуванні медійної грамотності особистості. *Бібліотекознавство. Документознавство. Інформологія.* 2021. № 4. С. 68-75.

28. Кузьма І. І. Формування медіаграмотності дітей старшого дошкільного віку: теорія і технологія: монографія / за наук. ред. проф. Чайки В. М. Тернопіль: Осадца Ю. В., 2019. 188 с

29. Лашук Н. Критичне мислення у процесі формування медіакомпетентності майбутніх фахівців. *Критичне мислення в епоху токсичного контенту* : збірник статей VIII Міжнародної науково-методичної конференції. Київ. 2020. С. 37-40.

30. Литвиненко О. Формування навичок критичного мислення у процесі медіаосвіти. *Педагогічний альманах*. 2019. № 2. С. 45-58.

31. Медіаграмотність: Підручник для вчителів / Сінді Шейбе, Фейз Рогоу/ перекл. з англ. С. Дьома; за загал. ред. В. Ф. Іванова, О. В. Волошенюк. Київ : Центр вільної преси, Академія української преси. 2017. 319 с.

32. Медіаосвіта та медіаграмотність: підручник / ред.-упор. В. Ф. Іванов, О. В. Волошенюк; за науковою редакцією В. В. Різуна. Київ : Центр вільної преси, 2012. 352 с.

33. Модельні навчальні програми для 5-9 класів Нової української школи. URL: https://mon. gov.ua/ua/osvita/zagalna-serednya-osvita/navchalni-programi/modelni-navchalni-programi-dlya- 5– 9-klasiv-novoyi-ukrayinskoyi-shkoli-zaprovadzhuyutsya-poetapno-z-2022-roku

34. Мокрогуз О. Критичне мислення в контексті медіаосвіти. *Критичне мислення в епоху токсичного контенту* : збірник статей VIII Міжнародної науково-методичної конференції. Київ. 2020. С. 26-29.

35. Мокрогуз О.П. Основи медіаграмотності, 7-8 класи: посібник для вчителя / за загал. ред. В. І. Іванова. Київ: Академія української преси, Центр вільної преси, 2024. 159 с.

36. Мокрогуз О. П. Модельна навчальна програма «Основи медіаграмотності» (5-6 класи) для закладів загальної середньої освіти / О. П. Мокрогуз / За редакцією О. В. Волошенюк, В. Ф. Іванова, Р. І. Євтушенко. Київ: Академія української преси, Центр вільної преси, 2023. 25 с.

37. Морзе Н., Нанаєва Т., Пасічник О. Стан та перспективи навчання інформатики в закладах загальної середньої освіти України. *Інформаційні технології і засоби навчання*. 2022. Том 92. №6. С.1-20

38. Муковіз О., Мельничук В. Шляхи формування основ медіаграмотності в молодших школярів на уроках інформатики. *Психолого-педагогічні проблеми сучасної школи.* 2023. Випуск 1 (9). С. 111-120

39. Нестеренко С. Медіаграмотність і критичне мислення: методичний посібник для вчителів. Київ: Логос, 2021. 105 с.

40. Омельяненко В. Цифрові права та онлайн безпека: як захистити дітей в інтернеті. 2020. URL: http://surl.li/tnvwj

41. Петренко Н. Вплив кібербезпеки на освітній процес. *Кіберпростір і суспільство*. 2021. № 8. С. 45-53.

42. Практична медіаосвіта: медіаграмотність в освітньому просторі : навч.-

метод. посібник / уклад. : В. В. Байдик, О. В. Проніна; за заг. ред. В. В. Байдик. Лисичанськ, 2021. 66 с.

43. Савченко К. Інформаційна грамотність як фактор безпеки у сучасному суспільстві. *Інформаційна безпека і медіаосвіта* : збірник статей. Київ: Логос, 2020. С. 56-70.

44. Сидоренко І. А. Вплив цифрових технологій на інформаційну безпеку в освіті. *Інформаційна безпека*. 2020. № 7. С. 65-75.

45. Словник термінів з онлайн-безпеки / Міністерство цифрової трансформації України. URL: https://thedigital.gov.ua/news/vid-dipfeyku-do-fishingu-mintsifra-rozpochinae-osvitnyu-kampaniyu-z-tlumachennya-terminiv-onlayn-bezpeki

46. Слюсар Т., Соловей С., Степаненко В. Медіаосвіта як засіб формування медіаграмотності підростаючого покоління : *збірник обласної науково-практичної інтернет-конференції*. Черкаси. 2020. С. 98-101.

47. Солдатенко І. О., Зінюк А. В. Медіаграмотність як складова інформаційної безпеки. *Актуальні проблеми філософії та соціології*. Київ. 2016. Вип. 10. С. 138-140.

48. Степанова О. Безпека інформаційного середовища для учнів у цифровому суспільстві. *Освітні технології та суспільство*. 2021. № 2. С. 78-90.

49. Твердохліб І. А., Завадський І. О., Коршунова О. В., Семко Л. П., Прикладна спрямованість навчання інформатики в гімназії: методичний посібник. Київ : Видавничий дім «Освіта», 2024. 112 с.

50. Твердохліб І. А., Семко Л. П. Роль і місце задач прикладного спрямування в шкільному курсі інформатики. *Сучасні цифрові технології та інноваційні методики навчання: досвід, тенденції, перспективи* : матеріали IX Міжнародної науково-практичної інтернет-конференції (м. Тернопіль, 28 квітн. 2022). Тернопіль. 2022. С. 162-164.

51. Ткаченко А. Психологічні аспекти розвитку медіаграмотності у школярів. *Педагогічний дискурс*. 2021. № 1. С. 34-45.

52. Ткачук В. Використання вебресурсів у навчанні інформаційної

безпеки. Київ: Інститут педагогіки, 2021. 98 с.

53. Федоренко О. Г., Кайдан Є. В. Формування медіаграмотності підлітків. *Технології електронного навчання*. №5. 2021. С. 66-72

54. Федоренко О. Г., Фісенко А. А., Зима Г. С. Розвиток медіаграмотності учнів під час вивчення інформатики. *Збірник наукових праць фізико-математичного факультету ДДПУ*. 2024. Вип. 14. С.66-74

55. Харченко М. Використання цифрових медіа у формуванні інформаційної культури школярів. *Наука і освіта*. 2020. № 9. С. 42-56.

56. Харченко М. Інформаційна культура у школі: основи і методи формування. Київ : Видавництво «Освіта», 2021. 136 с.

57. Чумакова А. Інформаційна безпека у шкільній освіті: проблеми та рішення. Київ : Академія. 2022. 160 с.

58. Шевченко Н. Медіаосвіта як засіб розвитку критичного мислення учнів. *Інформаційне суспільство*. 2022. № 2. С. 51-64.

59. Шмельова І. Інформаційна культура в умовах сучасного інформаційного простору. *Педагогіка і психологія*. 2020. № 5. С. 23-31.

60. Що таке експеримент із медіаосвіти в Україні : 15 запитань та відповідей URL: https://cutt.ly/qIFXvvD

61. Юрченко О. К. Освіта в інформаційному суспільстві: методичні засади розвитку медіаграмотності. Київ : Освіта України, 2021. 134 с.

ДОДАТКИ

ДОДАТОК А

ТЕХНІЧНЕ ЗАВДАННЯ

Вступ

Тема кваліфікаційної роботи: Методика навчання учнів основ інформаційної безпеки та медіаграмотності.

Назва програмного забезпечення: «Інтерактивна платформа для навчання інформаційній безпеці та медіаграмотності».

Підстави для розробки

Підставою для розробки є завдання кваліфікаційної роботи Конотопчика Д. О., виконуваної на кафедрі загальної математики та методики навчання інформатики у Волинському національному університеті імені Лесі Українки.

Призначення розробки

Інтерактивна платформа призначена для навчання основам інформаційної безпеки та медіаграмотності учнів старших класів. Її функціонал забезпечує:

- інтерактивне навчання;
- оцінювання знань учнів;
- збереження результатів тестувань для подальшого аналізу.

Платформа може використовуватись при змішаному та дистанційному навчанні.

Вимоги до програмного продукту

Експлуатаційне призначення

Веб-платформа створена для використання в освітніх закладах та під час самостійного навчання. Для роботи з платформою необхідно мати доступ до мережі Інтернет і пристрій з веб-браузером.

Вимоги до функціональних характеристик

Платформа повинна забезпечувати:

- можливість створення сертефікату;
- інтерактивні тести й завдання;
- автоматичну перевірку тестів із записом результатів;
- контрольний тест;
- захищений доступ до персональних даних користувачів.

Вимоги до надійності

Програмний продукт повинен передбачати:

- захист від несанкціонованого доступу до персональних даних;
- стійкість до збоїв у роботі мережі Інтернет;
- контроль за введенням коректних даних під час реєстрації та авторизації.

Умови експлуатації

Для адміністрування платформи необхідна хоча б одна особа з базовими навичками роботи з ПК, а також знаннями у сфері веб-технологій.

Вимоги до складу і параметрів технічних засобів

Для роботи потрібен комп’ютер чи мобільний пристрій із встановленим сучасним веб-браузером.

Вимоги до інформаційної і програмної сумісності

Платформа повинна підтримуватись операційними системами Windows, Linux, MacOS, Android, iOS. Для роботи з базою даних передбачена адміністративна панель. Браузери: Google Chrome, Mozilla Firefox, Microsoft Edge тощо.

Вимоги до маркування і упаковки

Не висуваються вимоги до маркування та упаковки.

Вимоги до транспортування та збереження програми

Програму можна зберігати на будь-яких електронних носіях (флеш-накопичувачі, SSD, HDD). Доступ до платформи можливий через мережу Інтернет.

Вимоги до програмної документації

Програмна документація повинна включати:

- технічне завдання;

- інструкцію користувача;
- керівництво для адміністраторів.

Техніко-економічні показники

Продукт не є комерційним і доступний для використання безкоштовно.

Етапи розробки програми

Розробка програми виконувалася у наступній послідовності (табл. А.1).

Таблиця А.1.

Етапи розробки програми

Етап	Зміст роботи	Результат
1.	Постановка задачі	Визначення основних вимог до платформи
2.	Формування структури програми	Створення структурної блок-схеми програмного продукту
3.	Вибір інструментів розробки	Вибір мов програмування, фреймворків і баз даних
4.	Реалізація проєкту	Створення функціонального прототипу програми
5.	Тестування та налагодження	Виявлення й усунення помилок
6.	Впровадження та супровід	Розробка документації, запуск програми

Порядок контролю і приймання

Остаточні випробування проводяться на сервері, на якому буде розміщено платформу. Після успішного тестування продукт готовий до використання.

ДОДАТОК Б

ІНТЕРАКТИВНІ ЗАВДАННЯ ДЛЯ УРОКІВ ІНФОРМАТИКИ НА ТЕМУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА МЕДІАГРАМОТНОСТІ

Завдання можуть бути використані як у класі, так і в онлайн-форматі.

1. Квест «Захист інформації»

Ціль: навчити основ безпечної роботи в Інтернеті.

Опис завдання: ділимо учнів на команди, даємо завдання на кількох «станціях»:

1. *Паролі:* створити надійний пароль, відповідаючи на підказки (врахувати довжину, символи, унікальність).

2. *Фішинг:* знайти в листі електронної пошти підозрілі елементи (зайві посилання, помилки в адресі тощо).

3. *Антивірус:* обговорити, як визначити підозрілі файли, та скласти план дій у разі зараження комп'ютера.

4. *Двофакторна аутентифікація:* зрозуміти, як вона працює, розв'язавши ребус або задачку.

Результат: команда, яка правильно виконає всі завдання, отримує сертифікат «Експерта з інформаційної безпеки».

2. Гра «Факт чи фейк»

Ціль: навчити розпізнавати дезінформацію та фейки.

Опис завдання: готуємо набір статей, новин або зображень (частина з них – реальна, частина – фейкова).

Учні мають:

1. Проаналізувати джерело (чи перевірене?).

2. Знайти підтвердження або спростування в інших джерелах.

3. Зробити висновок: факт це чи фейк?

Додатково: можна дати завдання створити короткий алгоритм перевірки достовірності інформації.

3. Розв'язування кейсів

Ціль: розвивати навички вирішення реальних ситуацій, пов'язаних з інформаційною безпекою.

Опис завдання: учні отримують кейси, наприклад:

1. Ваша сторінка в соцмережі зламана. Що робити?

2. Вам прийшло повідомлення про виграш у конкурсі. Як діяти?

3. Ви знайшли флешку на вулиці. Чи слід її підключати до комп'ютера?

Результат: кожна команда пропонує свої рішення, обговорюються правильні дії.

4. Вікторина «Хто хоче бути експертом з кібербезпеки?»

Ціль: перевірити знання в ігровій формі.

Опис завдання: створюємо презентацію у стилі гри, наприклад, у Kahoot чи PowerPoint.

Приклади питань:

1. Що таке фішинг?

2. Який пароль є найбільш захищеним?

3. Що робить брандмауер?

4. Які методи допомагають убезпечити смартфон?

5. Симуляція «Медіаштурм»

Ціль: навчити аналізувати контент і уникати маніпуляцій.

Опис завдання: ділимо учнів на 2 групи: авторів контенту та аналітиків.

- *Задача авторів:* створити короткі новини, використовуючи різні стилі (нейтральний, маніпулятивний).

- *Задача аналітиків:* визначити, які новини маніпулюють емоціями, а які подають інформацію об'єктивно.

6. Онлайн-квест «Безпечний Інтернет»

Ціль: розвивати практичні навички користування Інтернетом.

Опис завдання: створюємо інтерактивний квест у Google Forms або іншій платформі.

Завдання можуть включати:

1. Знайти в тексті підозрілий лінк.

2. Визначити, чи безпечний сайт за його адресою.

3. Пояснити, чому не можна завантажувати файли з невідомих джерел.

7. Рольова гра «Суд над хакером»

Ціль: обговорити моральні аспекти кіберзлочинності.

Опис завдання: учні розподіляють ролі: суддів, адвокатів, обвинувачів, свідків.

Сценарій: учень «зламав» комп’ютерну мережу школи. Команди готують аргументи «за» і «проти».

Обговорення завершується винесенням «вироку».

ДОДАТОК В

РОЗРОБКА ВИХОВНОЇ ГОДИНИ
БЕЗПЕКА В ІНТЕРНЕТІ ТА СОЦІАЛЬНИХ МЕРЕЖАХ

Захід проведено у закладі загальної середньої освіти «Великоглушанський ліцей» Камінь-Каширської міської ради Волинської області з учнями 10 класу (24.04.2024 року) у межах проходження педагогічної практики.

Мета: ознайомити учнів із ризиками, які можуть виникати в Інтернеті та соціальних мережах; надати поради щодо безпечної поведінки в онлайн-середовищі; сформувати критичне ставлення до інформації в Інтернеті; навчити правилам кібергігієни.

ХІД ВИХОВНОЇ ГОДИНИ

Вступ (до 5 хвилин):

Привітання учнів. Показ короткого відео, яке демонструє проблеми, пов’язані з необережною поведінкою в Інтернеті та соціальних мережах.

Основна частина (до 20 хвилин):

Ризики в Інтернеті

Пояснення основних загроз:

КІБЕРБУЛІНГ – це агресивна поведінка в Інтернеті, спрямована на приниження, залякування чи образу людини. Ця форма цькування здійснюється через соціальні мережі, месенджери, електронну пошту або інші онлайн-платформи.

Основні форми кібербулінгу:

- *Образливі повідомлення* – принизливі чи погрозливі слова, які надсилають через приватні чи відкриті платформи.

- *Поширення неправдивої інформації* – чутки, фейкові новини, які ганьблять людину.

- *Фейкові акаунти* – створення підроблених профілів з метою дискредитації.

- *Публікація особистих даних* – викладання приватної інформації без дозволу.

- *Онлайн-ізоляція* – ігнорування чи блокування особи у групових чатах або спільнотах.

- *Тролінг* – провокація агресивних відповідей, насмішки чи образи.

Як захиститися від кібербулінгу:

- *Не відповідати на агресію* (не вступайте у конфлікти з кривдником).

- *Блокувати кривдників* (використовуйте функції блокування в соціальних мережах та месенджерах).

- *Повідомляти про порушення* (зверніться до адміністрації платформи з проханням видалити образливий контент або заблокувати акаунт).

- *Зберігати докази* (робіть скріншоти повідомлень чи записів для подальших дій).

- *Довіритися дорослим* (розкажіть про проблему батькам, вчителям або дорослим, яким довіряєте).

- *Звернутися до поліції* (у разі серйозних погроз чи переслідувань).

ШАХРАЙСТВО (наприклад, фішингові сайти, неправдиві розіграші).

Основні види шахрайства:

Фішинг – шахраї створюють підроблені сайти, які виглядають як відомі сервіси (банки, соціальні мережі, магазини); надсилають посилання з проханням увійти у ваш акаунт, де ви випадково передаєте свої дані.

Неправдиві розіграші – «Ви виграли автомобіль/телефон/гроші! Щоб отримати приз, перекажіть символічну суму»; часто такі оголошення з’являються у соцмережах або через SMS/емейли.

Шахрайство в онлайн-магазинах – сайти з дуже низькими цінами, які вимагають передоплату, але товар так і не надходить; фейкові магазини без контактної інформації.

Лотереї та інвестиції – запрошення інвестувати у «вигідну» справу або брати участь у лотереї в результаті шахраї отримують доступ до вашого банківського рахунку.

Шкідливе програмне забезпечення – надсилання файлів чи посилань, які заражають ваш пристрій вірусами для крадіжки даних.

Як розпізнати шахрайство:

Нереалістичні обіцянки (призи або акції, які здаються надто вигідними, щоб бути правдою.

Дивні посилання (посилання, які виглядають неприродно, наприклад, *bank-login-secure.online* замість справжнього *bank.com*).

Терміновість (шахраї тиснуть на Вас, вимагаючи негайної дії: «Залишилося 5 хвилин, щоб отримати приз!»).

Запит особистих даних **(**банківська карта, паролі або дані паспорта, легітимні організації ніколи не запитують цю інформацію онлайн).

Відсутність контактної інформації (у шахрайських магазинах немає фізичної адреси, реальних телефонів чи служб підтримки).

Практична частина (15 хвилин):

Обговорення ситуацій, пов’язаних з ризиками в Інтернеті.

Наприклад:

Тобі написав незнайомець і просить надіслати фотографії або особисту інформацію.

Ти бачиш підозрілий конкурс у соцмережі з вимогою переказати гроші.

Хтось із друзів постить образливі коментарі.

Підсумок (до 5 хвилин):

Короткий висновок про важливість дотримання правил безпеки в Інтернеті.

Дотримання правил безпеки в Інтернеті є життєво важливим у сучасному світі, де технології стали невід’ємною частиною нашого життя. Це допомагає захистити особисту інформацію, уникнути шахрайства та кібератак, а також зберегти репутацію і фінансову безпеку. Усвідомлене та відповідальне користування мережею сприяє створенню безпечного цифрового простору для усіх.

Презентація (слайди з ключовими моментами).

Відео або картинки для ілюстрації ризиків.

Пам’ятка

10 правил безпечного користування Інтернетом

1. *Захищай особисту інформацію* (ніколи не розголошуй особисті дані: номер телефону, адресу, паролі, фінансову інформацію на сумнівних сайтах або незнайомцям).

2. *Використовуй надійні паролі* (паролі мають бути складними: мінімум 8 символів, комбінація великих і малих літер, цифр та спеціальних символів, їх потрібно регулярно змінювати).

3. *Будь обережним із посиланнями* (не клікай на підозрілі посилання з електронних листів, соцмереж або повідомлень, перевіряй URL перед тим, як переходити на сайт).

4. *Оновлюй програмне забезпечення* (регулярно оновлюй операційну систему, антивірус та браузери, щоб захиститися від нових загроз).

5. *Не завантажуй файли з ненадійних джерел* (завантажуй програми, документи та файли лише з офіційних сайтів або перевірених джерел).

6. *Перевіряй безпеку сайтів* (перед введенням особистих даних переконайся, що сайт захищений: URL починається з https://, є значок замка).

7. *Обмежуй особисту інформацію в соцмережах* (не публікуй фото документів, банківських карток або іншу конфіденційну інформацію.

8. *Стережись шахрайства* (якщо хтось обіцяє «легкі гроші» або «виграш у конкурсі», будь обережним).

9. *Навчайся розпізнавати фейки* (перевіряй інформацію, яку знаходиш в Інтернеті, за кількома джерелами, щоб уникнути поширення фейків).

10. *Розкажи про проблеми дорослим* (якщо ти зіткнувся з погрозами, шантажем або іншими неприємностями в Інтернеті, негайно звертайся до дорослих або відповідних організацій).

Дотримуючись цих правил, ви зможете значно знизити ризики, пов’язані з використанням Інтернету.