МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ
Кафедра комп'ютерних наук

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему: **«ЗАСОБИ ЕФЕКТИВНОГО ВИКЛАДАННЯ ВИБІРКОВОГО МОДУЛЮ «ІНФОРМАЦІЙНА БЕЗПЕКА»»**

Виконав: студент 2 курсу, групи 8.0143-ін-з
спеціальності 014 Середня освіта
(шифр і назв1а спеціальності)
освітньої програми 014.09 Середня освіта (Інформатика)
А. М. Харіна
(ініціали та прізвище)
Керівник доцент кафедри комп'ютерних наук, доцент, к.т.н. Решевська К.С.
(посада, вчене звання, науковий ступінь, прізвище та ініціали)
Рецензент доцент кафедри програмної інженерії, к.ф.-м.н. Кривохата А.Г.
(посада, вчене звання, науковий ступінь, прізвище та ініціали)

Запоріжжя – 2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет математичний

Кафедра комп'ютерних наук

Рівень вищої освіти магістр

Спеціальність 014 Середня освіта
(шифр і назва)

Освітня програма 014.09 Середня освіта (Інформатика)

ЗАТВЕРДЖУЮ

Завідувач кафедри
комп'ютерних наук, д.т.н., професор

_____ Шило Г.М.
(підпис)

« 5 » березня 2024 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТЦІ

Харіній Анастасії Миколаївні
(прізвище, ім'я та по-батькові)

1. Тема роботи (проекту) Засоби ефективного викладання вибіркового модулю «Інформаційна безпека»

керівник роботи (проекту) Решевська Катерина Сергіївна, доцент, к.т.н.
(прізвище, ім'я та по-батькові, науковий ступінь, вчене звання)

затверджені наказом ЗНУ від « 01 » березня 2024 року № 384-с

2. Строк подання студентом роботи 02.12.2024

3. Вихідні дані до роботи 1. Постановка задачі.
2. Перелік літератури.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Постановка задачі. Основні теоретичні відомості
2. Методика викладання
3. Статистичний аналіз

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
презентація

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 5.03.2024

К А Л Е Н Д А Р Н И Й П Л А Н

№	Назва етапів кваліфікаційної роботи магістра	Строк виконання етапів роботи	Примітка
1.	Розробка плану роботи.	12.05.2024	
2.	Збір вихідних даних.	01.09.2024	
3.	Обробка літературних джерел	5.10.2024	
4.	Розробка першого та другого розділу.	18.10.2024	
5.	Розробка третього розділу.	05.11.2024	
6.	Оформлення та нормоконтроль	28.11.2024	
	кваліфікаційної роботи магістра.		
7.	Захист кваліфікаційної роботи магістра.	10.12.2024	

Студент _____ А.М. Харіна
(підпис) (ініціали та прізвище)

Керівник роботи _____ К.С. Решевська
(підпис) (ініціали та прізвище)

Нормоконтроль пройдено

Нормоконтролер _____ О.Г. Спиця
(підпис) (ініціали та прізвище)

РЕФЕРАТ

Кваліфікаційна робота магістра «Засоби ефективного викладання вибіркового модулю «Інформаційна безпека»»: 68 с., 13 рис., 1 таблиця, 25 джерел, 8 додатків.

ВЕБКВЕСТ, ГЕЇМІФІКАЦІЯ У НАВЧАННІ, ІНТЕРАКТИВНА ПЛАТФОРМА, ІНФОРМАЦІЙНА БЕЗПЕКА, МЕТОДИКА ВИКЛАДАННЯ, МОЗКОВИЙ ШТУРМ, СТАТИСТИЧНІ МЕТОДИ

Об’єкт дослідження – методичні підходи, інструменти та технології, що забезпечують ефективність викладання вибіркового модулю «Інформаційна безпека».

Предмет дослідження – процес викладання вибіркового модулю «Інформаційна безпека» у старшій школі.

Мета роботи: розробити та обґрунтувати засоби і методи ефективного викладання вибіркового модуля «Інформаційна безпека», які сприятимуть формуванню в учнів практичних навичок і компетентностей у сфері захисту інформаці.

Методи дослідження – порівняння, аналіз, спостереження.

У роботі розроблено та обґрунтовано ефективні методичні засоби викладання вибіркового модуля «Інформаційна безпека», які включають сучасні підходи, інтерактивні технології та практичні завдання, спрямовані на формування в учнів і студентів ключових компетентностей у сфері захисту інформації.

Актуальність дослідження зумовлена зростанням кіберзагроз, необхідністю формування цифрової грамотності та навичок інформаційної безпеки у сучасних умовах, а також недостатнім методичним забезпеченням викладання цієї тематики в освітніх установах.

SUMMARY

Master’s Qualification Thesis «Effective Teaching Means of the Selective Module Information Security»: 68 pages, 13 figures, 1 table, 25 references, 8 appendixes.

BRAINSTORMING, GAMIFICATION IN EDUCATION, INFORMATION SECURITY, INTERACTIVE PLATFORM, STATISTICAL METHODS, TEACHING METHODOLOGY, WEBQUEST

The object of reseach is Methodological approaches, tools, and technologies that ensure the effectiveness of teaching the elective module "Information Security".

The subject of research is The process of teaching the elective module "Information Security" in high school.

The aim of research: to develop and substantiate tools and methods for effective teaching of the elective module "Information Security," aimed at fostering students' practical skills and competencies in the field of information protection.

Research methods - comparison, analysis, and observation.

The study developed and substantiated effective methodological tools for teaching the elective module "Information Security," incorporating modern approaches, interactive technologies, and practical tasks aimed at fostering key competencies in information protection among students.

The research is driven by the increasing prevalence of cyber threats, the necessity to enhance digital literacy and information security skills in modern conditions, and the insufficient methodological resources for teaching this topic in educational institutions.

ЗМІСТ

Завдання на кваліфікаційну роботу..... …..……..……..…...2
Реферат……..……..…….4
Summary ……...……...……5
Вступ..... 8
1 Методичні засади та сучасні підходи до викладання тематики інформаційної безпеки..... 11
1.1 Дослідження наявних в мережі навчальних матеріалів..... 11
1.2 Аналіз популярних педагогічних технологій у освітній практиці 13
1.3 Висновки за розділом 1 17
2 Методичні засоби ефективного викладання модуля «інформаційна безпека»..... 19
2.1 Використання гейміфікації у викладанні інформаційної безпеки..... 19
2.2 Підхід у навчанні з використанням персонажів: персоніфікація навчального процесу..... 21
2.3 Інтерактивні платформи для підвищення мотивації учнів..... 23
2.4 Інтеграція персоніфікації та гейміфікації у навчальний процес..... 26
3 Експериментальна перевірка ефективності методики викладання вибіркового модулю «інформаціна безпека»..... 32
3.1 Організація проведення експериментальної перевірки 32
3.2 Аналіз результатів експериментального дослідження ефективності Викладання модулю..... 36
Висновки 42
Перелік посилань..... 44
Додаток А Урок на тему: "Основні поняття в області безпеки інформаційних технологій. Основні причини загострення проблеми забезпечення безпеки інформаційних технологій"..... 47
Додаток Б Урок на тему: «Криптографічні методи захисту інформації» 50

Додаток В Урок на тему: "Керування механізмами захисту та виявлення атак у комп'ютерних мережах"... 52
Додаток Г Урок на тему: «Політика безпеки при доступі до мережі загального користування. Системи аналізу вмісту поштового і веб-трафіку. Віртуальні приватні мережі (VPN)»... 54
Додаток Д Розробка тестових завдань 56
Додаток Е Основні характеристики тестових завдань……………….………60
Додаток Ж Остаточний тест з модулю «Інформаційна безпека» 64
Додаток И Перевірка ефективності викладання вибіркового модулю «Інформаційна безпека,,,69

ВСТУП

У сучасному світі інформаційні технології пронизують усі сфери життя людини, забезпечуючи доступ до інформації, автоматизацію процесів і нові можливості для спілкування та роботи. Однак разом із цими перевагами постають нові загрози, пов’язані з безпекою інформації, зокрема кіберзлочинність, витік даних, несанкціонований доступ до ресурсів та інші виклики. У зв’язку з цим знання та навички забезпечення інформаційної безпеки стають необхідними не лише для ІТ-фахівців, а й для кожної людини.

Система освіти повинна оперативно реагувати на ці виклики, інтегруючи основи інформаційної безпеки в навчальні програми. Вибірковий модуль «Інформаційна безпека» є одним із способів забезпечення відповідності освітнього процесу сучасним реаліям. Цей модуль дозволяє поглиблено вивчати принципи та методи захисту інформації, формувати практичні навички розпізнавання загроз, використання інструментів захисту даних та забезпечення безпечної роботи в мережі.

Актуальність дослідження визначається тим, що викладання теми інформаційної безпеки часто стикається з низкою проблем, зокрема недостатнім методичним забезпеченням, відсутністю адаптованих до української освітньої системи матеріалів, обмеженим доступом до практичних ресурсів. Крім того, швидкий розвиток загроз та технологій захисту вимагає оновлення методик викладання, що підкреслює необхідність пошуку нових підходів.

Вибіркові модулі є гнучкою формою організації навчання, яка дозволяє адаптувати освітній процес до потреб здобувачів освіти та актуальних вимог суспільства. Успішна реалізація модуля «Інформаційна безпека» потребує ефективного методичного забезпечення, використання сучасних засобів навчання та інтеграції практичного компоненту в освітній процес.

Предмет дослідження: методичні підходи, інструменти та технології, що забезпечують ефективність викладання вибіркового модуля «Інформаційна безпека».

Об’єкт дослідження: процес викладання вибіркового модуля «Інформаційна безпека» у старшій школі.

Мета дослідження: розробити та обґрунтувати засоби і методи ефективного викладання вибіркового модуля «Інформаційна безпека», які сприятимуть формуванню в учнів та студентів практичних навичок і компетентностей у сфері захисту інформації.

Для досягнення поставленої мети необхідно розв’язати такі **завдання**:

- проаналізувати стан проблеми викладання вибіркових модулів із тематики інформаційної безпеки в сучасній освіті;
- визначити дидактичні принципи та методичні підходи, які забезпечують ефективність навчання з теми «Інформаційна безпека»;
- розробити модель викладання вибіркового модуля «Інформаційна безпека», що включає сучасні засоби та технології навчання;
- запропонувати систему практичних завдань для формування навичок забезпечення інформаційної безпеки в учнів та студентів;
- провести педагогічний експеримент для оцінки ефективності запропонованих методик;
- узагальнити результати дослідження та сформулювати рекомендації для викладачів щодо впровадження вибіркового модуля «Інформаційна безпека».

Структура роботи. Магістерська кваліфікаційна робота складається зі вступу, основної частини, яка включає три розділи, висновків та списку використаних джерел.

Основна частина включає три розділи. У першому розділі "Методичні засади та сучасні підходи до викладання тематики інформаційної безпеки" розглянуто стан викладання вибіркових модулів у сучасній освіті, аналіз існуючих методик та їх відповідність сучасним викликам. Проаналізовано

дидактичні принципи та методи, які сприяють ефективному засвоєнню знань у цій сфері.

Другий розділ "Методичні засоби ефективного викладання модуля «Інформаційна безпека»" присвячений розробці моделі викладання, що базується на сучасних підходах. Висвітлено використання цифрових інструментів, інтерактивних платформ та симуляцій реальних загроз для закріплення матеріалу. Запропоновано структуру модулів, що включає теоретичні блоки, практичні завдання та елементи проектного навчання.

У третьому розділі "Експериментальна перевірка ефективності методики викладання вибіркового модуля «Інформаційна безпека»" описано проведення педагогічного експерименту. Представлено результати впровадження запропонованої методики, порівняльний аналіз досягнень учнів експериментальної та контрольної груп, а також зроблено висновки про ефективність використаних підходів.

1 МЕТОДИЧНІ ЗАСАДИ ТА СУЧАСНІ ПІДХОДИ ДО ВИКЛАДАННЯ ТЕМАТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Розвиток цифрових технологій вимагає від системи освіти своєчасної адаптації навчальних програм до нових викликів. Інформаційна безпека стає важливою складовою навчання, особливо в умовах зростання кіберзагроз, що впливають на особисте життя, бізнес та державні структури. Вибірковий модуль «Інформаційна безпека» спрямований на вирішення цього завдання. Він спрямований на формування у здобувачів освіти компетентностей у сфері захисту інформації. З огляду на глобальні виклики, пов'язані з кіберзагрозами, актуальність розробки та впровадження якісних методичних матеріалів є надзвичайно високою.

Аналіз наявних методичних розробок дозволяє виявити їхні переваги та недоліки, визначити прогалини в змісті та запропонувати шляхи вдосконалення навчальних матеріалів для підвищення ефективності викладання.

1.1 Дослідження наявних в мережі навчальних матеріалів

Матеріали з модуля "Інформаційна безпека" для 10–11 класів, доступні на teach-inf.com.ua [1], є частиною 35 комплектів уроків для вибіркових модулів інформатики, що відповідають рівню стандарту. Ці розробки спрямовані на забезпечення викладачів готовими сценаріями уроків, включно з методичними рекомендаціями, завданнями, мультимедійними презентаціями та іншими допоміжними ресурсами.

Розробки охоплюють 17 уроків, які зосереджені на різних аспектах інформаційної безпеки, таких як загрози інформації, захист даних, паролі, мережні ризики тощо. Вони дозволяють викладачам зекономити час на

підготовці, забезпечуючи структурованість викладання. Ресурси адаптовані до нової навчальної програми, затвердженої МОН України.

Навчальні матеріали з модуля "Інформаційна безпека" для 10–11 класів, доступні на ресурсі vsimpptx.com [2], спрямовані на формування базових знань про загрози в інформаційному просторі, захист персональних даних і протидію шахрайству в Інтернеті.

Тематика матеріалів охоплює захист персональних даних, основні принципи інформаційної безпеки та способи ідентифікації загроз в Інтернеті.

Кожна тема розбита на уроки, які включають теоретичну частину, практичні завдання та рекомендації для викладачів щодо проведення занять.

Матеріали надаються у вигляді презентацій PowerPoint, що зручно для використання під час уроків. Включено ілюстрації, приклади реальних загроз, а також інтерактивні завдання для залучення учнів.

Завдання сприяють формуванню навичок розпізнавання фішингових атак, аналізу даних з точки зору безпеки та застосування основних правил безпечного користування Інтернетом. Особливу увагу приділено навчанню основ кіберетики.

Методичні матеріали модуля "Інформаційна безпека" для 11 класу з ресурсу [3] зосереджуються на основах захисту інформаційних технологій, ідентифікації загроз, правових аспектах безпеки, криптографії та мережевому захисті. Тематичний план включає 17 уроків із практичними завданнями, тренувальними вправами та тематичними оцінюваннями. Ключовими темами є забезпечення безпеки даних, контроль доступу, виявлення атак і міжнародні стандарти інформаційної безпеки.

1.2 Аналіз популярних педагогічних технологій у освітній практиці

Інноваційні методи навчання в старшій школі спрямовані на формування учня, здатного адаптуватися до швидкозмінного інформаційного суспільства [4]. Основний акцент робиться на створенні умов для набуття ключових компетентностей, розвитку критичного мислення, співпраці, креативності та використання сучасних технологій у навчальному процесі.

Інтерактивне навчання [7] є однією з ключових сучасних педагогічних технологій, яка активно впроваджується в освітню практику. Його основною метою є створення умов для залучення учнів або студентів до активного навчального процесу, що забезпечує краще засвоєння знань і розвиток навичок. Інтерактивне навчання дозволяє підлаштовувати освітній процес під індивідуальні потреби та темп учня або студента. Наприклад, використання цифрових платформ надає можливість створювати персоналізовані навчальні плани.

Завдяки залученню різних методів, таких як рольові ігри, симуляції або дискусії, інтерактивне навчання сприяє кращому розумінню складних тем, наприклад, у природничих науках чи технологіях.

Включення інтерактивних елементів, таких як віртуальні лабораторії або інтеграція AR/VR технологій, підвищує зацікавленість і залученість учнів до навчального процесу.

У Новій українській школі інтерактивне навчання активно використовується для формування ключових компетентностей, таких як співпраця, критичне мислення та комунікація. Методи "Мозковий штурм", "Рольова гра" чи "Дебати" допомагають створювати умови для діалогу і взаємного навчання. Недоліки інтерактивного навчання полягають у потребі технічних ресурсів, які не завжди доступні, необхідності підвищення кваліфікації викладачів для ефективного використання технологій.

Особистісно орієнтоване навчання [4, 12] є педагогічним підходом, що ставить учня в центр навчального процесу, підкреслюючи його індивідуальні особливості, потреби, здібності та інтереси. Воно ґрунтується на принципах, які спрямовані на розвиток та самореалізацію особистості. Основними аспектами цього підходу є індивідуалізація змісту освіти, методів та форм навчання, що дозволяють учневі реалізовувати свій потенціал у різних видах діяльності. Він орієнтований на формування духовних, інтелектуальних та соціальних якостей особистості, зважаючи на її унікальність та суб'єктивний досвід; надає учневі можливостей вибору змісту, форм і методів навчання, що відповідають його особистісним характеристикам; визначає учня головним суб’єктом освітнього процесу, на основі чого створюються умови для самовираження та самоактуалізації.

В рамках особистісно орієнтованого навчання пропонуються різні моделі уроків, наприклад, акцент на проєктній діяльності, рефлексії та діалозі між учнем і вчителем. Підходи варіюються залежно від контексту, але спільною рисою є увага до індивідуальності кожного учасника освітнього процесу.

Особистісно орієнтоване навчання ефективно застосовується у формуванні навичок критичного мислення, розвитку креативності та навичок роботи в команді. У статті [8] наголошується, що цей підхід дозволяє інтегрувати сучасні технології, роблячи навчання гнучкішим і адаптивнішим до потреб учня.

Гейміфікація [6, 10] у навчанні є популярною педагогічною технологією, яка інтегрує елементи гри в освітній процес для підвищення мотивації та залучення студентів. Сучасні публікації зосереджені на розгляді її переваг, обмежень та практичних прикладів впровадження.

Гейміфікація включає використання ігрових механік, таких як бали, рівні, нагороди та змагання, для стимулювання навчальної активності. Вона відрізняється від ігор та навчання, заснованого на грі, оскільки не передбачає створення повноцінних ігор, а лише адаптує їх елементи до освітніх цілей (наприклад, рейтинги чи системи заохочень)

При впровадженні гемифікації студенти активніше долучаються до процесу навчання, коли отримують миттєвий зворотний зв’язок і нагороди; завдяки ігровим елементам, процес навчання стає більш інтерактивним і захоплюючим; під час гейміфікованих завдань учні вчаться працювати в команді, приймати рішення і досягати поставлених цілей

До недоликів геміфікації відносять надмірну концентрація на грі: студенти можуть фокусуватися на нагородах, а не на засвоєнні матеріалу; складність впровадження: вимагає додаткових зусиль від викладачів для створення та підтримки системи гейміфікації.

Гемифікація у навчання впроваджується з використання таких платформ, як Quizizz, Kahoot, Blooket, Всеосвіта і т.д. Гейміфікація особливо ефективна під час дистанційних занять, де вона підтримує увагу та інтерес учнів.

Для успішного впровадження гейміфікації необхідне відповідне навчання викладачів.

Проєктне навчання [8, 5, 15] є ефективною методикою, яка передбачає залучення учнів до розв’язання практичних чи теоретичних завдань з метою створення конкретного продукту. Цей підхід сприяє формуванню навичок критичного мислення, співпраці, управління часом та комунікації, а також дозволяє глибше зрозуміти навчальний матеріал через активну участь. При реалызації цього підходу учні розв’язують реальні чи близькі до реальних завдання, створюючи матеріальні чи інтелектуальні продукти. Значна частина роботи виконується самостійно або в команді, розвиваючи лідерські та організаційні навички. Метод передбачає міждисциплінарний підхід, об’єднуючи знання з різних предметів для досягнення спільної мети.

Перевагами проєктного навчання є покращення мотивації учнів, глибше розуміння матеріалу, розвиток навичок XXI століття, але потребує ретельного планування, достатнього часу, залучення ресурсів і навчання вчителів для ефективної реалізації.

Проєктне навчання активно впроваджується в умовах Нової української школи (НУШ). Приклади включають STEAM-проєкти, уроки тривимірного

моделювання, інтегровані проєкти в рамках дистанційного чи змішаного навчання, а також підвищення кваліфікації педагогів через спеціальні курси та вебінари

Дослідницьке навчання [9, 11, 16] є сучасним методом навчання, який акцентує увагу на активній участі учнів у процесі отримання знань. Цей підхід базується на розвитку дослідницької компетентності учнів, що передбачає формування вмінь знаходити, аналізувати й інтерпретувати інформацію, а також критично і творчо мислити.

Учні активно шукають інформацію, формулюють питання і пропонують гіпотези, що стимулює їхню пошукову активність і критичне мислення. Наприклад, застосування цього підходу до створення підручників дозволяє розвивати в учнів індивідуальні здібності та забезпечує диференційований підхід до навчання.

Учитель виступає як фасилітатор, координатор дослідницької діяльності та науковий керівник, що сприяє формуванню високої методологічної культури учнів

Психологічні дослідження підтверджують, що дослідницька поведінка, яка є основою цього підходу, виникає через природну потребу людини в пошуку нових знань та активному вивченні світу. Цей підхід створює умови для розвитку самостійного мислення та зменшує страх перед невизначеністю.

Переваги дослідницького навчання:

- підвищення мотивації учнів через залучення до реальних проблем;
- формування навичок самостійного навчання, необхідних для сучасного світу;
- збільшення ефективності засвоєння матеріалу через практичну діяльність.

Дослідницьке навчання застосовується на різних уроках, включаючи уроки з інформатики. Для його ефективного впровадження важливо забезпечити учням доступ до відповідних інструментів та матеріалів, а також

провести підготовку педагогів, які зможуть адаптувати свої методики до цього підходу.

1.3 Висновки за розділом 1

Аналіз методичних матеріалів модуля "Інформаційна безпека" для 10-11 класів показує високий рівень відповідності навчальній програмі та забезпечення необхідної теоретичної бази. Розробки охоплюють важливі теми, такі як загрози інформаційній безпеці, методи захисту даних, основи криптографії та юридичні аспекти. Це створює міцний фундамент для формування в учнів знань із ключових питань сучасної кібербезпеки.

Разом із тим, матеріали не містять інноваційних елементів, які могли б суттєво покращити зацікавленість і мотивацію учнів, а саме:

- впровадження ігрових механік, як-от балів, рівнів чи змагань, які роблять навчання більш динамічним і емоційно залучаючим;
- використання платформ, популярних серед учнів (TikTok, Instagram), для створення інтерактивних завдань або поширення матеріалів у зручному форматі;
- залучення відеоматеріалів із графікою, анімацією чи реальними прикладами для пояснення складних тем, що полегшують сприйняття;
- моделювання реальних загроз або ситуацій, де учні можуть на практиці застосовувати отримані знання (наприклад, виявлення фішингових атак чи налаштування мережевої безпеки);
- використання навчання через створення персонажів або сценаріїв, які сприяють емоційному зв’язку з матеріалом і розвитку критичного мислення.

Додавання таких елементів зробить навчальний процес більш інтерактивним і адаптованим до потреб сучасних учнів, зокрема поколінь Z та альфа, які звикли до високого рівня технологій і візуальної взаємодії. Це також сприятиме розвитку практичних навичок і підвищенню їхньої мотивації до навчання.

Щоб зробити навчання з модуля "Інформаційна безпека" більш цікавим і сучасним, є сенс додати такі заохочувальні елементи:

- навчальні квести або рольові ігри, де учні виступають, наприклад, аналітиками безпеки, розслідуючи кібератаки;
- організація хакатонів або командних змагань із вирішення кейсів з кібербезпеки.
- короткі модулі чи задачі, які легко інтегрувати в щоденну рутину.
- розбір гучних випадків кібератак чи витоків даних.

2 МЕТОДИЧНІ ЗАСОБИ ЕФЕКТИВНОГО ВИКЛАДАННЯ МОДУЛЯ «ІНФОРМАЦІЙНА БЕЗПЕКА»

2.1 Використання гейміфікації у викладанні інформаційної безпеки

Гейміфікація у навчанні [6] – це використання ігрових елементів, принципів і механік для підвищення зацікавленості, мотивації та залучення учнів до навчального процесу. Це не означає, що навчання перетворюється на гру, але принципи гри, як-от досягнення цілей, змагання, рівні складності та винагороди, застосовуються для створення більш захопливого і продуктивного досвіду навчання.

Основні елементи гейміфікації.

Рейтинги та лідерборди (таблиці лідерів). Учні можуть змагатися між собою, отримуючи бали за виконання завдань або досягнення певних навчальних цілей. Таблиці лідерів показують, хто має найкращі результати, що стимулює учнів до покращення своїх показників. Це особливо ефективно у групових або командних проектах.

Нагороди та бейджі. Нагороди можуть бути віртуальними (наприклад, бейджі, медалі, сертифікати) або матеріальними (подарунки, призи). Бейджі можуть бути привласнені за досягнення певних віх, наприклад, за успішне завершення модулю з інформаційної безпеки чи за активність у класі.

Рівні складності. Завдання можуть мати різні рівні складності: від базових до складніших, що дозволяє учням просуватися через «рівні», подібно до відеоігор. Перехід до вищих рівнів після виконання поточних завдань або досягнення мети стимулює прогрес і допомагає учням відчувати свої досягнення.

Виконання місій та квестів. Це можуть бути комплексні завдання або проекти, які потрібно виконати, щоб отримати нагороду або просунутись далі. Місії можуть бути інтегровані в певний навчальний модуль, наприклад,

"захистити комп'ютерну мережу від атак" або "створити програму для захисту даних".

Зворотний зв'язок і досягнення. Важливо, щоб учні отримували зворотний зв'язок у реальному часі, коли вони виконують завдання або досягають мети. Це може бути через автоматичні оцінки в онлайн-системах або від вчителя. Завдяки такому підходу учні розуміють, що вони вже досягли або що ще треба вдосконалити.

Ігрові сценарії та рольові ігри (РПГ). Використання рольових ігор, де учні беруть на себе ролі різних персонажів або фахівців у галузі (наприклад, хакер, аналітик безпеки, криптограф), дає змогу реалізувати креативний підхід до навчання. У цьому контексті, інформаційна безпека може бути вивчена через захист мережі чи системи від нападів або розробку алгоритмів шифрування.

Переваги гейміфікації у навчанні:

Підвищення мотивації. Ігрові елементи роблять навчання більш захопливим і менш нудним. Учні відчувають себе залученими в процес і прагнуть досягти кращих результатів, щоб заробити більше балів або нагород.

Інтерактивність і залучення. Завдяки гейміфікації, учні активніше взаємодіють із матеріалом. Вони не просто пасивно слухають виклад, а активно працюють, виконуючи завдання, вирішуючи проблеми і проходячи місії.

Розвиток критичного мислення і співпраці. У гейміфікації часто є командні завдання, що сприяє розвитку комунікативних і командних навичок. Крім того, вирішення складних задач стимулює розвиток критичного мислення.

Персоналізація навчання. Гейміфікація дозволяє адаптувати завдання під рівень кожного учня. Це робить навчання більш доступним для різних груп учнів: від початківців до досвідчених.

Залучення до конкуренції та самовдосконалення. Використання рейтингових систем мотивує учнів змагатися за кращі результати, а також порівнювати свої досягнення з іншими.

2.2 Підхід у навчанні з використанням персонажів: персоніфікація навчального процесу

Персоніфікація у навчанні передбачає використання вигаданих персонажів, які виконують роль посередника або наставника в процесі викладання та засвоєння навчального матеріалу. Персонаж може бути як живою істотою, так і абстрактним, наприклад, у вигляді анімованого образу чи персонажа з мультиків, книг або ігор. Цей підхід сприяє створенню емоційної прив'язаності учнів до навчального процесу і активізує їхню мотивацію та зацікавленість у темі.

Персонаж, з яким учень "взаємодіє", робить процес навчання більш захопливим. Діти або студенти відчувають, що навчання є частиною пригоди чи гри. Так, персонаж може бути "героєм" певної історії або бути у вигляді симпатичного наставника, який допомагає вчити важливі уроки з інформатики чи іншої дисципліни.

Персонаж може виступати як пояснювач або демонстратор, спрощуючи складні ідеї і надаючи їм контекст. Наприклад, для теми "Інформаційна безпека" можна створити персонажа, який навчає учнів, як захищати дані від кібератак, і показує правильні стратегії безпеки через захоплюючу історію.

Персонаж, який має певні риси та характеристики (смішний, серйозний, добрий чи рішучий), може викликати емоційний відгук у учнів, що сприяє кращому засвоєнню інформації. Вони починають сприймати персонажа як вірного супутника у навчанні, що підвищує їх зацікавленість.

Створення персонажа, який адаптується до індивідуальних потреб і рівня знань учня, робить процес навчання персоналізованим. Наприклад, персонаж може задавати питання, на основі яких підбираються індивідуальні завдання для учня. Якщо учень показує високий рівень знань, персонаж може "підняти рівень складності", і навпаки.

Типи персонажів у навчанні.

Анімовані персонажі. Анімація надає можливість створювати віртуальних героїв або супутників, які можуть пояснювати матеріал через

діалоги, інтерактивні сцени або навіть мультфільми. Такі персонажі можуть бути використані для пояснення технологій, таких як комп'ютерні мережі або криптографія, де персонаж може "переводити" складні теоретичні поняття в простіше та цікаве пояснення.

Вигадані наставники. Це персонажі, які виконують роль вчителів або експертів у конкретній галузі. Наприклад, в контексті інформаційної безпеки, персонаж може бути кіберагентом, який навчить учнів, як працюють захисні механізми, або "хакером", який намагається зламати систему, але в процесі уроку вчить учнів важливих аспектів безпеки.

Історичні або міфологічні персонажі. Вони можуть бути адаптовані для навчальних цілей. Наприклад, можна створити персонажа, який базується на відомому історичному діячеві або міфологічному герої, що допомагає учням не тільки вчити матеріал, а й знайомитися з культурою, історією чи наукою.

Персонажі-роботи або штучний інтелект. Цей тип персонажа може використовуватися в сучасних освітніх технологіях, де "боти" або штучні інтелекти взаємодіють з учнями, відповідаючи на питання, допомагаючи з виконанням завдань або надаючи допомогу у вирішенні проблем.

Персонажі можуть бути частинами великих навчальних історій чи пригод. Наприклад, учень може виконувати завдання разом з персонажем, як у квесті або грі. Вони разом можуть вирішувати різні проблеми, долати перешкоди або вивчати нові концепції.

Створення ролевих ігор з використанням персонажів дозволяє учням "вжитися" в обрану роль і дізнатися більше про певні аспекти навчання. Наприклад, для теми кібербезпеки можна організувати гру, де учень має виступати як системний адміністратор, що захищає мережу, чи як "хакер", що намагається проникнути в систему.

Онлайн-курси та платформи можуть використовувати персонажів для взаємодії з учнями. Персонаж може вести уроки, надавати поради, задавати питання чи допомагати у виконанні вправ, створюючи таким чином більш персоналізоване та захоплююче навчання.

Відео або анімації з персонажами, які допомагають пояснювати певні теми. Наприклад, використання анімацій для візуалізації складних тем у програмуванні або кібербезпеці, де персонажі виконують різні завдання або пояснюють принципи роботи програм.

Використання персонажів у навчанні дозволяє зробити процес навчання більш захоплюючим, персоналізованим і ефективним. Це дозволяє інтегрувати гейміфікацію в навчальний процес, підвищує мотивацію учнів і сприяє кращому засвоєнню складних матеріалів. Персоніфікація навчання через персонажів – це потужний інструмент для створення позитивного, інтерактивного та продуктивного навчального середовища.

2.3 Інтерактивні платформи для підвищення мотивації учнів

Впровадження таких платформ, як Kahoot!, Blooket, Quizizz, а також національної платформи Всеосвіта, дозволяє трансформувати традиційний підхід до навчання, інтегруючи змагальні елементи, рейтингування та систему винагород. Такий підхід не лише підтримує інтерес учнів, а й створює умови для глибшого засвоєння матеріалу через активну участь і взаємодію.

Kahoot! [17] – це платформа для створення інтерактивних вікторин, тестів і опитувань, яка активно використовує елементи гейміфікації для залучення учнів до навчального процесу. Це один із найбільш відомих інструментів для використання у класі, який активно підтримує елементи співпраці, конкуренції і захоплюючого навчання.

Вчителі можуть створювати опитування та вікторини з варіантами відповідей. Питання можуть бути одно- або багатоваріантними, і учні повинні вибрати правильний варіант за обмежений час.

Учні можуть бачити на екрані свої результати в реальному часі, що додає елемент змагання.

В кожному питанні є таймер, який обмежує час на відповідь, додаючи елемент терміновості та емоційного напруження.

Після кожного раунду з’являються лідери, що створює дух змагання серед учнів. Лідерборд мотивує учнів працювати швидше та ефективніше.

Платформа дозволяє візуально оцінити успіхи учнів, зокрема через кольорові індикатори і позначення за правильні або неправильні відповіді, дозволяє використовувати наявні шаблони або створювати власні ігри, що робить її надзвичайно гнучкою для будь-яких навчальних завдань.

Blooket [18] – це інноваційна освітня платформа, що інтегрує елементи відеоігор і навчання. Вона дозволяє створювати вікторини та інші типи ігор для перевірки знань учнів.

Blooket пропонує декілька різних ігрових режимів, таких як "Tower Defense", "Gold Rush" і "Crypto Hack". Кожен режим має свою унікальну механіку, що дозволяє зберегти інтерес учнів протягом усього уроку.

Учні можуть змагатися в іграх, відповідаючи на питання в рамках певної теми, що робить навчання захоплюючим і дозволяє учням активно взаємодіяти з матеріалом.

Викладачі можуть створювати власні питання для вікторин, а також вибирати підходящі ігрові формати для своїх учнів. Як і в більшості ігрових платформ, учні заробляють бали за правильні відповіді. Ці бали можна використовувати для розвитку персонажів чи вигравання призів у межах гри.

Деякі ігри у Blooket передбачають командну роботу, що стимулює учнів до колективної діяльності.

Гейміфікація в Blooket ефективно поєднує навчальний процес з елементами стратегічної гри, де кожен учень може обрати свій підхід до перемоги, покращуючи при цьому свої знання та навички.

Quizizz [19] – це ще одна платформа для створення тестів та вікторин, що активно використовує елементи гейміфікації, створюючи інтерактивне та конкурентне середовище для учнів.

Quizizz дозволяє створювати тести, що включають різні типи запитань, від мультивибору до відкритих запитань, а також поєднувати різні формати в одному тесті.

У Quizizz можна проводити вікторини в реальному часі, де учні можуть бачити лідерборд під час гри, або давати можливість проходити тести в індивідуальному темпі.

За правильні відповіді учні отримують бали, і ці бали миттєво відображаються на екрані. Лідери з’являються в кінці гри, що мотивує учнів до покращення своїх результатів.

Викладачі можуть бачити детальну статистику по кожному учню, що дозволяє проводити аналіз їх результатів і коригувати подальший навчальний процес.

Платформа використовує нагороди та анімації, щоб зробити процес навчання більш цікавим та захоплюючим. Таким чином, Quizizz створює умови для здорової конкуренції, водночас даючи можливість кожному учню пройти тест у комфортному для себе темпі.

Всеосвіта [20] – це українська онлайн-платформа для навчання, яка включає в себе тестування, завдання для самостійної роботи та інтерактивні ресурси. Платформа застосовує елементи гейміфікації, щоб зробити процес навчання більш інтерактивним і захоплюючим для учнів.

Учні можуть проходити тести з різних дисциплін, де є можливість отримувати миттєвий зворотний зв'язок щодо результатів. Платформа дозволяє викладачам створювати індивідуальні завдання для кожного учня залежно від рівня їх підготовки. Учні отримують бали та нагороди за успішне виконання завдань, що мотивує до подальшої активності. Викладачі можуть отримувати детальні звіти про успіхи своїх учнів, що дозволяє відстежувати прогрес і коригувати навчальний план. Учні можуть заохочуватись нагородами та отримувати звання за успішне виконання завдань, що підтримує їх мотивацію.

Всеосвіта впроваджує прості, але ефективні елементи гейміфікації для заохочення учнів до навчання, при цьому зберігаючи фокус на традиційних освітніх цілях.

Усі ці платформи використовують різноманітні механізми гейміфікації, що допомагають зробити навчання більш захоплюючим і мотиваційним. Вони поєднують традиційні навчальні методи з елементами відеоігор, що дозволяє створити змагальну та взаємодієву атмосферу, яка сприяє глибшому засвоєнню матеріалу. Використання таких інструментів дозволяє підвищити рівень залученості учнів та зробити навчальний процес більш ефективним та цікавим.

2.4 Інтеграція персоніфікації та гейміфікації у навчальний процес

Інтеграція гейміфікації та персоніфікації у навчальний процес може значно підвищити ефективність уроків, збільшити мотивацію учнів і допомогти їм краще засвоювати матеріал. У додатках А, Б, В, Г наведено приклади уроків з модулю «Інформаційна безпека» на теми: «Основні поняття в області безпеки інформаційних технологій. Основні причини загострення проблеми забезпечення безпеки інформаційних технологій», «Криптографічні методи захисту інформації», «Керування механізмами захисту та виявлення атак у комп'ютерних мережах», та «Політика безпеки при доступі до мережі загального користування. Системи аналізу вмісту поштового і веб-трафіку. Віртуальні приватні мережі (VPN» з використанням персонажа Ліса Гарда (рис. 2.1).

Ліс Гард – віртуальний наставник для учнів з інформаційної безпеки. Він створений для проведення уроків з модулю «Інформаційна безпека». Ліс Гард є гнучким персонажем, який адаптується до потреб учнів і надає їм персоналізовану підтримку.



Рисунок 2.1 – Персонаж ліс Гард

Він може змінювати свої поради та рівень складності завдань в залежності від рівня знань кожного учня. Для учнів, які потребують додаткової підтримки, Ліс може пропонувати простіші завдання, а для більш підготовлених складніші.

Персонаж надає мотиваційні коментарі після виконання кожного завдання, що допомагає учням залишатися мотивованими і зосередженими. Він також дає персоналізовані поради на основі результатів роботи учнів.

Ліс також є частиною ігрової історії, де учні допомагають йому розв'язати проблеми, пов'язані з інформаційною безпекою, і отримують нагороди за кожен етап або правильну відповідь.

Для інтеграції гейміфікації у навчальний процес після викладання теоретичного матеріалу учням пропонується проходження ігор на платформах Kahoot, Все освіта, Blooket та на інтерактивній дошці Miro. Цей етап допомагає закріпити отримані знання в інтерактивній та захопливій формі, стимулюючи активність, змагання та колективну участь.

Для проведення гри вчитель реєструється або входить у свій обліковий запис на платформі Kahoot. Створює новий тест з теми "Основні поняття в області безпеки інформаційних технологій" (рис. 2.2).

Додає запитання з варіантами відповідей (типи запитань: тест, правда/неправда, упорядкування тощо).

Налаштовує тривалість відповіді на кожне запитання (зазвичай 20–30 секунд).

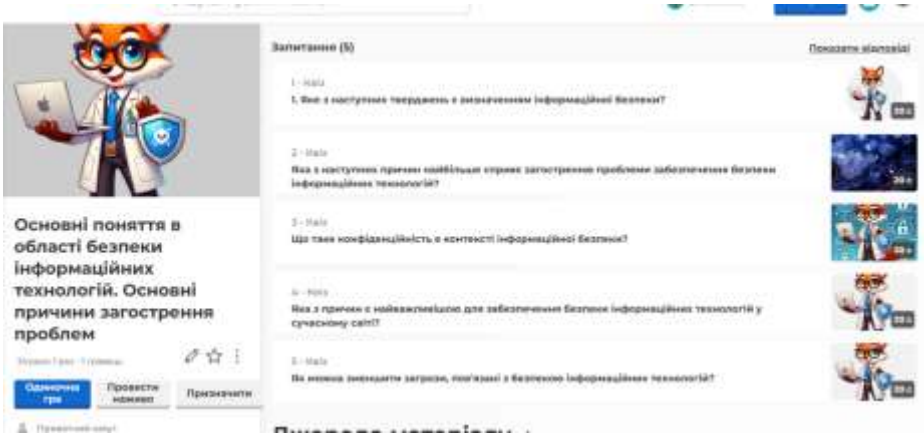


Рисунок 2.2 – Питання гри на платформі Kahoot

Зберігає тест і готує код гри для запуску. Далі через проектор або інтерактивну дошку вчитель демонструє головний екран гри (із сайту Kahoot).

Запускає гру в режимі "Classic" (індивідуальна гра) або "Team Mode" (групова гра). Отримує унікальний PIN-код гри. Учні заходять на сайт kahoot.it або через мобільний додаток Kahoot. Вводять PIN-код та своє ім’я або псевдонім.

Вчитель перевіряє список підключених учасників, за потреби коментує вибір імен для дотримання етики. Вчитель запускає перше запитання. На екрані відображається запитання та варіанти відповідей із кольоровими кнопками (відповідники кольорів: червоний, синій, зелений, жовтий). Учні обирають правильну відповідь на своїх пристроях. Після завершення часу (або вибору відповідей) вчитель демонструє правильну відповідь, пояснюючи її, якщо потрібно.

Система автоматично нараховує бали за правильність і швидкість відповіді.

На екрані з’являється таблиця лідерів після кожного запитання. Після останнього запитання система формує остаточний рейтинг учасників.

Вчитель вітає переможців і обговорює складні запитання, на які учні відповіли неправильно.

Закріплення знань з криптографічних алгоритмів пропонується здійснити проведенням веб-квесту в рамках укроку з теми «Криптографічні методи захисту інформації» (додаток Б) на платформі Всеосвіта (рис.2.3).

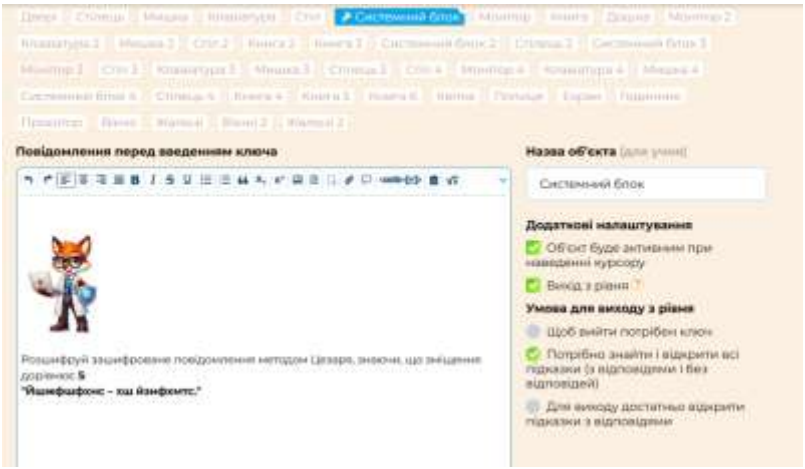


Рисунок 2.3 – Процес створення вебквесту на платформі Всеовіта

Учитель знайомить учнів із темою та цілями вебквесту. Розповідає про платформу Всеосвіта, як працювати з інтерфейсом, вводити відповіді та орієнтуватися на етапах квесту. Учні отримують доступ до квесту через посилання або код. Учні працюють самостійно, проходячи завдання один за одним.

Типові завдання:

– розшифрувати повідомлення за допомогою шифру Цезаря:

– знайти ключ до повідомлення, використовуючи алгоритм XOR;

– відновити фразу, зашифровану за алгоритмом RSA;

– завдання на пошук інформації: наприклад, визначити історичний метод шифрування, який використовували під час Другої світової війни.

Платформа автоматично перевіряє відповіді та показує учасникам результати кожного етапу.Учитель у режимі реального часу відстежує, як учні проходять завдання, бачить їхні результати та може надати підказки.

Після завершення всіх завдань платформа формує загальний рейтинг учасників. Учитель оголошує переможців і пояснює складні моменти, якщо вони виникли.Такі квести не лише поглиблюють знання учнів, а й розвивають їхні аналітичні, дослідницькі та командні навички.

При проведенні уроку «Керування механізмами захисту та виявлення атак у комп'ютерних мережах» (додаток В) пропонується проведення мозкового штурму "Захист фортеці" на інтерактивній дошці Miro з метою розвитку навичок командної роботи, стратегічного мислення, аналізу та вирішення проблем у сфері кібербезпеки (рис. 2.4).



Рисунок 2.4 – Інтерактивна карта для проведення мозкового штурму на дошці Miro

Учні поділяються на 3–4 команди по 3–4 учасники. Кожна команда отримує роль:

– захисники периметра (захист зовнішніх зон);
– аналітики серверної зони (робота із внутрішніми загрозами);
– інженери комунікацій (забезпечення безпеки каналів зв’язку);

На дошці Miro представлено інтерактивну карта фортеці, яка містить:

– периметр (стіни, ворота, датчики руху);
– центральна зона (серверна кімната);
– критичні точки (вхід, канали зв’язку, енергопостачання).

Викладач дає короткий опис умов:

– можливі загрози: вірусні атаки, DDoS-атаки, внутрішні інсайдери;

– цілі: виявити загрози, захистити критичні точки, підтримати стійкість системи.

Кожна команда створює план захисту. Позначає на карті Miro свої зони відповідальності. Вносить ідеї у вигляді стікерів або малюнків. Викладач вводить сценарії атак (напр., зараження вірусом, DDoS-атака). Команди оперативно реагують, пропонуючи рішення:

– захисники периметра описують, як зупинити загрозу на вході;
– аналітики знаходять заражені системи;
– інженери відновлюють комунікації.

Теоретична база з уроку на тему "Політика безпеки при доступі до мережі загального користування. Системи аналізу вмісту поштового і веб-трафіку. Віртуальні приватні мережі (VPN)" (додаток Г) закріплюється проведенням гри на платформі Blooket (рис. 2.5).

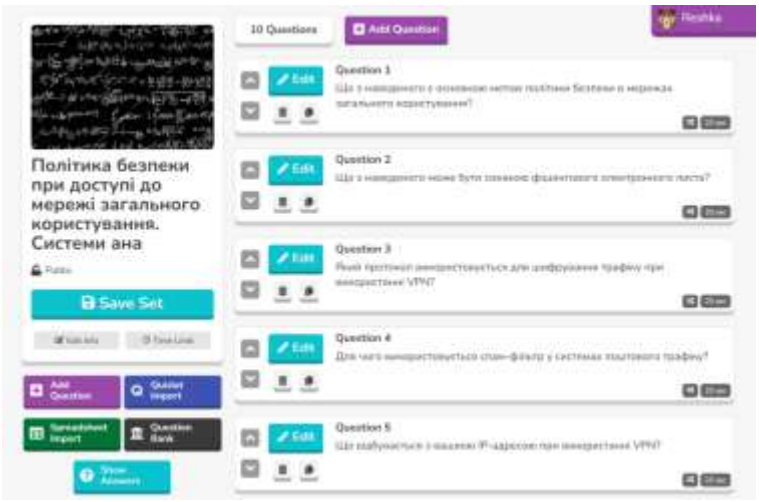


Рисунок 2.5 – Питання для проведення гри на платформі Blooket

Розроблена гра містить питаннями, що охоплюють всю теорію з теми.

Для проведення гри викладач обирає у Blooket формат гри Crypto hack. Учні отримують код гри для nf підключаються до гри. Викладач пояснює правила. Під час гри викладач коментує відповіді та додає пояснення.

Гра завершується, коли закінчується час. Blooket автоматично показує результати: найуспішніших гравців і загальний рейтинг.

3 ЕКСПЕРИМЕНТАЛЬНА ПЕРЕВІРКА ЕФЕКТИВНОСТІ МЕТОДИКИ ВИКЛАДАННЯ ВИБІРКОВОГО МОДУЛЮ «ІНФОРМАЦІНА БЕЗПЕКА»

3.1 Організація проведення експериментальної перевірки

З метою перевірки ефективності розробленої методики було проведено педагогічний експеримент. Експеримент здійснювався згідно з основними положеннями реалізації цього емпіричного дослідження [21, 22]. В експерименті взяли участь учні двох класів 10-А (15 учень), 10-Б (12 учнів). Дві групи експериментальна та контрольна були отримані згідно з поділом учнів на підгрупи, заняття в яких проводили різні вчителі. В експериментальній групі (ЕГ) 15 учнів, а в контрольній (КГ) – 12.

Педагогічний експеримент проходив в наступні етапи: підготовчий, констатувальний, формувальний і контрольний.

Підготовчий етап експерименту полягав у вивченні наукових джерел та методичних публікацій з метою розробки методики навчання вибіркового модулю «Інформаційна безпека». Також на цьому етапі здійснювалася підготовка наступних тестів: тест до вибіркового модулю «Інформаційна безпека»; тесту залишкових знань з таких тем (вивчаються в 5–9 класах): «Мережні технології та Інтернет», «Служби Інтернету», «Основи інформаційної безпеки».

Перш ніж здійснювати експеримент були розроблені тестові завдання з вибіркового модуля «Інформаційна безпека». Вихідний тест складався з 15 тестових завдань (додаток Д). Результати проведення пробного тестування за допомогою тесту, що складається з 15 тестових завдань, наведено в табл.Е.1 (додатку Е). Згідно з отриманими показниками складності тестових завдань виявилося, що тестові завдання 1, 4, 6, 12, 13 занадто прості. Тому їх було вилучено з тесту. Згідно з вимогами класичної теорії тестування [23] тестові завдання були перерозподілені згідно з рис. 3.1.

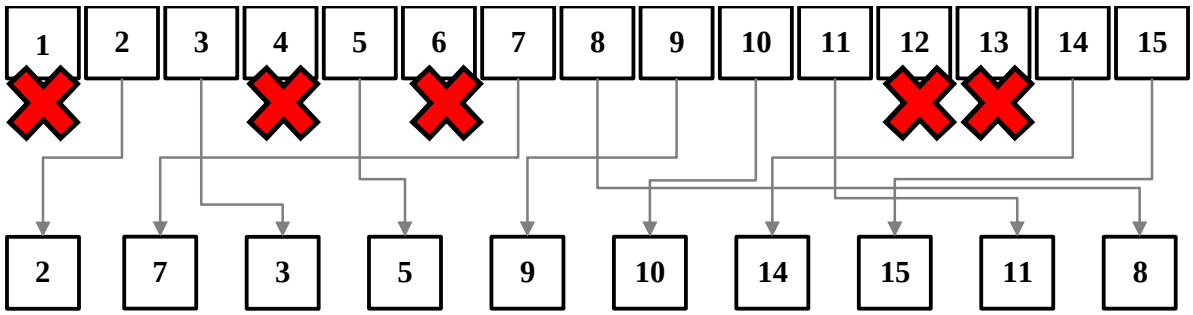


Рисунок 3.1 – Перерозподіл тестових завдань вихідного тесту

У результаті було отримано тест, представлений в додатку Є.

На *констатувальному етапі* було здійснено порівняння груп на основі перевірки залишкових знань учнів. Здійснювалася перевірка однорідності відібраних груп. Для цього застосовувалися методи математичної статистики: порівняння розподілів, описовий аналіз та перевірка статистичної гіпотези. На заключному етапі здійснювалося узагальнення отриманих результатів розрахунків.

На *формувальному етапі* здійснювалося навчання учнів експериментальної групи на основі розробленої в кваліфікаційній роботі методики. Ознайомлення з думкою учнів довело, що для них найбільш цікавими виявилися такі методи навчання: квест, навчальні ігри, мозковий штурм в ігровій формі.

На рис. 3.2 представлено один з етапів проходження учнями квесту.

Інші завдання – проходження гри на платформі Kahoot (рис. 3.3), Blooket (рис. 3.4) та проведення мозкового штурму на інтерактивнй дошці Miro (рис. 3.5).

На *контрольному етапі* експерименту було проведено аналіз результатів тестування (додаток Ж), після вивчення модулю «Інформаціна безпека».

Для оцінки рівня засвоєння модулю учнями використовувалися методи математичної статистики. Дослідження охопило такі статистичні характеристики: частотні показники за різними оцінками, середні значення

оцінок тестування та розкид результатів тестування. Для порівняння навчальних досягнень різних груп учнів (ЕГ і КГ) застосовувався непараметричний статистичний критерій Манна-Вітні.

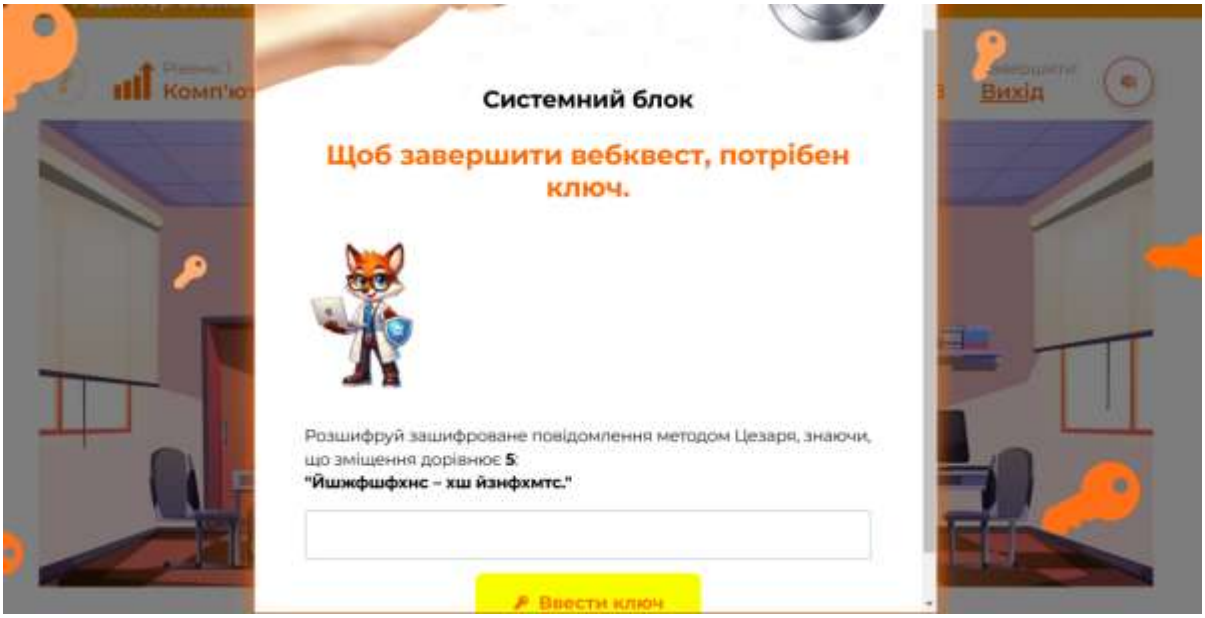


Рисунок 3.2 – Проходження учнями веб-квесту

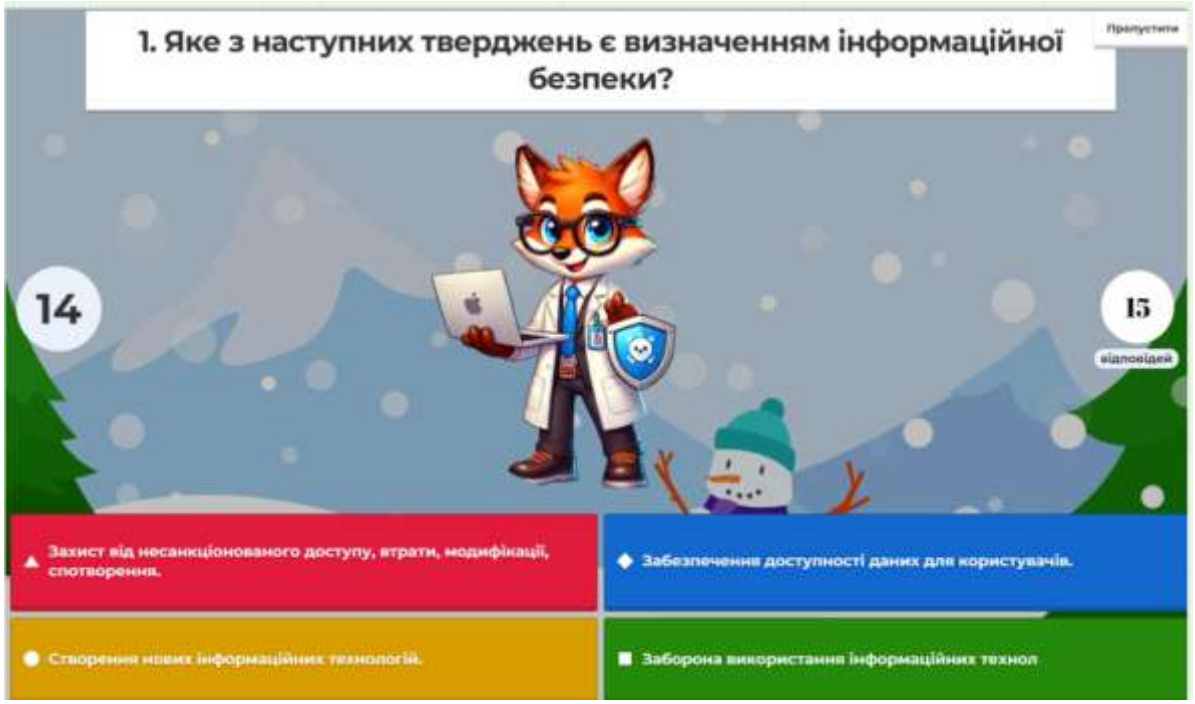


Рисунок 3.3 – Проходження гри на платформі Kahoot



Рисунок 3.4 – Результати проходження гри на Blooket



Рисунок 3.5 – Результат проведення мозкового штурму на Miro

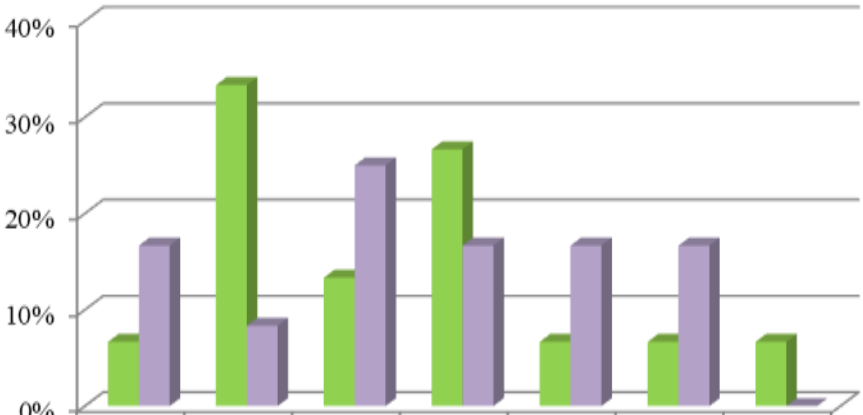
У наступному розділі представлено результати проведеного статистичного аналізу.

3.2 Аналіз результатів експериментального дослідження ефективності викладання модулю

Згідно з правилами здійснення педагогічного експерименту на початку його проведення була перевірена однорідність двох відібраних груп. Перевірці піддавалися результати тестування залишкових знань учнів з тем (5–9 класи): «Мережні технології та Інтернет», «Служби Інтернету», «Основи інформаційної безпеки». Результати тестування наведені у табл. И.1 (додаток И).

Результати констатувального етапу.

На основі отриманих даних оцінювання були визначені частотні показники. Як видно з діаграми (рис. 3.6) розподіл учнів за оцінками в обох групах – неоднорідний. Так в експериментальній групі найбільші кількість учнів отримала оцінку 6, на другому місті кількість учнів з оцінкою 8, а кількість учнів з оцінками 5, 9, 10, 11 – однакова (найменша). В контрольній групі: найбільша кількість учнів отримали оцінку 7, найменша – 6, а розподіл за оцінками 5, 8, 9, 10 – рівномірний.



	5	6	7	8	9	10	11
ЕГ	6,7%	33,3%	13,3%	26,7%	6,7%	6,7%	6,7%
КГ	16,7%	8,3%	25,0%	16,7%	16,7%	16,7%	0,0%

Рисунок 3.6 – Гістограма розподілу учнів за оцінками тестування на констатувальному етапі педагогічного експерименту

За результатами тестування залишкових знань були обчислені описові статистичні показники оцінок: середнє, дисперсія, стандартне відхилення та коефіцієнт варіації. Всі обчислення здійснювалися за формулами математичної статистики [24]. Зведені результати наведено у табл. 3.1. Порівняння отриманих показників свідчить, що середні значення оцінок в обох групах майже ідентичні: ЕГ – 7,40, а в КГ – 7,58. Показники мінливості, доводять, що в обох групах оцінки однорідні, оскільки дисперсія, стандартне відхилення та коефіцієнт варіації майже ідентичні.

Таблиця 3.1 – Результати описового статистичного аналізу (констатувальний етап)

Показник	ЕГ	КГ
Середнє	7,40	7,58
Дисперсія	2,83	2,99
Стандартне відхилення	1,68	1,73
Коефіцієнт варіації	22,7%	22,8%

Незважаючи на те, що порівняльний аналіз статистичних показників доводить однорідність двох груп, необхідно провести перевірку статистичних гіпотез.

Формулювання статистичних гіпотез:

H_0: На констатувальному етапі експерименту між результатами оцінювання учнів контрольної та експериментальної груп існують лише випадкові розбіжності.

H_0: На констатувальному етапі експерименту між результатами оцінювання учнів контрольної та експериментальної груп існують невипадкові розбіжності.

Для перевірки гіпотез застосовується критерій Манна-Вітні, який обчислюється за формулою (3.1) [25].

$$U_{\text{емп}} = (n_1 \cdot n_2) + \frac{n_x \cdot (n_x + 1)}{2} - T_x, \quad (3.1)$$

де n_1 і n_2 – обсяги вибірок;

n_x – обсяг вибірки з більшою ранговою сумою;

T_x – найбільша з двох рангових сум.

У результаті визначення суми рангів було визначено, що найбільші сума рангів 217,5 в експериментальні групі (табл. Ж.2, Додаток Ж). Відповідно були проведені обчислення емпіричного значення критерія Манна-Вітні:

$$U_{\text{емп}} = (15 \cdot 12) + \frac{15 \cdot (15+1)}{2} - 217{,}5 = 180 + 120 - 217{,}5 = 82{,}5.$$

Знайдене по таблицям критичне значення критерія Манна-Вітні: $U_{\text{кр}} = 55$ (на рівні значущості $\alpha > 0{,}05$). Оскільки $U_{\text{емп}} > U_{\text{кр}}$, то приймається нульова гіпотеза. Отже, на констатувальному етапі експерименту доведено, що між результатами експериментальної та контрольної груп існують лише випадкові розбіжності. Це свідчить про однорідність двох відібраних груп.

Після формувального етапу експерименту були отримані оцінки учнів, які наведені в табл. И.3 (Додаток И).

Результати контрольного етапу.

Частотні показники розподілу учнів згідно з оцінками свідчать, що в експериментальній групі значно збільшилася кількість учнів з високими оцінками (рис. 3.8): зникли учні з оцінками 6 (на 6,7%); на 26,7% зменшилася кількість учнів з оцінкою 7; не змінилася кількість учнів з оцінкою 8; на 6,7% збільшилася кількість учнів з оцінкою 9; на 13,3% збільшилася кількість учнів з оцінкою 10; на 6,7% збільшилася кількість учнів з оцінкою 11; на 6,7% збільшилася кількість учнів з оцінкою 12. Водночас в контрольній групі динаміка не настільки виразна: не змінилася кількість учнів з оцінкою 6; на 16,7% збільшилася кількість учнів з оцінкою 7; на 8,3% збільшилася кількість учнів з оцінкою 8; на 8,3% зменшилася кількість учнів з оцінкою 9; на 8,3%

зменшилася кількість учнів з оцінкою 10; на 8,3% зменшилася кількість учнів з оцінкою 11.

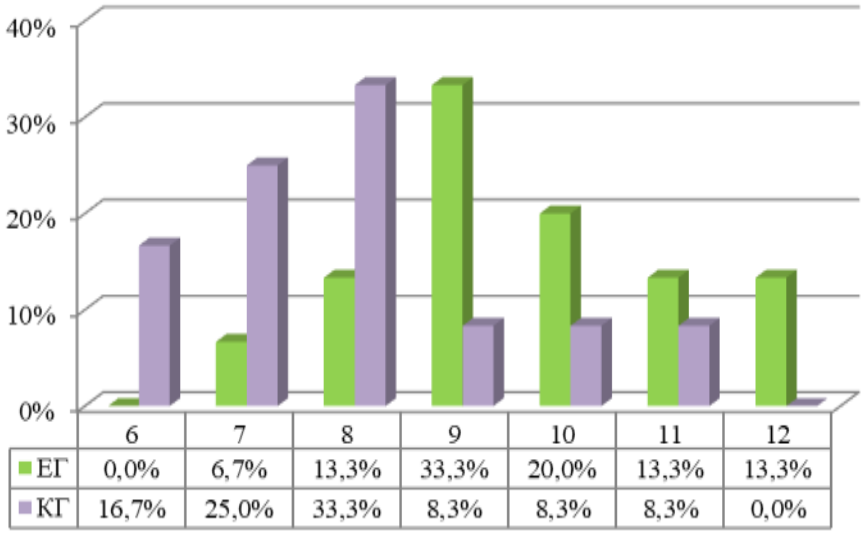


Рисунок 3.8 –Гістограма розподілу учнів за оцінками на контрольному етапі педагогічного експерименту

Обчислені описові статистичні показники наведені у табл. 3.2. Середні значення оцінок в групах розрізняються: ЕГ – 9,20, а в КГ – 7,92. Показники мінливості в обох групах стали меншими, однак в експериментальній групі оцінки більш однорідні.

Таблиця 3.2 – Результати описового статистичного аналізу (контрольний етап)

Показник	ЕГ	КГ
Середнє	9,60	7,92
Дисперсія	2,11	2,27
Стандартне відхилення	1,45	1,51
Коефіцієнт варіації	15,1%	19,0%

Перевірка статистичних гіпотез здійснювалася аналогічно за критерієм Манна-Вітні.

Формулювання статистичних гіпотез:

H_0: На контрольному етапі експерименту між результатами оцінювання учнів контрольної та експериментальної груп існують лише випадкові розбіжності.

H_0: На контрольному етапі експерименту між результатами оцінювання учнів контрольної та експериментальної груп існують невипадкові розбіжності.

На основі розрахунку сум рангів була визначена найбільші сума рангів – 221,5 в контрольній групі (табл. Ж.4, Додаток Ж). Обчислення емпіричного значення критерія Манна-Вітні:

$$U_{\text{емп}} = (15 \cdot 12) + \frac{12 \cdot (12+1)}{2} - 221{,}5 = 180 + 96 - 221{,}5 = 54{,}5.$$

Для критичного значення критерія Манна-Вітні $U_{\text{кр}} = 55$ $U_{\text{емп}} < U_{\text{кр}}$, тому нульова гіпотеза відхиляється і приймається альтернативна гіпотеза. Отже, на контрольному етапі експерименту між результатами експериментальної та контрольної груп існують невипадкові розбіжності.

Щоб додатково впевнитися в ефективності розробленої методики необхідно порівняти результати експериментальної групи на етапах експерименту. Для порівняння зв’язаних груп зазвичай застосовують непараметричні критерії знаків або Вілкоксона. Також можна за допомогою критерія Манна-Вітні порівняти зсуви, які сталися в обох групах.

Формулювання статистичних гіпотез:

H_0: У змінах в оцінках учнів обох груп на етапах експерименту існують лише випадкові розбіжності.

H_0: У змінах в оцінках учнів обох груп на етапах експерименту існують невипадкові розбіжності.

На основі розрахунку сум рангів була визначена найбільші сума рангів – 226 в експериментальній групі (табл. Ж.5, Додаток Ж). Обчислення емпіричного значення критерія Манна-Вітні:

$$U_{\text{емп}} = (15 \cdot 12) + \frac{12 \cdot (12+1)}{2} - 226 = 180 + 96 - 226 = 50.$$

Для критичного значення критерія Манна-Вітні $U_{\text{кр}} = 55$ $U_{\text{емп}} < U_{\text{кр}}$, тому нульова гіпотеза відхиляється і приймається альтернативна гіпотеза.

Отже, проведений статистичний аналіз результатів педагогічного експерименту свідчить про ефективність викладання вибіркового модуля «Інформаціїна безпека».

ВИСНОВКИ

У ході проведеного дослідження було досягнуто поставлену мету – розроблено та обґрунтовано засоби і методи ефективного викладання вибіркового модуля «Інформаційна безпека», що сприятимуть формуванню практичних навичок і компетентностей у сфері захисту інформації.

На основі аналізу сучасного стану проблеми викладання тематики інформаційної безпеки в освіті визначено ключові труднощі: недостатнє методичне забезпечення, обмежений доступ до практичних ресурсів, недостатня адаптація матеріалів до української системи освіти та стрімкий розвиток кіберзагроз. Це обґрунтовує актуальність дослідження та необхідність впровадження інноваційних методик викладання.

У дослідженні було розглянуто дидактичні принципи та методичні підходи, які дозволяють підвищити ефективність навчання. Визначено, що інтеграція сучасних засобів навчання, зокрема цифрових інструментів, моделювання реальних ситуацій та інтерактивних методів, значно підвищує зацікавленість учнів та якість засвоєння матеріалу.

Розроблена модель викладання вибіркового модуля «Інформаційна безпека» включає:

- використання інтерактивних платформ для теоретичного навчання;
- впровадження практичних завдань для розвитку навичок виявлення загроз і захисту інформації;
- симуляцію реальних кіберзагроз для формування стійкості до зовнішніх викликів.

Педагогічний експеримент підтвердив ефективність запропонованих методик. Учні, які навчалися за оновленим підходом, демонстрували вищі результати у тестуванні та практичних завданнях порівняно з контрольною групою. Це доводить, що розроблена система сприяє якісному формуванню знань і практичних умінь.

У результаті сформульовано практичні рекомендації для викладачів, які включають:

- використання інтерактивних ігрових методів для пояснення теоретичних аспектів.
- впровадження методу мозкового штурму для закріплення практичних навичок.
- регулярне оновлення змісту модуля відповідно до нових загроз і технологій.

Висновки дослідження підтверджують, що успішне викладання модуля «Інформаційна безпека» не лише формує критично важливі компетентності, але й сприяє підвищенню загальної цифрової грамотності учнів та їхньої готовності до викликів сучасного світу.

ПЕРЕЛІК ПОСИЛАНЬ

1. Комплекти для проведення уроків інформатики в 10(11) класі. Рівень стандарту. Вибірковий модуль "Інформаційна безпека" URL : https://teach-inf.com.ua/load/vibirkovi_moduli_10_11_klas/informacijna_bezpeka/135 (дата звернення: 05.09.2024).

2. Готові презентації та конспекти уроків. URL : https://vsimpptx.com/author/informatika-10-11-klas-modul-informacijna-bezpeka (дата звернення : 04.10.2024).

3. Інформаційна безпека. URL : http://surl.li/qqczgl (дата звернення : 04.10.2024).

4. Коваленко О. П. Інноваційні методи навчання у старшій школі : навчальний посібник. Київ : Освіта, 2021. 256 с.

5. Петрова М. С. Використання інформаційних технологій у процесі викладання у старшій школі. *Інформаційні технології в освіті*. 2022. № 2. С. 14–21.

6. Іванов А. М. Гейміфікація у навчанні: новий погляд на методику викладання. *Збірник матеріалів міжнародної науково-практичної конференції "Освіта і цифровий світ"*. Харків : ХНУ ім. Каразіна, 2023. С. 43–46.

7. Сидоренко Н. Г. Інтерактивні технології як засіб активізації навчального процесу. Інноваційна педагогіка: теорія і практика. Київ : Либідь, 2020. С. 120–135.

8. Романенко В. Г. Технології формування критичного мислення у старшій школі. Освітній портал «Наука і школа». 2023. URL : https://www.nauka-i-shkola.ua/information. (дата звернення : 04.10.2024).

9. Бондаренко О. М. Сучасні інноваційні технології навчання у старшій школі: теорія і практика. *Педагогічний альманах*. 2022. № 4. С. 37–42.

10. Сидоренко Н. П. Гейміфікація як метод активізації навчального процесу в старшій школі. *Інноваційна освіта*. 2021. № 6. С. 25–30.

11. Іваненко О. А. Цифрові трансформації у шкільній освіті: інноваційні методи і технології: монографія. Харків : Ранок, 2020. 320 с.

12. Петрова М. В. Компетентнісний підхід у старшій школі: теорія і практика: монографія. Київ : Освіта України, 2022. 288 с.

13. Смирнова Л. Г. Використання інтерактивних методів у викладанні природничих дисциплін у старшій школі. *Матеріали Всеукраїнської науково-практичної конференції «Освіта в умовах цифровізації»*. Київ: НПУ ім. М. П. Драгоманова, 2023. С. 49–53.

14. Іванов Д. О. Цифрові інструменти в освітньому середовищі старшої школи. *Збірник тез доповідей міжнародної конференції «Цифрова освіта: виклики і перспективи»*. Львів : ЛНУ ім. І. Франка, 2023. С. 88–92.

15. Коваленко П. Сучасні інноваційні технології в шкільній освіті. Освіта XXI століття. 2023. URL : osvita21.com/innovations (дата звернення : 04.10.2024).

16. Лисенко А. Технології змішаного навчання у старшій школі. Освітній портал «Всеосвіта». 2022. URL : vseosvita.ua/edtech (дата звернення : 04.10.2024).

17. Інтерактивна платформа Kahoot. URL : https://kahoot.com/ (дата звернення : 04.10.2024).

18. Геімфікована платформа Blooket. URL : https://dashboard.blooket.com (дата звернення : 04.10.2024).

19. Інтерактивна платформа Quizizz. URL : https://quizizz.com/ (дата звернення : 04.10.2024).

20. Всеосвіта. Національна освітня платформа. URL : https://vseosvita.ua/ (дата звернення : 04.10.2024).

21. Андрєєв А. М., Пшенична О. С. Методологія наукових досліджень : навчальний посібник для здобувачів ступеня вищої освіти магістра спеціальності «Середня освіта» освітньо-професійної програми «Середня

освіта (Інформатика)». Запоріжжя : Запорізький національний університет, 2024. 145 с.

22. Сисоєва С. О., Кристопчук Т. Є. Методологія науково-педагогічних досліджень : підруч. Рівне : Волинські обереги, 2013. 359 с.

23. Вимірювання в освіті : підручник / за ред. О. В. Авраменко. Кіровоград : Лисенко В. Ф., 2011. 360 с., с. 138

24. Руденко В. М. Математична статистика : навч. посіб. Київ : Центр учбової літератури, 2012. 304 с., с. 36–40.

25. Руденко В. М. Математична статистика : навч. посіб. Київ : Центр учбової літератури, 2012. 304 с., с. 196

ДОДАТОК А

Урок на тему: "Основні поняття в області безпеки інформаційних технологій. Основні причини загострення проблеми забезпечення безпеки інформаційних технологій"

Мета уроку:

1. Ознайомити учнів з основними поняттями та термінами в області безпеки інформаційних технологій.
2. Визначити основні причини загострення проблеми забезпечення безпеки інформаційних технологій.
3. Використовувати елементи персоніфікації матеріалу для підвищення зацікавленості та залученості учнів.

Обладнання:

1. Презентація PowerPoint.
2. Інтерактивна дошка або проектор.
3. Картки для групової роботи (для обговорення причин загострення проблеми безпеки).
4. Віртуальний помічник – персонаж "Ліс Гард", спеціаліст з кібербезпеки (створений для персоніфікації навчання).

Хід уроку:

1. Організаційний момент (5 хв)

Вітання.

Ознайомлення учнів з метою та завданнями уроку.

Коротке введення до теми: чому проблема безпеки в інформаційних технологіях є настільки важливою у сучасному світі?

2. Введення в тему та персоніфікація (10 хв)

Викладач представляє персонажа Ліса Гарда – спеціаліста з кібербезпеки, який допоможе учням зрозуміти, що таке безпека інформаційних технологій і чому вона важлива.

Ліс Гард: "Привіт! Я Ліс Гард, і сьогодні я буду вашим провідником у світі безпеки інформаційних технологій. Подібно до того, як ми захищаємо свій дім, ми повинні захищати наші дані та інформаційні системи від різноманітних загроз. Давайте разом розберемося, чому це так важливо!"

3. Основні поняття в області безпеки інформаційних технологій (15 хв)

Пояснення термінів:

Інформаційна безпека – захист інформації від несанкціонованого доступу, втрати, модифікації або спотворення.

Конфіденційність – забезпечення того, щоб інформація була доступна лише тим, хто має право на доступ.

Цілісність – гарантування, що інформація не буде змінена або пошкоджена без дозволу.

Доступність – забезпечення постійного доступу до інформації та систем для авторизованих користувачів.

Ліс Гард додає: "Всі ці аспекти є важливими для захисту наших цифрових активів, будь то особисті дані, фінансові операції або корпоративна інформація."

Обговорення практичних прикладів:

1. Що може статися, якщо хтось отримає доступ до наших особистих даних?

2. Приклад: випадок з крадіжкою ідентичності через несанкціонований доступ до акаунтів.

4. Основні причини загострення проблеми забезпечення безпеки інформаційних технологій (15 хв)

Ліс Гард пояснює: "У світі інформаційних технологій існує кілька основних причин, чому проблеми з безпекою стають все більш актуальними."

Причини загострення проблеми:

1. Швидкий розвиток технологій та постійно зростаюча кількість нових технологій створює нові вразливості.

2. Хакери та кіберзлочинці постійно шукають способи проникнення в інформаційні системи.

3. Багато користувачів не знають, як правильно захищати свої особисті дані та облікові записи.

4. Безпечні мережі та протоколи для зберігання та передачі даних не завжди забезпечують належний рівень захисту.

Ліс Гард запитує учнів: "Які, на вашу думку, ще є причини, чому безпека інформаційних технологій стає проблемою? Давайте обговоримо!"

5. Групова робота: Обговорення та виявлення причин загострення проблеми безпеки (15 хв)

Розділити клас на кілька груп і дати кожній групі картки з питаннями для обговорення:

1. Які ви знаєте приклади кіберзлочинності?

2. Як на вашу думку можна покращити безпеку в Інтернеті?

3. Чи можна повністю захистити інформаційні технології?

Після обговорення групи представляють свої відповіді класу. Ліс Гард коментує їх, додаючи важливі акценти та практичні поради.

6. Підсумки уроку та рефлексія (10 хв)

Підсумок матеріалу, акцент на основних поняттях і причинах загострення проблеми.

Ліс Гард: "Пам’ятайте, що безпека інформаційних технологій – це не тільки технічні засоби, але й ваша обізнаність. Завжди будьте уважні до своїх даних!"

Завершення уроку за допомогою короткої вікторини через платформу **Kahoot!**, де учні можуть перевірити свої знання.

Домашнє завдання:

1. Напишіть коротке есе (до 300 слів) на тему "Чому важливо захищати свої дані в Інтернеті?".
2. Підготувати короткий список порад з кібербезпеки для молодших школярів.

ДОДАТОК Б

Урок на тему: «Криптографічні методи захисту інформації»

Мета уроку:

1. Ознайомити учнів із криптографічними методами захисту інформації, їх застосуванням у повсякденному житті.
2. Розвивати навички логічного мислення, аналізу й узагальнення інформації.
3. Виховувати відповідальне ставлення до захисту інформації та даних у цифровому середовищі.

Обладнання

- Комп’ютери або планшети з доступом до Інтернету.
- Інтерактивна дошка або проектор.
- Робочі аркуші із завданнями.
- Фігурка або зображення персонажа **Ліс Гард.**

Структура уроку

1. Організаційний момент (3 хв)

Привітання учнів.

Ознайомлення з темою уроку та персонажем **Ліс Гард**.

Учитель: "Сьогодні у нас незвичайний урок! Ми вирушимо в подорож разом із лісовим стражником цифрової безпеки – Лісом Гардом. Він проведе нас через захопливий світ криптографії та покаже, як можна захистити свої дані."

2. Актуалізація опорних знань (5 хв)

Запитання до учнів:

- Що таке інформація?
- Чому її потрібно захищати?
- Які методи захисту інформації ви знаєте?

Ліс Гард (від імені вчителя):

"Як ви думаєте, що роблять у старовинних казках, щоб захистити секрети? Так само і в цифровому світі є свої таємні коди. Сьогодні ми їх розгадаємо!"

3. Пояснення нового матеріалу (15 хв)

Криптографія – це наука про шифрування інформації.

- **Симетричне шифрування:** один ключ для шифрування та розшифрування.
- **Асиметричне шифрування:** два ключі – публічний і приватний.
- **Приклади криптографії:** шифри Цезаря, шифрування в месенджерах, банківські системи.

Візуалізація: Слайди з прикладами шифрування.

Ліс Гард: "Зараз я покажу вам старовинний шифр Цезаря. Він замінює кожну букву на іншу, зміщену на кілька позицій в алфавіті. Давайте спробуємо разом!"

Практика: Використання шифру Цезаря для шифрування фрази.

4. Інерактивна частина – проходження веб-квесту з теми

5. Узагальнення і рефлексія (7 хв)

1. **Обговорення:**

Як криптографія використовується в повсякденному житті?

2. **Питання для рефлексії:**

– Що вам найбільше сподобалося на уроці?

– Як можна застосувати отримані знання?

Ліс Гард: "Я бачу, ви чудово справилися із завданням! Тепер ви знаєте, як захищати свої секрети в цифровому світі!"

6. Домашнє завдання

1. Розробити власний простий шифр і написати повідомлення для однокласників.

2. Дослідити, як працює асиметричне шифрування в месенджерах (наприклад, у WhatsApp).

Завершення уроку

Учитель: "Дякую вам за активну участь! Сьогодні разом із Лісом Гардом ми відкрили світ криптографії та дізналися, як захистити свої дані. До нових зустрічей!"

Додатково: Фігурка Ліса Гарда може бути використана як нагорода для найактивнішого учня.

ДОДАТОК В

Урок на тему: "Керування механізмами захисту та виявлення атак у комп'ютерних мережах"

Мета уроку

1. Ознайомити учнів із основними принципами захисту комп'ютерних мереж, методами виявлення атак та захисту периметра.
2. Розвинути навички критичного мислення, співпраці та вирішення задач.
3. Використати елементи гейміфікації для закріплення теоретичного матеріалу.

План уроку (45 хвилин)

1. Організаційний момент (2 хвилини)

- Привітання учнів.
- Налаштування на активну роботу, оголошення теми уроку.

2. Мотивація (5 хвилин)

– Запитання для класу:

1. Як ви уявляєте захист комп'ютерної мережі?
2. Що можуть зробити хакери, якщо захисту немає?

– Показ відеофрагменту або ілюстрації, що демонструє наслідки кібератак (наприклад, втрату даних).

– Оголошення мети уроку: навчитися виявляти загрози та будувати захист мережі.

3. Теоретична частина (15 хвилин)

Механізми захисту

- Антивірусне програмне забезпечення.
- Фаєрволи.
- VPN.
- Системи резервного копіювання.
- Оновлення програмного забезпечення.

Методи виявлення атак

- IDS/IPS (системи виявлення та запобігання).
- Журнали реєстрації активності.
- Моніторинг трафіку.

Захист периметра

- Шифрування даних.
- Закриття невикористовуваних портів.
- Обмеження доступу до мережі.

Учням пропонуються приклади з реального життя для кожного методу.

4. Практична частина: мозковий штурм "Захист фортеці" (20 хвилин) на інтерактивній дошці Miro

5. Рефлексія та підбиття підсумків (3 хвилини)

– Обговорення результатів гри:

1. Що вдалося захистити?
2. Які методи були найефективнішими?

– Запитання для учнів:

1. Що нового ви дізналися про захист комп’ютерних мереж?
2. Як ви будете застосовувати ці знання?

Додатково: Нагородження команди-переможця символічним "сертифікатом захисника мережі".

Необхідні ресурси:

- **Інтерактивна дошка** або **проектор** для демонстрації карти фортеці.
- Роздаткові матеріали: картки із завданнями, ресурси (стікери/жетони).
- Доступ до мережі для показу відео чи інтерактивних інструментів (якщо онлайн-формат).

ДОДАТОК Г

Урок на тему: «Політика безпеки при доступі до мережі загального користування. Системи аналізу вмісту поштового і веб-трафіку. Віртуальні приватні мережі (VPN)»

Мета уроку:

1. Ознайомити учнів з основами політики безпеки при використанні мережі; пояснити принципи роботи систем аналізу трафіку (поштового та веб); розкрити призначення та принцип роботи VPN.
2. Розвивати критичне мислення, вміння аналізувати ризики в Інтернеті та приймати рішення щодо безпечного користування мережею.
3. Виховувати культуру відповідального користування Інтернетом.

Обладнання та ресурси:

- Мультимедійний проектор або інтерактивна дошка.
- Комп’ютери або ноутбуки з доступом до Інтернету.
- Презентація з ключовими поняттями.
- Відео/анімація про роботу VPN.

Хід уроку

1. Організаційний момент (3 хв)

- Привітання учнів.
- Перевірка готовності до уроку.

2. Актуалізація знань (7 хв)

Бесіда:

- Що таке мережа загального користування?
- Які небезпеки можуть виникати при використанні Інтернету?
- Чи стикались ви з фішингом, вірусами або спамом? Як діяли в цих ситуаціях?

3. Мотивація (3 хв)

Ситуаційна задача: "Уявіть, що ви підключилися до відкритої мережі Wi-Fi у кафе. Після цього ваш акаунт в соціальних мережах почали використовувати для розсилки спаму. Як це могло статися, і як уникнути подібних ситуацій?"

4. Вивчення нового матеріалу (20 хв)

4.1. Політика безпеки в мережах загального користування

- Використання антивірусного ПЗ.
- Налаштування брандмауера.
- Уникнення підключення до незахищених мереж.

4.2. Системи аналізу поштового та веб-трафіку

- Що таке спам-фільтри та як вони працюють.
- Захист від фішингу та інших кіберзагроз.
- Моніторинг трафіку через системи захисту, наприклад, DLP (Data Loss Prevention).

4.3. Віртуальні приватні мережі (VPN)

- Що таке VPN та його призначення.
- Як VPN захищає дані в мережі.
- Приклади безкоштовних та платних VPN-сервісів.

(Під час пояснення використовувати презентацію та демонстрацію роботи VPN.)

5. Практична частина (15 хв)

Проходження гри з теми у Blooket

6. Закріплення матеріалу (5 хв)

Запитання для рефлексії:

- Які переваги використання VPN?
- Чому важливо захищати свій поштовий трафік?
- Як можна виявити фішинговий лист?

7. Підсумок уроку та домашнє завдання (2 хв)

Домашнє завдання:

1. Підготувати приклади реальних випадків кіберзагроз і їх наслідків.
2. Дослідити додаткові функції обраного VPN-клієнта та створити короткий звіт (до 1 сторінки).

Підсумок:

Учитель разом з учнями підсумовує значення безпеки в Інтернеті та роль сучасних технологій у її забезпеченні.

ДОДАТОК Д

Розробка тестових завдань

Вихідний тест

1. **Що таке Інтернет?**

a) Комп’ютер

b) Всесвітня мережа, що з’єднує комп’ютери

c) Місце для зберігання даних

d) Програма для перегляду сайтів

(Правильна відповідь: b)

2. **Що є прикладом апаратного забезпечення для підключення до мережі?**

a) Монітор

b) Маршрутизатор (роутер)

c) Програма для відеозв'язку

d) Миша

(Правильна відповідь: b)

3. **Яка основна функція протоколу IP?**

a) Передача електронної пошти

b) Адресація пристроїв у мережі

c) Відтворення мультимедіа

d) Захист даних

(Правильна відповідь: b)

4. **Що таке локальна мережа (LAN)?**

a) Мережа для мобільних пристроїв

b) Мережа в межах одного приміщення або будівлі

c) Мережа, що охоплює весь світ

d) Мережа супутникового зв'язку

(Правильна відповідь: b)

5. **Що таке URL?**

a) Адреса веб-сторінки

b) Програма для завантаження файлів

c) Код для шифрування інформації

d) Тип файлу

(Правильна відповідь: a)

6. **Що таке браузер?**

a) Програма для перегляду веб-сторінок

b) Пристрій для підключення до мережі

c) Електронна пошта

d) Операційна система

(Правильна відповідь: a)

7. **Яка служба Інтернету використовується для обміну електронними листами?**

a) FTP

b) HTTP

c) E-mail

d) DNS

(Правильна відповідь: c)

8. **Що таке хмарне сховище?**

a) Фізичний сервер у будинку

b) Програма для завантаження музики

c) Сервіс для зберігання даних у мережі Інтернет

d) Комп’ютерна гра

(Правильна відповідь: c)

9. **Що таке блог?**

a) Приватний електронний лист

b) Онлайн-щоденник або вебсайт із записами автора

c) Інструмент для програмування

d) Розважальний відеосервіс

(Правильна відповідь: b)

10. **Яка служба використовується для відеозв’язку?**

a) Google Drive

b) Zoom

c) Facebook

d) DNS

(Правильна відповідь: b)

11. **Що таке пароль?**

a) Код доступу до облікового запису

b) Назва комп’ютерної гри

c) Програма для збереження інформації

d) Текстове повідомлення

(Правильна відповідь: a)

12. **Яке правило допоможе створити надійний пароль?**

a) Використовувати просте слово, наприклад, "1234"

b) Використовувати комбінацію великих і малих літер, цифр і символів

c) Пароль має бути коротким і простим

d) Повторювати один і той самий пароль для всіх облікових записів

(Правильна відповідь: b)

13. **Що таке вірус у контексті інформаційної безпеки?**

a) Захищена програма для комп'ютера

b) Програма, яка шкодить комп'ютеру або даним

c) Частина операційної системи

d) Файл для оновлення програми

(Правильна відповідь: b)

14. **Який із цих способів допомагає уникнути вірусів?**

a) Використовувати антивірусну програму

b) Відкривати всі невідомі файли

c) Користуватися тільки старими версіями програм

d) Ніколи не оновлювати систему

(Правильна відповідь: a)

15. **Що таке фішинг?**

a) Метод захисту інформації

b) Шахрайство, спрямоване на отримання конфіденційної інформації

c) Вид комп’ютерної гри

d) Процес оновлення операційної системи

(Правильна відповідь: b)

Додаток Е

Основні характеристики тестових завдань

Таблиця Е.1 – Основні характеристики тестових завдань

№	завдання 1	завдання 2	завдання 3	завдання 4	завдання 5	завдання 6	завдання 7	завдання 8	завдання 9	завдання 10	завдання 11	завдання 12	завдання 13	завдання 14	завдання 15
1	1	1	1	0	1	1	0	0	1	1	1	0	0	0	0
2	0	0	0	0	1	1	1	0	0	0	0	1	0	0	0
3	1	1	1	0	1	1	0	0	0	0	0	1	0	0	1
4	1	1	1	0	0	1	0	0	1	0	0	1	0	0	1
5	1	1	1	1	0	1	0	0	0	1	1	1	0	0	1
6	1	1	1	0	1	1	0	0	0	0	1	1	0	1	1
7	1	1	1	0	0	1	0	0	0	1	1	1	0	1	1
8	1	1	1	0	1	1	0	0	0	1	0	1	0	1	0
9	0	1	1	0	0	1	0	0	1	1	0	1	0	0	1
10	1	1	1	0	0	1	1	1	0	1	0	1	0	1	0
11	1	0	0	0	0	1	1	0	0	0	0	1	0	0	1
12	1	1	1	1	0	1	1	0	1	1	0	1	0	0	1
13	1	1	1	0	1	1	0	0	0	0	0	1	0	0	1
14	1	1	1	0	0	1	0	1	1	0	0	1	1	0	1
15	1	1	0	0	0	1	0	0	0	1	0	1	0	1	1
16	1	1	0	0	1	1	0	0	0	0	0	1	0	0	1
17	1	1	0	0	0	1	1	0	0	1	0	1	0	1	0
18	1	0	1	0	0	1	0	1	1	1	0	1	0	0	1
19	1	1	1	0	0	1	0	0	1	0	0	1	0	1	0
20	1	1	0	0	0	0	0	0	0	0	0	0	1	1	1
R_j	18	17	14	2	7	19	5	3	7	10	4	18	2	8	14
p_j	0,9	0,85	0,7	0,1	0,35	1	0,3	0,2	0,4	0,5	0,2	0,9	0,1	0,4	0,7
q_j	0,1	0,15	0,3	0,9	0,65	0,1	0,8	0,9	0,7	0,5	0,8	0,1	0,9	0,6	0,3
σ^2_j	0,09	0,13	0,21	0,09	0,23	0,05	0,19	0,13	0,23	0,25	0,16	0,09	0,09	0,24	0,21

ДОДАТОК Ж

Остаточний тест з модулю «Інформаційна безпека»

1. **Що є прикладом апаратного забезпечення для підключення до мережі?**
    a) Монітор
    b) Маршрутизатор (роутер)
    c) Програма для відеозв'язку
    d) Миша
    (Правильна відповідь: b)
2. **Яка служба Інтернету використовується для обміну електронними листами?**
    a) FTP
    b) HTTP
    c) E-mail
    d) DNS
    (Правильна відповідь: c)
3. **Яка основна функція протоколу IP?**
    a) Передача електронної пошти
    b) Адресація пристроїв у мережі
    c) Відтворення мультимедіа
    d) Захист даних
    (Правильна відповідь: b)
4. **Що таке URL?**
    a) Адреса веб-сторінки
    b) Програма для завантаження файлів
    c) Код для шифрування інформації
    d) Тип файлу

(Правильна відповідь: a)

5. **Що таке блог?**

a) Приватний електронний лист

b) Онлайн-щоденник або вебсайт із записами автора

c) Інструмент для програмування

d) Розважальний відеосервіс

(Правильна відповідь: b)

6. **Який із цих способів допомагає уникнути вірусів?**

a) Використовувати антивірусну програму

b) Відкривати всі невідомі файли

c) Користуватися тільки старими версіями програм

d) Ніколи не оновлювати систему

(Правильна відповідь: a)

7. **Який із цих способів допомагає уникнути вірусів?**

a) Використовувати антивірусну програму

b) Відкривати всі невідомі файли

c) Користуватися тільки старими версіями програм

d) Ніколи не оновлювати систему

(Правильна відповідь: a)

8. **Що таке фішинг?**

a) Метод захисту інформації

b) Шахрайство, спрямоване на отримання конфіденційної інформації

c) Вид комп’ютерної гри

d) Процес оновлення операційної системи

(Правильна відповідь: b)

9. **Що таке пароль?**

a) Код доступу до облікового запису

b) Назва комп’ютерної гри

c) Програма для збереження інформації

d) Текстове повідомлення

(Правильна відповідь: a)

10. **Що таке хмарне сховище?**

a) Фізичний сервер у будинку

b) Програма для завантаження музики

c) Сервіс для зберігання даних у мережі Інтернет

d) Комп’ютерна гра

(Правильна відповідь: c)

ДОДАТОК И

Перевірка ефективності викладання вибіркового модулю «Інформаційна безпека»

Таблиця И.1 – Оцінки учнів з тесту залишкових знань (констатувальний етап експерименту)

№	ЕГ	КГ
1	8	10
2	6	6
3	8	5
4	7	7
5	9	8
6	6	9
7	7	7
8	8	5
9	6	7
10	8	9
11	6	8
12	5	10
13	11	
14	6	
15	10	
Мінімальна оцінка	5	5
Максимальна оцінка	11	10
Середня оцінка	7,4	7,6
Дисперсія	2,83	2,99
Стандартне відхилення	1,68	1,73
Коефіцієнт варіації	22,7%	22,8%

Таблиця И.2 – Розрахунок емпіричного значення U-критерію Манна-Вітні (констатувальний етап)

№	ЕГ		КГ	
	значення	ранг	значення	ранг
1	8	10,5	10	3
2	6	21,5	6	21,5
3	8	10,5	5	26
4	7	16	7	16
5	9	6	8	10,5
6	6	21,5	9	6
7	7	16	7	16
8	8	10,5	5	26
9	6	21,5	7	16
10	8	10,5	9	6
11	6	21,5	8	10,5
12	5	26	10	3
13	11	1		
14	6	21,5		
15	10	3		
$\sum R_i$		217,5		160,5
T_x	217,5			
n_x	15			

Таблиця И.3 – Оцінки учнів з вибіркового модулю «Комп’ютерна безпека» (контрольний етап експерименту)

№	ЕГ	КГ
1	10	11
2	9	7
3	12	6
4	8	8
5	10	8
6	9	8
7	12	7
8	9	6
9	7	7
10	9	9
11	10	8
12	9	10
13	11	
14	8	
15	11	
Мінімальна оцінка	7	6
Максимальна оцінка	12	11
Середня оцінка	9,60	7,92
Дисперсія	2,11	2,27
Стандартне відхилення	1,45	1,51
Коефіцієнт варіації	15,1%	19,0%

Таблиця И.4 – Розрахунок емпіричного значення U-критерію Манна-Вітні (констатувальний етап)

№	ЕГ		КГ	
	значення	ранг	значення	ранг
1	10	7,5	11	4
2	9	12,5	7	23,5
3	12	1,5	6	26,5
4	8	18,5	8	18,5
5	10	7,5	8	18,5
6	9	12,5	8	18,5
7	12	1,5	7	23,5
8	9	12,5	6	26,5
9	7	23,5	7	23,5
10	9	12,5	9	12,5
11	10	7,5	8	18,5
12	9	12,5	10	7,5
13	11	4		
14	8	18,5		
15	11	4		
$\sum R_i$		156,5		221,5
T_x	221,5			
n_x	12			

Таблиця И.5 – Розрахунок емпіричного значення U-критерію Манна-Вітні для порівняння результатів двох груп на етапах експерименту

№	ЕГ		КГ	
	значення	ранг	значення	ранг
1	0	0	1	14
2	2	7,5	1	14
3	3	5,5	1	14
4	4	3	1	14
5	1	14	1	14
6	1	14	0	23
7	3	5,5	-1	27
8	5	1	0	23
9	1	14	1	14
10	1	14	0	23
11	1	14	0	23
12	4	3	0	23
13	4	3		
14	0	23		
15	2	7,5		
$\sum R_i$		129		226
T_x	226			
n_x	12			