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

«Допущено до захисту»
Завідувач кафедри
_____ Моісеєнко Н.В.
«____» _____ 2024 р.

Реєстраційний № _____
«____» _____ 2024 р.

# Факультатив з кібербезпеки для профільного навчання інформатики

Кваліфікаційна робота студента
групи Ім-23
ступінь вищої освіти «магістр»
спеціальності 014 Середня освіта (Інформатика)
**Кукси Владислава Владиславовича**

Керівник: доц., к. ф.-м.н.
Тарасова Олена Юріївна

Оцінка:
Національна шкала _____
Шкала ECTS __ Кількість балів ___

Голова ЕК _____ _____
Члени ЕК _____ _____
_____ _____
_____ _____

Кривий Ріг — 2024

## ЗАПЕВНЕННЯ

Я, Кукса Владислав Владиславович, розумію і підтримую політику Криворізького державного педагогічного університету з академічної доброчесності. Запевняю, що ця кваліфікаційна робота виконана самостійно, не містить академічного плагіату, фабрикації, фальсифікації. Я не надавав і не одержував недозволену допомогу під час підготовки цієї роботи. Використання ідей, результатів і текстів інших авторів мають покликання на відповідне джерело. Із чинним Положенням про запобігання та виявлення академічного плагіату в роботах здобувачів вищої освіти Криворізького державного педагогічного університету ознайомлений. Чітко усвідомлюю, що в разі виявлення у кваліфікаційній роботі порушення академічної доброчесності робота не допускається до захисту або оцінюється незадовільно.

# ЗМІСТ

# ВСТУП

**Актуальність дослідження.** Стрімке зростання кількості та складності кіберзагроз у сучасному цифровому просторі робить дослідження організації та проведення факультативу з кібербезпеки важливим. Кібератаки, які призводять до витоку конфіденційної інформації та значних фінансових втрат, останнім часом зросли. За даними міжнародних досліджень, у світі дефіцит фахівців з кібербезпеки перевищує 3,5 мільйона осіб, що вказує на гостру потребу в створенні освітніх програм у цій галузі. Аналіз наукової літератури та досвіду впровадження освітніх програм з кібербезпеки показує, що методичні підходи до факультативного навчання у вищих навчальних закладах недостатньо розроблені. Існуючі освітні програми часто не встигають за швидким розвитком технологій і появою нових типів загроз, що створює розрив між теоретичною підготовкою та практичними вимогами галузі. Проблема практичної підготовки майбутніх фахівців, здатних ефективно протидіяти сучасним кіберзагрозам, набуває особливої гостроти. Стандартні методи навчання не дають учням необхідних навичок для роботи з сучасними технологіями захисту інформації та протидії кібератакам. Впровадження факультативних курсів за допомогою сучасних платформ і віртуальних середовищ навчання дозволяє учням ліцеїв отримати практичний досвід у безпечному освітньому середовищі. Зростання попиту на онлайн-освіту та розвиток дистанційних технологій навчання створюють додаткові виклики для організації високоякісної підготовки фахівців з кібербезпеки. Розробка нових методів і впровадження спеціалізованих освітніх платформ є необхідним для забезпечення інтерактивності навчального процесу, контролю якості засвоєння матеріалу та розвитку практичних навичок під час віддаленого навчання.

**Об'єкт дослідження** – формування знань, умінь та навичок з основ кібербезпеки у рамках профільного навчання інформатики учнів ліцеїв.

**Предмет дослідження** – розробка та впровадження факультативу з кібербезпеки для учнів ліцеїв.

**Мета дослідження** – розробити та експериментально перевірити ефективність методики організації факультативного курсу з кібербезпеки на основі сучасних освітніх технологій та практико-орієнтованого підходу.

Відповідно до мети дослідження сформульовано наступні **завдання:**

- Проаналізувати теоретичні засади організації факультативного курсу з кібербезпеки.
- Розробити структуру та змістове наповнення факультативного курсу з кібербезпеки.
- Створити методичне забезпечення для проведення факультативних занять.
- Експериментально перевірити ефективність розробленої методики.

Для досягнення поставленої мети та розв'язання визначених завдань використано наступні **методи дослідження:**

–теоретичні – аналіз наукової літератури з проблем кібербезпеки та методики викладання інформатики; систематизація та узагальнення передового педагогічного досвіду; моделювання навчального процесу; проєктування змісту факультативного курсу;

–емпіричні – педагогічне спостереження за навчальним процесом; анкетування учнів та вчителів; тестування рівня знань та навичок;

–статистичні – методи математичної обробки експериментальних даних для оцінки достовірності отриманих результатів.

**Наукова новизна** отриманих результатів полягає в тому, що:

• вперше розроблено комплексну методику організації факультативного курсу з кібербезпеки на базі платформи Nearpod;

• удосконалено підходи до практичної підготовки учнів з кібербезпеки;

• отримало подальший розвиток застосування інтерактивних методів у навчанні учнів інформаційній безпеці.

**Практичне значення о**триманих результатів визначається:

1. створенням навчально-методичного комплексу для проведення факультативного курсу з кібербезпеки;

2. розробкою системи практичних завдань;

3. впровадженням методичних рекомендацій щодо організації самостійної роботи учнів.

**Структура та обсяг роботи.**

Текст роботи складається зі вступу, двох розділів, висновків, додатків, списку з 23 джерел.

# Розділ 1. Теоретичні основи щодо впровадження факультативу з кібербезпеки

## 1.1. Основи кібербезпеки

Дуже швидкий розвиток цифрових технологій і широка інформатизація соціально-економічних процесів значно змінили те, як функціонує сучасне суспільство. Інформаційно-комунікаційні системи проникли в кожну сферу людської діяльності, створивши кіберпростір, який є життєво важливим компонентом цивілізації. Масштабна діджиталізація, впровадження хмарних технологій, інтернету речей і штучного інтелекту створили принципово нові виклики у сфері інформаційної безпеки, але також відкрили нові можливості.

Сучасний кіберпростір характеризується надзвичайно високою швидкістю змін і постійною появою інноваційних технологічних рішень. Нові види кіберзагроз з'являються завдяки швидкому розвитку технологій, який перевершує створення систем захисту. Зловмисники активно використовують нові технології, щоб створити більш складні методи атак, які можуть перешкоджати традиційним системам захисту. Машинне навчання та штучний інтелект використовуються як для проведення масштабних кібератак, так і для створення надскладних шкідливих програм [1].

Однією з найбільших загроз у сучасному кіберпросторі стали атаки програм-вимагачів, атаки блокують доступ до важливих даних чи систем, вимагаючи викуп за їх відновлення. Відомі випадки, коли такі атаки паралізували діяльність великих корпорацій, державних установ і навіть цілих секторів економіки. Наприклад, атака на компанію Colonial Pipeline у 2021 році спричинила значні перебої в постачанні палива у США, що призвело до багатомільйонних збитків. Такі інциденти вказують на необхідність вдосконалення систем виявлення та реагування на подібні загрози [2].

Фішингові кампанії залишаються основним методом компрометації систем, орієнтуючись на людський фактор як найслабшу ланку в ланцюгу захисту. Зловмисники використовують техніки соціальної інженерії для отримання

доступу до конфіденційних даних, таких як паролі, фінансова інформація або дані доступу до корпоративних систем. Ефективність таких атак зростає завдяки використанню персоналізованих повідомлень, які здаються легітимними для кінцевого користувача.

Загрози кібербезпеки не обмежуються лише фінансовими втратами компаній. Вони також можуть спричинити серйозні наслідки для національної безпеки, особливо у випадках атак на критичну інфраструктуру, таку як енергетичні системи, транспорт або водопостачання. Наприклад, атака на українську енергосистему у 2015 році показала, наскільки вразливою може бути інфраструктура навіть у розвинених країнах, випадок підкреслює необхідність тісної співпраці державних органів і приватного сектора у розробці комплексних стратегій кіберзахисту.

Хмарні технології змінили кібербезпеку, створивши нові моделі небезпек і захисту. Передача даних і обчислювальних процесів у хмару вимагає перегляду традиційних методів захисту інформації. У зв'язку з розподіленою природою хмарних сервісів виникають додаткові труднощі щодо контролю доступу та захисту даних, коли вони передаються між різними частинами інфраструктури. Комплексні рішення, які забезпечують наскрізний захист даних незалежно від їх розташування, необхідні в гібридних хмарних середовищах.

Генеративні моделі дозволяють створювати переконливі фішингові повідомлення, які важко відрізнити від легітимних. Підроблені відео- та аудіоматеріали створюються за допомогою синтетичних медіа та технологій deepfake. Підвищення цифрової грамотності користувачів і розробка технологій виявлення синтетичного контенту необхідні для боротьби з такими загрозами [3].

Сучасна кібербезпека ґрунтується на моделі нульової довіри, багаторівневому захисті та проактивному виявленні загроз. Автоматизація процесів безпеки, використання штучного інтелекту та розробка предиктивної аналітики дозволяють створювати адаптивні системи захисту, здатні

протистояти сучасним кіберзагрозам. Зважаючи на глобальний характер кіберпростору, необхідно працювати разом на міжнародному рівні, щоб протидіяти кіберзлочинності. Стратегічні цілі національної безпеки держав включають захист важливих інфраструктур, гарантування приватності даних і створення цифрової стійкості суспільства [4]. Розвиток квантових обчислень, технологій штучного інтелекту та блокчейну безпосередньо пов'язаний з майбутнім кібербезпекою.

Фундаментальні принципи кібербезпеки базуються на тріаді CIA (Confidentiality, Integrity, Availability), яка визначає основні властивості захищених систем [5]. Конфіденційність передбачає забезпечення доступу до інформації лише авторизованим користувачам, цілісність гарантує незмінність даних при їх передачі та зберіганні, а доступність забезпечує можливість використання інформації, коли виникає така потреба [21].

Методологія забезпечення кібербезпеки включає системний підхід до ідентифікації та оцінки ризиків, розробки та впровадження захисних механізмів, моніторингу безпеки та реагування на інциденти [7]. Сучасні стандарти інформаційної безпеки, такі як ISO 27001, NIST Cybersecurity Framework, визначають структуровані підходи до організації процесів захисту інформації на всіх рівнях організації [8].

Еволюція кіберзагроз демонструє тенденцію до зростання складності атак та використання комбінованих методів проникнення в системи [9]. Застосування методів соціальної інженерії у поєднанні з технічними засобами злому створює особливо небезпечні сценарії атак, що вимагають комплексного підходу до забезпечення безпеки [10]. Розуміння психології зловмисників та механізмів проведення атак становить важливу складову підготовки фахівців з кібербезпеки [11].

Аналіз тенденцій кібербезпеки демонструє зростання масштабу та складності атак на інформаційні системи, що відображено в статистичних даних

міжнародних організацій з безпеки [12]. Систематизація основних типів кіберзагроз представлена в таблиці 1.1.

Таблиця 1.1. Класифікація сучасних кіберзагроз

| **Тип загрози** | **Характеристика** | **Рівень критичності** | **Тенденція зростання** |
|---|---|---|---|
| Ransomware | Шифрування даних з вимогою викупу | Високий | +156% |
| APT-атаки | Цільові довготривалі атаки | Критичний | +89% |
| DDoS | Відмова в обслуговуванні | Середній | +234% |
| Фішинг | Соціальна інженерія | Високий | +178% |

Архітектурні рішення у сфері кібербезпеки еволюціонують відповідно до змін у ландшафті загроз. Впровадження хмарних технологій та парадигми граничних обчислень створює нові вектори атак, що вимагає адаптації традиційних механізмів захисту. Модернізація підходів до безпеки відображається у концепції Security by Design, яка передбачає врахування аспектів безпеки на всіх етапах життєвого циклу інформаційних систем [13].

Методологія оцінки ризиків інформаційної безпеки базується на систематичному аналізі вразливостей та потенційних загроз. Кількісна оцінка ризиків дозволяє оптимізувати розподіл ресурсів на забезпечення захисту відповідно до критичності активів, що відображено в таблиці 1.2.

Таблиця 1.2. Матриця оцінки інформаційних ризиків

| **Ймовірність** | **Низький вплив** | **Середній вплив** | **Високий вплив** |
|---|---|---|---|
| Висока | Середній ризик | Високий ризик | Критичний ризик |
| Середня | Низький ризик | Середній ризик | Високий ризик |
| Низька | Мінімальний ризик | Низький ризик | Середній ризик |

Аналіз методів соціальної інженерії показує зростання складності та витонченості атак, спрямованих на маніпулювання користувачами [14]. Освітні програми з підвищення обізнаності у сфері кібербезпеки стають критично важливим компонентом загальної стратегії захисту. Формування культури кібербезпеки вимагає систематичного підходу до навчання учнів та регулярного оновлення знань відповідно до еволюції загроз.

Забезпечення безпеки веб-додатків становить окремий напрям кібербезпеки, що вимагає комплексного підходу до захисту від різноманітних типів атак. Методологія тестування безпеки веб-додатків OWASP Top 10 визначає найбільш критичні вразливості та методи їх усунення. Впровадження практик безпечної розробки (SecDevOps) дозволяє мінімізувати ризики появи вразливостей на етапі створення програмного забезпечення [15].

Сучасні тенденції у сфері автентифікації та управління доступом демонструють перехід до безпарольних технологій та багатофакторної автентифікації. Використання біометричних даних, апаратних ключів та поведінкової біометрії дозволяє підвищити надійність процесів ідентифікації користувачів. Концепція управління цифровими ідентичностями (Identity and Access Management, IAM) набуває особливого значення в умовах розподілених корпоративних середовищ.

Розвиток технологій Інтернету речей (IoT) створює нові виклики для забезпечення кібербезпеки, оскільки кількість підключених пристроїв стрімко зростає. Специфіка захисту IoT-екосистем вимагає врахування обмежених обчислювальних ресурсів пристроїв та особливостей протоколів взаємодії. Статистика вразливостей IoT-пристроїв демонструє критичну необхідність впровадження спеціалізованих механізмів захисту, що відображено в таблиці 1.3.

Таблиця 1.3. Аналіз вразливостей IoT-пристроїв

| **Категорія вразливості** | **Частота виявлення** | **Складність експлуатації** | **Потенційний вплив** |
|---|---|---|---|
| Слабка автентифікація | 78% | Низька | Критичний |
| Незахищені комунікації | 65% | Середня | Високий |
| Відсутність оновлень | 82% | Низька | Високий |
| Вразливості прошивки | 56% | Висока | Критичний |

Резервування та забезпечення відмовостійкості набувають критичного значення для безперервності технологічних процесів. Промислові системи управління проєктуються з урахуванням можливості швидкого відновлення після збоїв та кібератак. Регулярне резервне копіювання конфігурацій контролерів, наявність апаратних дублерів критичного обладнання, відпрацьовані процедури аварійного перемикання дозволяють мінімізувати час простою виробництва [16].

## 1.2. Роль і місце факультативу з кібербезпеки у навчальному процесі

Факультативний курс з кібербезпеки становить невід'ємну складову і може стати основою сучасної підготовки учнів у галузі інформаційних технологій [17]. Інтеграція поглибленого вивчення методів та засобів захисту інформації в навчальний процес відповідає актуальним тенденціям розвитку IT-індустрії та зростаючому попиту на спеціалістів з кібербезпеки на ринку праці. Систематизація освітніх компонентів факультативу представлена в таблиці 1.4.

Таблиця 1.4. Структура освітніх компонентів факультативу

| **Компонент** | **Обсяг годин** | **Форма контролю** | **Компетентності** |
|---|---|---|---|
| Теоретична підготовка | 45 | Тестування | Фундаментальні знання |
| Практичні заняття | 90 | Лабораторні роботи | Технічні навички |
| Проєктна робота | 45 | Захист проєкту | Аналітичні здібності |
| Самостійна робота | 60 | Портфоліо | Дослідницькі навички |

Методологічне значення факультативу полягає у формуванні системного підходу до розуміння проблем інформаційної безпеки та розвитку практичних навичок захисту інформаційних систем. Міждисциплінарний характер курсу забезпечує інтеграцію знань з різних галузей інформатики: криптографії, мережевих технологій, операційних систем, програмування [18]. Взаємозв'язок факультативу з іншими дисциплінами створює синергетичний ефект у підготовці майбутніх висококваліфікованих фахівців.

Організація навчального процесу в рамках факультативу базується на принципах проблемно-орієнтованого навчання та практичної спрямованості. Професійна спрямованість факультативного курсу реалізується через моделювання реальних ситуацій та використання актуальних інструментів захисту інформації. Поглиблене вивчення методів виявлення та протидії кіберзагрозам дозволяє учням отримати практичний досвід, необхідний для майбутньої професійної діяльності. Розвиток аналітичних здібностей та навичок критичного мислення становить фундаментальну мету факультативного курсу.

Методика викладання факультативу враховує різні стилі навчання та індивідуальні особливості учнів. Комбінування теоретичного матеріалу з практичними завданнями дозволяє забезпечити глибоке розуміння принципів

кібербезпеки та розвинути необхідні технічні навички. Інтерактивний характер занять стимулює активну участь учнів у навчальному процесі та сприяє формуванню професійних компетенцій.

Факультативні заняття, які традиційно доповнюють основну навчальну програму, набувають нового змісту завдяки впровадженню інноваційних освітніх платформ та інструментів дистанційного навчання. Гнучкість та адаптивність онлайн-середовища дозволяє враховувати індивідуальні особливості кожного учня, забезпечуючи персоналізований підхід до навчання. Віртуальні лабораторії стали потужним інструментом практичної підготовки учнів у рамках факультативних занять. Моделювання складних експериментів, проведення досліджень з використанням цифрових двійників реального обладнання, візуалізація абстрактних концепцій – можливості віртуальних лабораторій значно розширюють спектр практичних завдань для самостійного опрацювання.

Системи управління навчанням (LMS) забезпечують комплексну підтримку самостійної роботи учнів. Структурована подача матеріалу, інтерактивні елементи, засоби комунікації та контролю створюють єдиний освітній простір. Автоматизована перевірка завдань дозволяє учням миттєво отримувати зворотний зв'язок щодо результатів своєї роботи.

Соціальне навчання та колаборативні інструменти дозволяють організувати ефективну групову роботу учнів у віртуальному середовищі. Спільне розв'язання задач, обговорення проблем на форумах, взаємне оцінювання робіт розвивають навички командної роботи та критичного мислення. Інтеграція соціальних мереж в освітній процес створює неформальні канали обміну знаннями між учнями.

Мультимедійний контент нового покоління поєднує різні формати подачі інформації для максимально ефективного засвоєння матеріалу. Інтерактивні відеолекції з вбудованими тестами, анімовані презентації, інфографіка створюють багатовимірне навчальне середовище. Адаптивне стиснення

контенту забезпечує якісне відтворення навіть при обмеженій пропускній здатності мережі.

Аналітичні інструменти навчання надають вчителю детальну інформацію про активність учнів та ефективність освітнього процесу. Візуалізація даних про час виконання завдань, типові помилки, траєкторії навчання допомагає оптимізувати структуру курсу та методики викладання. Предикативна аналітика дозволяє виявляти учнів з ризиком академічної неуспішності та своєчасно надавати необхідну підтримку.

Персоналізоване навчальне середовище дозволяє учням самостійно формувати набір інструментів та ресурсів для навчання. Інтеграція різних освітніх платформ, сервісів зберігання документів, інструментів комунікації створює єдиний робочий простір.

Реалізація професійних стандартів кібербезпеки через факультативний курс дозволяє забезпечити відповідність підготовки майбутніх фахівців сучасним вимогам галузі. Програма курсу регулярно оновлюється відповідно до змін у технологіях та появи нових типів загроз.

Розвиток комунікативних навичок та вміння працювати в команді становить важливий аспект факультативного курсу. Групова робота над проєктами та спільне вирішення практичних завдань сприяють формуванню професійних зв'язків та обміну досвідом між старшокласниками. Навички документування результатів досліджень та презентації технічних рішень розвиваються через підготовку звітів та захист проєктів [19].

Поглиблене вивчення методів виявлення та протидії кіберзагрозам дозволяє учням отримати практичний досвід, необхідний для майбутньої професійної діяльності. Розвиток аналітичних здібностей та навичок критичного мислення становить фундаментальну мету факультативного курсу.

Методика викладання факультативу враховує різні стилі навчання та індивідуальні особливості учнів. Комбінування теоретичного матеріалу з

практичними завданнями дозволяє забезпечити глибоке розуміння принципів кібербезпеки та розвинути необхідні технічні навички.

Організація самостійної роботи учнів у рамках факультативу передбачає використання сучасних освітніх технологій та платформ дистанційного навчання. Система автоматизованої перевірки завдань та миттєвого зворотного зв'язку підвищує ефективність самостійного навчання [13].

Методологічна база факультативу з кібербезпеки ґрунтується на принципах адаптивного навчання, що дозволяє враховувати різний рівень початкової підготовки учнів [10]. Навчальні матеріали структуровані за рівнями складності, починаючи від базових концепцій інформаційної безпеки до поглибленого вивчення специфічних аспектів захисту інформації. Гнучкість програми дозволяє коригувати темп та глибину вивчення матеріалу відповідно до прогресу класу.

Практична складова факультативу реалізується через систему лабораторних робіт та проєктних завдань, що моделюють реальні сценарії порушення інформаційної безпеки. Учні отримують досвід роботи з професійними інструментами аналізу захищеності, вивчають методи виявлення вразливостей та техніки захисту від різних типів атак.

Факультативний курс з кібербезпеки виступає комплексним освітнім компонентом, що забезпечує формування практичних навичок у сфері захисту інформації. Інтеграція курсу в навчальний процес створює платформу для поглибленого вивчення актуальних технологій та методів забезпечення кібербезпеки.

## 1.3 Аналіз аналогічної навчальної програми факультативного курсу «Основи кібербезпеки»

Розглянемо програму факультативного курсу «Основи кібербезпеки», автори: Войцеховський М. О., Проценко Т.Г., Гапонюк Ю.М. [22].

Дана розробка є спеціалізованою програмою для учнів старших класів, спрямованою на формування базових знань і практичних навичок у сфері

захисту інформації та мережевої безпеки. Він базується на програмі Cisco «Cybersecurity Essentials». Метою курсу є підготовка учнів до свідомого, безпечного і відповідального використання інформаційних технологій у повсякденному житті та професійній діяльності.

**Вступна частина**

Навчальна програма розпочинається з ознайомлення з основними поняттями кібербезпеки. Згідно опису учні згідно програми дізнаються про ключові ризики сучасного кіберпростору, включаючи випадки порушення конфіденційності, крадіжки персональних даних, атаки на мережі та шкідливе програмне забезпечення. У вступному розділі підкреслюється важливість кібербезпеки для сучасного суспільства та значення цієї сфери для професійного розвитку. Навчаючись за даною програмою учні ознайомляться з перспективами професійного зростання у цій галузі, а також із концепціями національної кібербезпеки.

**Особливості курсу**

Програма орієнтована на формування ключових компетентностей, таких як інформаційно-цифрова, критичне мислення, ініціативність, уміння працювати в команді. Значна увага приділяється виконанню лабораторних робіт, які включають моделювання мережевих загроз, налаштування VPN і брандмауерів, аналізу ризиків. Використовуються професійні інструменти, такі як Cisco Packet Tracer, Wireshark, криптографічні програми TrueCrypt і VeraCrypt. Після завершення курсу учні можуть скласти фінальний тест і отримати сертифікат, що підтверджує їхню компетентність у галузі кібербезпеки.

**Структура навчальної програми**

Курс складається з 35 годин, поділених на 8 розділів:

1. **Вступ (1 година):** Ознайомлення з кіберпростором, його загрозами, викликами та професійними перспективами у сфері кібербезпеки.

2. **Кібербезпека: світ експертів і злочинців (4 години):** Аналіз видів загроз, діяльності кіберзлочинців та методів їхньої протидії. Практичне завдання: пошук роботи у сфері кібербезпеки.
3. **Куб кібербезпеки (4 години):** Принципи конфіденційності, цілісності, доступності даних. Практична робота: шифрування файлів і перевірка цілісності даних.
4. **Кібербезпека: загрози, вразливості та атаки (4 години):** Вивчення видів атак, шкідливого програмного забезпечення, методів соціальної інженерії. Практика з використанням Wireshark для аналізу загроз.
5. **Мистецтво захисту таємниць (4 години):** Основи криптографії, шифрування, стеганографії. Практична робота: налаштування VPN у транспортному й тунельному режимах.
6. **Мистецтво забезпечення цілісності даних (4 години):** Хешування, цифрові підписи, сертифікація. Практична робота: налаштування HMAC та використання цифрових сертифікатів.
7. **Концепція п'яти дев'яток (4 години):** Забезпечення високої доступності даних, резервування систем, управління ризиками. Практика: аналіз конфігурацій мереж із використанням Packet Tracer.
8. **Узагальнення та підсумки (2 години):** Фінальне тестування, захист індивідуальних проєктів, отримання сертифікатів.

**Практична частина**

Практичні заняття складають значну частину курсу і проводяться з використанням сучасних інструментів, таких як симулятор Cisco Packet Tracer. Завдяки йому учні отримують можливість налаштовувати безпечні мережеві з'єднання, включаючи VPN та брандмауери, виявляти та усувати мережеві вразливості, виконувати аналіз ризиків та розробляти заходи для їхнього зменшення. Працювати з криптографічними інструментами, такими як цифрові підписи та сертифікати. Практичні роботи спрямовані на формування навичок

аналізу загроз, налаштування захисту систем, тестування системної стійкості та відпрацювання алгоритмів реагування на інциденти.

**Компетентнісний потенціал курсу**

Компетентнісний потенціал курсу є однією з його ключових характеристик, яка відображає сучасні підходи до організації освітнього процесу. Навчальна програма спрямована на формування цілісної системи знань, умінь і навичок, що дозволяють учням ефективно діяти в умовах цифрового середовища. Зокрема, значна увага приділяється розвитку інформаційно-цифрової компетентності, яка включає вміння орієнтуватися у великому обсязі інформації, розпізнавати маніпулятивні техніки, критично оцінювати отримані дані, а також дотримуватися етичних норм у віртуальному просторі.

Курс сприяє розвитку уміння вчитися протягом життя, адже учні здобувають здатність самостійно планувати свою навчальну діяльність, шукати необхідні ресурси, аналізувати їх та інтегрувати у власну систему знань. Формування критичного мислення допомагає учням аналізувати реальні проблеми, пропонувати можливі рішення та оцінювати їх ефективність. Соціальна та громадянська компетентності формуються через усвідомлення важливості дотримання правових норм, етичної поведінки в Інтернеті та відповідальності за власні дії в цифровому середовищі. Крім того, учні опановують уміння працювати в команді, що є надзвичайно важливим для вирішення складних завдань у професійній сфері.

**Критерії оцінювання навчальних досягнень учнів**

Курс передбачає чітку систему оцінювання, яка включає тести, лабораторні роботи та підсумковий іспит. Фінальний онлайн-екзамен дає змогу отримати сертифікат, що підтверджує набуті знання та навички.

Кожному балу відповідає певний відсоток правильних відповідей учнів за результатами контрольних робіт. Для отримання сертифікату по закінченні

курсу учень має набрати під час тестування не менше 75% правильних відповідей, що відповідає достатньому рівню навчальних досягнень учнів. Також у курсі представлена наглядна таблиця рівнів навчальних досягнень та критеріїв досягнень учнів. В таблиці наведено 4 рівні навчальних досягнень (початковий, середній, достатній, високий). Для досягнення певного рівню учень повинен відповідати критеріям оцінювання. Наприклад для високого рівня навчального досягнення учень повинен продемонструвати знання, вміння і навички, які відповідають вимогам програми у повному обсязі.

Учень (учениця): володіє міцними знаннями, самостійно визначає проміжні етапи власної навчальної діяльності, аналізує нові факти та явища. Судження логічні і достатньо обґрунтовані. Учень має сформовані навички керування інформаційними системами.

**Навчально-методичне забезпечення**

1. **Cisco Packet Tracer:** Симулятор для моделювання мереж, аналізу ризиків, конфігурування мережевих пристроїв.
2. **Wireshark:** Інструмент для аналізу мережевого трафіку та виявлення атак.
3. **TrueCrypt і VeraCrypt:** Програми для демонстрації шифрування даних.
4. **NetAcad (Cisco Networking Academy):** Платформа для інтерактивного навчання, тестування та додаткових курсів.
5. **Посібник «Introduction to Cybersecurity» від Cisco:** Матеріал для поглибленого вивчення.
6. **OWASP (Open Web Application Security Project):** Ресурси для вивчення безпеки веб-додатків.
7. **Електронний словник термінів із кібербезпеки:** Інтерактивний довідник для вивчення термінології.

Таким чином можемо зробити висновок, що згідно опису програми факультативного курсу, курс «Основи кібербезпеки» є важливим і своєчасним інструментом для підготовки старшокласників до реалій цифрового суспільства. Він ефективно інтегрує теоретичні знання з практичними навичками,

забезпечуючи учнів необхідною базою для захисту інформації та пристроїв. Особливу цінність курсу становить його практична спрямованість, що дозволяє учням не лише засвоювати концепції кібербезпеки, але й застосовувати їх у реальних ситуаціях.

Програма також виконує соціальну функцію – вона не лише формує цифрову грамотність, але й навчає критично мислити, аналізувати загрози та діяти в умовах постійного оновлення технологій. Завдяки модульному підходу та інтеграції міжнародних стандартів курс створює платформу для подальшого професійного розвитку учнів у сфері ІТ. Таким чином, курс забезпечує не лише навчальну, але й стратегічну підготовку молодого покоління до цифрових викликів, формуючи компетентних користувачів і майбутніх фахівців у галузі кібербезпеки.

### 1.4 Визначення цілей та завдань факультативу з кібербезпеки

Формування системи цілей та завдань факультативного курсу з кібербезпеки базується на комплексному підході до підготовки учнів як майбутніх фахівців у сфері захисту інформації. Стратегічною метою факультативу повинно бути: розвиток професійних компетенцій, необхідних для ефективної протидії сучасним кіберзагрозам та забезпечення безпеки інформаційних систем.

Освітні цілі факультативного курсу мають охоплювати формування глибокого розуміння принципів систем захисту інформації, розвиток практичних навичок використання інструментів безпеки.

Розвиток аналітичних здібностей учнів під час роботи на факультативі реалізується через систему практичних завдань, спрямованих на формування навичок критичного мислення та системного аналізу проблем безпеки. Формування комунікативних компетенцій становить важливу складову цілей факультативного курсу. Крім того, важливі також: розвиток навичок командної

роботи, здатність ефективно презентувати технічні рішення та документувати результати досліджень.

Важливо врахувати і психологічні аспекти підготовки фахівців з кібербезпеки, які охоплюють розвиток стресостійкості, здатності працювати в умовах обмеженого часу та приймати зважені рішення.

Дослідницька складова завдань факультативу має бути спрямована на розвиток навичок самостійного вивчення нових технологій захисту інформації та аналізу emerging threats. Учні під час занять факультативу навчаються працювати з науковою літературою, вивчають методологію проведення досліджень у сфері кібербезпеки, опановують техніки документування та презентації результатів досліджень. Старшокласники також мають бути ознайомлені і з правовими аспектами забезпечення інформаційної безпеки, принципами захисту персональних даних та нормами професійної етики.

**Висновки до розділу 1**

У даному розділі описані фундаментальні принципи організації факультативного навчання у сфері кібербезпеки, що забезпечують ефективність формування професійних компетенцій. Обґрунтовано необхідність розробки комплексної системи підготовки учнів, яка інтегрує теоретичну базу з практичним досвідом роботи із сучасними інструментами захисту інформації. Визначено важливість оптимізації структури та змісту факультативного курсу для забезпечення поетапного формування ключових навичок у сфері кібербезпеки. Проаналізовано нормативно-правову базу та стандарти освіти в галузі інформаційної безпеки, що дозволило окреслити вимоги до рівня підготовки старшокласників і визначити пріоритети розвитку освітніх програм. Виявлено потребу у впровадженні інноваційних методичних стратегій, які поєднують теоретичний фундамент із практичною спрямованістю, акцентуючи увагу на формуванні професійних компетенцій.

Досліджено місце факультативного курсу з кібербезпеки у профільному навчанні інформатики. Встановлено, що його впровадження сприятиме

розширенню знань з інформаційної безпеки, розвитку критичного мислення, аналітичних здібностей та формуванню практичних навичок протидії загрозам. Сформульовано концептуальний фундамент для подальшої розробки змістового наповнення та методичного забезпечення факультативного курсу. Обґрунтовано доцільність комплексного підходу до організації факультативного навчання, який враховує міжнародний досвід, сучасні тенденції розвитку інформаційної безпеки та спрямований на формування ключових компетенцій учнів.

# Розділ 2. Розробка змісту та методичного забезпечення факультативу

## 2.1 Навчальна програма факультативного курсу «Основи кібербезпеки» для 10-11 класів

Програма факультативу “Кібербезпека для профільного навчання інформатики” розрахована на учнів 10-11 класів в обсязі 1 години на тиждень.

**Мета факультативу:** формування базових знань, практичних умінь і навичок у сфері кібербезпеки, що сприятиме безпечному використанню інформаційних технологій у повсякденному житті, розвитку критичного мислення для оцінки ризиків у цифровому середовищі та вихованню відповідального ставлення до захисту персональних даних.

**Завдання факультативу:**

- Ознайомити учнів із поняттям кібербезпеки, її ключовими принципами та актуальністю у сучасному світі.
- Навчити розпізнавати основні види кіберзагроз, аналізувати їх наслідки та розробляти базові стратегії захисту.
- Надати практичні навички роботи з інструментами кіберзахисту, включаючи шифрування даних, двофакторну автентифікацію, налаштування мережевої безпеки та базові методи виявлення загроз.
- Сформувати у ліцеїстів вміння реагувати на кіберінциденти, аналізувати їх причини та наслідки в контрольованому навчальному середовищі.
- Розвинути в учнів навички роботи у групах для виконання завдань, пов'язаних із розробкою стратегій безпеки та захистом інформації.
- Ознайомити учнів із сучасними технологіями, що використовуються у сфері кібербезпеки, такими як штучний інтелект, блокчейн і квантова криптографія.
- Підготувати ліцеїстів до викликів цифрового середовища, зокрема у контексті безпечного користування Інтернетом, соціальними мережами та персональними пристроями.

**Загальна характеристика програми:**

**Тривалість:** 1 семестр (16 занять);

**Періодичність:** 1 заняття на тиждень;

**Тривалість заняття:** 40-45 хвилин;

**Обладнання:** комп'ютери/ноутбуки/планшети, доступ до Інтернету, інтерактивна платформа Nearpod.

**Навчально-тематичний план факультативу**

| **МОДУЛЬ 1. ОСНОВИ КІБЕРБЕЗПЕКИ** | | | | |
|---|---|---|---|---|
| Тема заняття | Зміст заняття | Тип заняття | ПЗ | Години |
| 1. Вступ до кібербезпеки: ключові поняття, принципи та актуальність проблематики | Огляд основних понять кібербезпеки, важливість інформаційної безпеки в сучасному світі, приклади з життя | Лекція, Дискусія | PowerPoint, інтерактивна платформа Nearpod | 1 |
| 2. Загрози кібербезпеці: типологія, еволюція та вектори реалізації | Аналіз видів кіберзагроз (віруси, фішинг, атаки типу Man-in-the-Middle, DDoS), демонстрація прикладів загроз та їх наслідків | Лекція, Практика | Відеоматеріали, інтерактивні тести | 1 |
| 3. Правові та етичні аспекти кібербезпеки | Основи правових аспектів захисту даних, етичні принципи роботи | Лекція | Документи, відкриті джерела | 1 |

| | | | | |
|---|---|---|---|---|
| | в кіберпросторі, розгляд законодавства України у сфері кібербезпеки | | | |
| 4. Стратегії та методології забезпечення кібербезпеки | Розробка та реалізація стратегій забезпечення безпеки в мережі: створення паролів, автентифікація, багатофакторний захист | Лекція, Практика | Генератори паролів, Google Authenticator | 1 |
| **МОДУЛЬ 2. ПРАКТИКА ЗАХИСТУ ІНФОРМАЦІЇ** | | | | |
| Тема заняття | Зміст заняття | Тип заняття | ПЗ | Години |
| 1. Криптографічні методи захисту даних | Вивчення базових принципів шифрування, створення зашифрованих файлів | Практичне заняття | Інструменти шифрування (наприклад, VeraCrypt) | 1 |
| 2. Технології ідентифікації та автентифікації | Ознайомлення з методами автентифікації: логіни, паролі, біометричні дані | Лекція, Практика | Google Authenticator, Microsoft Authenticator | 1 |

| | | | | |
|---|---|---|---|---|
| 3. Мережева безпека: архітектура та протоколи | Основи налаштування мережевих з'єднань, протоколи HTTPS, VPN, безпека мереж Wi-Fi | Лекція, Практика | Інтерактивні симулятори, віртуальні машини | 1 |
| 4. Системи виявлення та запобігання вторгненням | Вивчення базових налаштувань IDS/IPS-систем, виявлення атак за допомогою програмного забезпечення | Практичне заняття | Wireshark, демонстраційні симулятори | 1 |
| 5. Тестування на проникнення: методологія та інструменти | Ознайомлення з методами пентестингу, основні інструменти (Nmap, Metasploit) | Практика | Nmap, Metasploit Framework | 1 |
| 6. Управління інцидентами інформаційної безпеки | Підготовка до реагування на кіберінциденти, інструктаж щодо їх документування | Практичне заняття | Шаблони звітів | 1 |

| | | | | |
|---|---|---|---|---|
| 7. Цифрова криміналістика та розслідування інцидентів | Аналіз кіберзагроз, робота з журналами подій, розслідування фішингових атак | Практичне заняття | Аналіз логів | 1 |
| **МОДУЛЬ 3. ПІДСУМКОВИЙ** | | | | |
| 1.Кейси з кібербезпеки: аналіз реальних інцидентів | Розбір реальних ситуацій з кібербезпеки, аналіз помилок і правильних рішень | Практика | Симуляції | 1 |
| 2.Розробка стратегії кібербезпеки для організації | Створення власного плану захисту для вигаданої організації, презентація результатів | Групова робота | Canva, Google Docs | 1 |
| 3. Перспективні напрями розвитку кібербезпеки | Ознайомлення з новітніми технологіями: штучний інтелект, блокчейн, квантова криптографія | Лекція | Презентації, відео | 1 |

| | | | | |
|---|---|---|---|---|
| 4. Підсумкове заняття: презентація та захист проєктів | Захист проєктів перед класом, оцінка роботи груп | Презентація | PowerPoint, Nearpod | 2 |

**Покликання на модулі на платформі Nearpod:**

Модуль 1

https://np1.nearpod.com/sharePresentation.php?code=38a3fa08ee3c94593798dcb33029f54e-1&oc=user-created&utm_source=link

Модуль 2

https://np1.nearpod.com/sharePresentation.php?code=776e04e9bd921be27933499f0c716766-1&oc=user-created&utm_source=link

Модуль 3

https://np1.nearpod.com/sharePresentation.php?code=5fe4903c637c381242a715c03237c3fb-1&oc=user-created&utm_source=link

**Критерії оцінювання**

| **Критерій** | Максимальний бал | Опис |
|---|---|---|
| **Знання теоретичного матеріалу** | 20 | Перевірка засвоєння основних понять, принципів та стратегій кібербезпеки через тести, опитування та теоретичні запитання. |
| **Практичні навички** | 30 | Уміння працювати з інструментами кіберзахисту (налаштування мережевої безпеки, створення паролів, використання програмного забезпечення). |

| | | |
|---|---|---|
| **Робота в групах** | 10 | Оцінювання ефективності роботи у команді під час виконання практичних завдань, таких як розробка стратегії захисту чи вирішення кейсів. |
| **Розробка та презентація проєкту** | 25 | Захист власного проєкту, що включає розробку стратегії захисту конфіденційної інформації, або аналіз кейсу, аргументованість і оформлення презентації. |
| **Активність на заняттях** | 10 | Участь у дискусіях, виконання інтерактивних вправ, внесення пропозицій під час обговорення завдань. |
| **Самостійні роботи** | 5 | Виконання додаткових завдань вдома, включаючи пошук інформації, заповнення шаблонів звітів та підготовку до практичних занять. |
| **Загальний бал** | 100 | Для успішного завершення курсу учень має набрати не менше 60 балів. |

Список використаної літератури, на основі якої створювалась навчальна програма факультативу [9], [23], [10].

## 2.2 Розробка та опис навчальних матеріалів курсу

Методичне забезпечення факультативного курсу з кібербезпеки для профільного навчання інформатики становить комплексну систему навчально-методичних матеріалів, спрямованих на формування у старшокласників компетентностей у сфері інформаційної безпеки. Структурування навчального матеріалу здійснюється за модульним принципом, що дозволяє забезпечити послідовне та системне засвоєння знань і практичних

навичок. Перший модуль факультативного курсу «Основи кібербезпеки» присвячений фундаментальним основам кібербезпеки та закладає теоретичне підґрунтя для подальшого навчання. Вступ до кібербезпеки включає розгляд основних понять і принципів, а також ролі і значення захисту даних у сучасному суспільстві. Основні складові кібербезпеки охоплюють конфіденційність, цілісність та доступність, а також аналізуються елементи, які не належать до основних складових кібербезпеки. У розділі, присвяченому загрозам кібербезпеці, вивчаються різноманітні ризики та потенційні загрози для комп'ютерних систем, мереж та даних, які виникають у результаті зловмисних дій, таких як кібератаки чи несанкціонований доступ. Далі розглядаються практичні аспекти захисту особистих даних, включаючи важливість використання двофакторної автентифікації, регулярне оновлення програмного забезпечення, створення унікальних паролів для кожного облікового запису та ігнорування підозрілих повідомлень. Окрему увагу приділяється аналізу слабких місць у діях користувачів чи систем, які дозволяють зловмисникам здійснювати атаки, а також можливим наслідкам, що можуть виникнути через розкриття конфіденційної інформації. Завершується розгляд запропонуванням заходів, спрямованих на попередження подібних ситуацій, включаючи технічні, організаційні та поведінкові рекомендації для користувачів і адміністраторів систем.

Матеріал починається з розгляду базових концепцій інформаційної безпеки, зокрема принципів конфіденційності, цілісності та доступності інформації. Навчальний контент містить мультимедійні презентації, інтерактивні схеми та відеоматеріали, які демонструють актуальні приклади порушення інформаційної безпеки та їхні наслідки. Практичні завдання модуля спрямовані на розвиток аналітичного мислення учнів та формування навичок оцінки потенційних загроз [21].

Другий модуль «Практика захисту інформації» розроблений з урахуванням практичних потреб учнів ліцею і має на меті формування базових навичок

безпечного користування інформаційними технологіями. У межах модуля учні поступово знайомляться з основами захисту інформації через виконання практичних завдань. Вивчення розпочинається із криптографічних методів, де учні дізнаються про шифрування даних і створення зашифрованих файлів. Наступний етап охоплює технології ідентифікації та автентифікації, включаючи прості інструменти для створення двофакторного захисту. Далі учні вивчають основи мережевої безпеки, зокрема налаштування Wi-Fi та базовий захист мереж. Особлива увага приділяється практикам виявлення загроз за допомогою доступних інструментів, наприклад, аналізу простих журналів подій та налаштування базових антивірусів. У процесі навчання ліцеїсти також знайомляться з основами тестування на проникнення, виконуючи завдання у симуляціях, що відповідають їхньому рівню підготовки. Завершальними заняттями модуля є ознайомлення з основами управління інцидентами інформаційної безпеки та розслідуванням базових кіберзагроз через прості симулятори реальних випадків. Усі завдання адаптовані до можливостей учнів і виконуються у контрольованому середовищі під керівництвом учителя. Перелік ресурсів, рекомендованих для проведення факультативу з кібербезпеки представлено в (Додаток Б)

Тематика охоплює ключові аспекти кібербезпеки та інформаційного захисту, починаючи зі вступу до понять фішингу як однієї з найпоширеніших кіберзагроз, аналізу основних ознак підозрілих електронних листів та дій користувачів у разі отримання підозрілих повідомлень. Розглядається також поняття інформаційної безпеки під час війни, психологічний портрет жертви кібератак та ефективність використання VPN у сучасному цифровому середовищі. Завершується курс підсумковими питаннями, які спонукають учнів розробити комплексну стратегію забезпечення інформаційної безпеки особистості із врахуванням технічних інструментів, правових механізмів та цифрової культури для протидії сучасним кіберзагрозам. У кожній темі акцентується увага на практичній орієнтації та логіці викладення матеріалу, що

забезпечує глибоке розуміння теоретичних аспектів і їх прикладне застосування.

Особливу роль відіграють завдання з розпізнавання методів соціальної інженерії, які реалізуються через рольові ігри та аналіз реальних випадків кібершахрайства [20].

Методичне забезпечення практичних занять реалізується через інтерактивну платформу Nearpod, де розміщені покрокові інструкції до виконання лабораторних робіт, відеодемонстрації налаштування захисних механізмів, тестові завдання для самоперевірки. Платформа дозволяє організувати синхронну роботу групи учнів, забезпечити моніторинг виконання завдань та надати оперативний зворотний зв'язок (рис. 2.1).

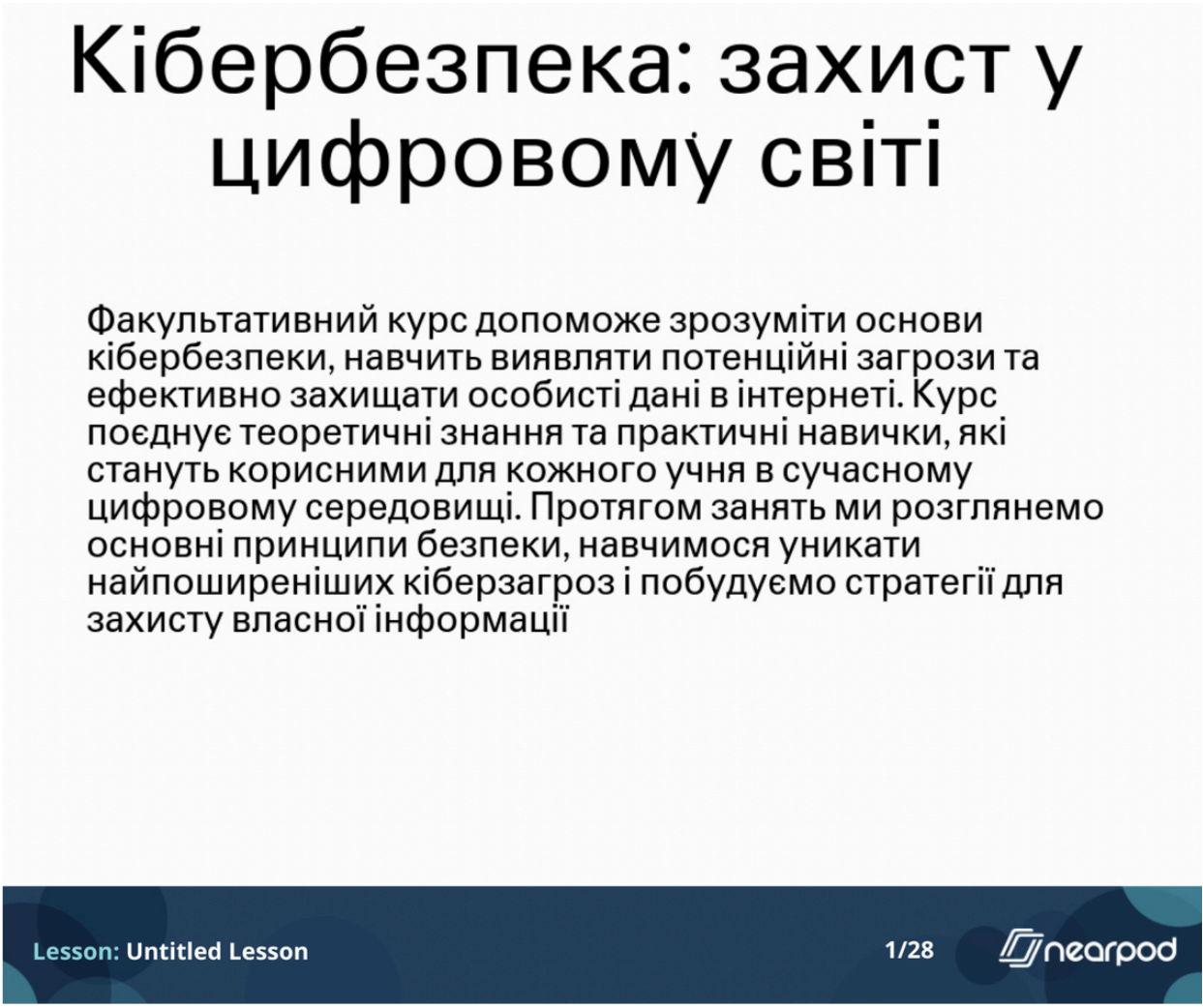


Рис. 2.1. Скріншот першої сторінки модулю на курсі в Nearpod

Третій модуль “Підсумковий” узагальнює набуті знання та навички через виконання комплексних проєктних завдань. Методичні матеріали містять шаблони проєктної документації, рекомендації щодо проведення аналізу захищеності інформаційних систем, критерії оцінювання результатів роботи. Навчально-методичний комплекс факультативу передбачає використання різноманітних форм організації навчальної діяльності: лекції-візуалізації з елементами дискусії, практичні заняття з виконанням індивідуальних та групових завдань, лабораторні роботи на реальному та віртуальному обладнанні, проєктна діяльність, ділові ігри. Матеріали структуровані за принципом наростання складності та забезпечують поступовий перехід від теоретичних знань до практичних навичок. Комплексна система діагностичних матеріалів становить фундаментальну основу методичного забезпечення навчального процесу в галузі захисту інформації. Багаторівнева структура оцінювання забезпечує послідовний моніторинг формування компетентностей учнів від початкового етапу навчання до завершального контролю. Вхідне діагностування дозволяє визначити базовий рівень підготовки кожного учня та сформувати індивідуальну траєкторію навчання.

Портфоліо навчальних досягнень формується протягом усього періоду навчання. Документування виконаних завдань, з кібербезпеки створюють комплексну картину професійного розвитку учня.

Критерії оцінювання теоретичної підготовки охоплюють розуміння фундаментальних концепцій інформаційної безпеки, знання сучасних технологій захисту, обізнаність щодо нормативно-правової бази. Рубрики оцінювання включають здатність аналізувати загрози, обґрунтовувати вибір засобів захисту, розробляти політики безпеки.

Розроблений комплекс навчально-методичних матеріалів враховує міждисциплінарні зв'язки інформатики з іншими предметами, зокрема математикою, фізикою, правознавством. Матеріали містять приклади застосування криптографічних методів захисту інформації, фізичних принципів

роботи апаратних засобів захисту, правових аспектів забезпечення інформаційної безпеки.

Методичне забезпечення факультативу постійно оновлюється з урахуванням появи нових видів кіберзагроз та методів захисту. Платформа Nearpod дозволяє оперативно додавати актуальні матеріали, модифікувати практичні завдання, адаптувати зміст відповідно до потреб конкретної групи учнів. Передбачено механізм збору зворотного зв'язку від учнів для вдосконалення навчальних матеріалів та методів викладання.

Факультативний курс завершується захистом індивідуальних проєктів, які демонструють здатність учнів застосовувати отримані знання та навички для вирішення практичних завдань з інформаційної безпеки. Методичні рекомендації щодо виконання підсумкових проєктів містять вимоги до структури та змісту роботи, приклади тем, критерії оцінювання, рекомендації щодо презентації результатів. Методичні розробки занять курсу (Додаток А).

## 2.3. Організація та проведення факультативу

На початку 2024-2025 навчального року факультативний курс з кібербезпеки було запропоновано до впровадження у навчальний процес Рацівського ліцею №1.

Для участі в опитуванні щодо зацікавленості у заняттях з факультативного курсу залучено учнів 10-11 класів. Метою опитування було визначити інтерес до теми кібербезпеки, дослідити наявний рівень знань та виявити зацікавленість у впровадженні факультативу. Для організації опитування було застосовано анонімний опитувальник учнів на платформі Google Forms (Додаток В). Покликання на опитувальник https://forms.gle/ziYwDEjPzXeq37QF7

Також було проведено опитування серед вчителів ліцею. Головною метою опитування є вивчення ставлення вчителів до ідеї впровадження факультативу з кібербезпеки, оцінка рівня їхньої обізнаності у цій сфері, якості програми та

зручності викладення інформації та визначення потреб у методичних матеріалах. Проведення опитування серед учителів є важливим етапом у процесі впровадження факультативу з кібербезпеки. Залучення педагогів до формування курсу не лише підвищить їхню зацікавленість тематикою, але й сприятиме створенню якісного та актуального навчального матеріалу для учнів. Ознайомлення вчителів з курсом дозволило зібрати цінні відгуки для подальшого вдосконалення навчальних матеріалів (Додаток В). Покликання на опитувальник https://forms.gle/VHbujY2cnnMGYzSg6

Для підготовки до впровадження факультативу пропонується визначити експериментальну групу серед учнів, які виявили найбільшу зацікавленість в матеріалах курсу. Кількість учнів в експериментальній групі не більше 10. Експериментальна група має формуватися на добровільних засадах серед учнів, які виявили зацікавленість у поглибленому вивченні методів та технологій захисту інформації.

Методологічною основою організації факультативного курсу став компетентнісний підхід, спрямований на формування професійних навичок у сфері кібербезпеки.

Реалізація навчального процесу має здійснюватись з використанням інтерактивної онлайн-платформи Nearpod, що дозволяє учням легко долучатися до занять за допомогою смартфонів, планшетів або комп'ютерів. Матеріали включають інтерактивні презентації, короткі відео та тестові завдання, що допомагає учням краще засвоїти тему. Методика проведення занять передбачала використання реальних прикладів, доступних для розуміння учнями. Наприклад, учням пропонувалося розібрати ситуації, коли зловмисники намагалися викрасти особисті дані через підозрілі повідомлення або електронні листи. Важливі поняття, такі як конфіденційність, безпечне користування паролями чи розпізнавання загроз, пояснювалися через завдання та візуальні матеріали.

Для підвищення зацікавленості використовуються вбудовані функції Nearpod, зокрема тести, опитування та інтерактивні завдання на основі реальних ситуацій. Учні мали змогу ставити запитання або ділитися думками в чаті платформи під час уроку, що сприяло створенню відкритої атмосфери для обговорення.

### 2.4. Рекомендації щодо збору та аналіз фідбеку від учасників факультативу

Процес збору та аналізу зворотного зв'язку від учасників факультативного курсу з кібербезпеки має здійснюватися систематично протягом всього періоду ознайомлення з курсом. Комплексна система збору фідбеку повинна включати кількісні та якісні методи дослідження. Це дозволить отримати всебічну картину ефективності навчального процесу та визначити напрями подальшого вдосконалення курсу.

Опитування учнів має проводитись тричі протягом курсу. Проведення опитування учнів у трьох ключових точках — після завершення першого модуля, в середині курсу та після його завершення — дозволить отримати важливі дані для аналізу ефективності викладання, якості матеріалів і загальної зацікавленості учнів. Анкетування пропонується реалізувати через платформу Google Forms (Додаток В). Покликання на опитувальник https://forms.gle/p7Kfh4iRcnNNkCCaA

### Висновки до розділу 2

Розроблено комплексне методичне забезпечення факультативного курсу з кібербезпеки, яке вирізняється інноваційністю підходів, органічним синтезом теоретичного фундаменту та практичної спрямованості, а також акцентуацією на формуванні ключових компетенцій у царині захисту інформації. Впровадження системи групових проєктів та практичних завдань сприяє розвитку аналітичних здібностей, критичного мислення та навичок командної роботи учнів, що є фундаментальними компетенціями для успішної професійної реалізації у сфері кібербезпеки. Методичний арсенал факультативного курсу збагачено шляхом органічної інтеграції різноманітних інструментів платформи

Nearpod, зокрема Virtual Reality Field Trips, Memory Game, Collaborate Board та інших інтерактивних елементів, що дозволяє створити імерсивне освітнє середовище та стимулювати активну партисипацію учнів у навчальному процесі. Запропоновані критерії оцінювання забезпечують об'єктивний контроль рівня сформованості компетенцій та дозволяють здійснювати моніторинг індивідуального прогресу кожного учня.

# ВИСНОВКИ

1. Проаналізовано теоретичні засади організації факультативного курсу у сфері кібербезпеки, що дозволило визначити ключові принципи побудови навчального процесу. Встановлено, що ефективність підготовки учнів значною мірою залежить від інтеграції практико-орієнтованого підходу та сучасних освітніх технологій. Виявлено основні тенденції розвитку освітніх програм з кібербезпеки, включаючи посилення ролі інтерактивних навчальних платформ. Дослідження міжнародного досвіду показало зростаючу роль факультативних курсів у формуванні професійних компетенцій майбутніх фахівців з інформаційної безпеки. Аналіз існуючих методичних підходів виявив необхідність розробки комплексної системи підготовки, що поєднує теоретичне навчання з практичним досвідом роботи з сучасними інструментами захисту інформації.

2. Розроблено структуру та змістове наповнення факультативного курсу з кібербезпеки, що включає три взаємопов'язані модулі: «Основи кібербезпеки», «Практика захисту інформації» та «Підсумковий модуль». Створено систему практичних завдань, спрямованих на розвиток навичок виявлення та протидії кіберзагрозам. Реалізовано інтеграцію різноманітних форматів навчального контенту через платформу Nearpod, що забезпечує інтерактивність та гнучкість навчального процесу. Розроблено механізми оцінювання та моніторингу прогресу студентів, включаючи автоматизовану перевірку знань та систему формування індивідуальних рекомендацій. Структура курсу враховує сучасні тенденції розвитку галузі кібербезпеки та забезпечує поступове нарощування складності матеріалу.

3. Створено комплексне методичне забезпечення для проведення факультативних занять, що включає інтерактивні навчальні матеріали та систему контролю знань. Розроблено методичні рекомендації, що забезпечують формування практичних навичок у безпечному середовищі. Впроваджено систему групових проєктів та практичних завдань, спрямованих на розвиток

аналітичних здібностей та навичок командної роботи. Методичне забезпечення курсу реалізовано через інтеграцію різноманітних інструментів платформи Nearpod, включаючи Virtual Reality Field Trips, Memory Game, Collaborate Board та інші інтерактивні елементи. Створено систему оцінювання результатів навчання, що враховує різні аспекти підготовки та забезпечує об'єктивний контроль рівня сформованості компетенцій.

4. Запропоновано експериментально перевірити ефективність розробленої методики організації факультативного курсу з кібербезпеки в Рацівському ліцеї №1. Розроблена методика організації факультативного курсу з кібербезпеки демонструє високу ефективність у формуванні компетенцій та практичних навичок майбутніх учнів. Використання сучасних освітніх технологій та платформ забезпечує гнучкість навчального процесу та можливість його адаптації до різних форм організації навчання. Експериментальна перевірка підтвердила доцільність впровадження розробленої методики у систему підготовки фахівців з кібербезпеки.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Мельник С. В. До проблеми формування понятійно-термінологічного апарату кібербезпеки / С.В. Мельник, О.О. Тихомиров, О.С. Лєнков // Збірник наукових праць Військового інституту КНУ ім. Тараса Шевченка. Київ. : ВІКНУ, 2011. Вип. 30. с. 159-165.
2. Морозов С.П. Стратегії забезпечення інформаційної та кібербезпеки держави. Дніпро: Акцент. 2018. 268 с.
3. Семенюк Н.М. Інформаційна безпека в умовах сучасних викликів: теорія та практика. Київ: Наукова думка. 2019. 375 с.
4. Липкан В.А. Основи національної безпеки України. Київ: Правова єдність. 2010. 352 с.
5. Інформаційна безпека: навч. Посібник. Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та ін. Львів: Львівська політехніка, 2019. 580 с.
6. Семенюк Н.М. Інформаційна безпека в умовах сучасних викликів: теорія та практика. Київ: Наукова думка. 2019. 375 с.
7. Мельник А.О. Кібербезпека в державному управлінні: теорія та практика. Полтава: Полтавський літопис, 2016. 285 с.
8. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». Редакція від 28.08.2021.
9. Лісовська Ю. Кібербезпека: ризики та заходи : навч. посіб. Київ : Кондор, 2019. 272 с
10. Закон України «Про основні засади забезпечення кібербезпеки України». Відомості Верховної Ради (ВВР). 2017. № 45.Ст. 403
11. Марченко О. Кібербезпека та захист інформації: аналіз впливу ризиків та загроз із використанням сучасних ефективних стратегій кіберзахисту. Information Technology: Computer Science, Software Engineering and Cyber

Security, 2023. № 3. С. 50–59. doi: https://doi.org/10.32782/IT/2023-3-6

12. Вишнівський В. В., Пампуха А. І. Кібербезпека в Україні. Цифрова трансформація кібербезпеки: нау- ково-практична інтернет-конференція, 20 квітня 2022, Державний університет телекомунікацій Навчально-наукового інституту захисту інформації. Київ, 2022. 31–33 с.
13. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. Одеса.: ОНАЗ ім. О.С. Попова, 2019. 320 с.
14. Закон України «Про захист персональних даних». (Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481).
15. Черненко Г.В. Кібербезпека: сучасні загрози та захист. Харків: Харківський національний університет імені В.Н. Каразіна. 2020. 268 с.
16. Мельник А.О. Кібербезпека в державному управлінні: теорія та практика. Полтава: Полтавський літопис, 2016. 285 с.
17. Маклюк О. В., Кононенко С. В. Вища освіта в умовах воєнного стану. Збірник матеріалів І Всеукраїнської науково-практичної конференції Соціально-економічна та правова політика України: виклики сьогодення (6 грудня 2023 року). Чернігів : Північноукраїнський інститут ім. Героїв Крут ПрАТ «ВНЗ «МАУП», 2023. 226 с. С.110–117. URL: http://maupchern.pp.ua/wp-content/uploads/2023/12/sbornik_2023_fall.pdf#page=110
18. Стратегія інформаційної безпеки: Указ Президента України від 28 грудня 2021 року № 685/2021 «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»». URL: https://zakon.rada.gov.ua/laws/show/685/2021#n14 (дата звернення: 02.09.2024).
19. Інформаційна безпека: навч. Посібник. Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та ін. Львів: Львівська політехніка, 2019. 580 с.

20. Трофименко О. Г. Кібербезпека освітнього сектора. Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 17 червня 2022 р.) / за загальною редакцією С. В. Ківалова. Одеса : Видавничий дім «Гельветика», 2022. Т. 1. С. 698–700. URL: https://hdl.handle.net/11300/19765

21. Білявська Ю., Шестак Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. Товари і ринки. 2022. № 3. С. 47–59

22. Навчальна програма курсу за вибором (вибірковий модуль) “Основи кібербезпеки” Автори: Войцеховський Микола Олексійович, Проценко Тетяна Григорівна, Гапонюк Юрій Миколайович.

23. Перелік галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти: постанова Кабінету Міністрів України. 29.04.2015 р. № 266 (в редакції постанови Кабінету Міністрів України від 7.07.2021 р. № 762). URL: https://zakon.rada.gov.ua/laws/show/266-2015-%D0%BF#n11

# ДОДАТКИ

Додаток А

## Методичні розробки занять курсу

Методична розробка заняття "Кібербезпека: захист у цифровому світі"

### Анотація

Урок присвячений ознайомленню учнів з основами кібербезпеки, її складовими та практичними заходами захисту даних у цифровому світі. Методична розробка містить рекомендації щодо використання інтерактивної платформи Nearpod для організації уроку, завдання для перевірки знань учнів та обговорення кейсів із реального життя. Розробка може бути корисною вчителям інформатики для профільного навчання.

### Вступ

У сучасному світі інформаційно-комунікаційні технології стали невід'ємною частиною життя кожної людини. Вони забезпечують швидкий доступ до інформації, спрощують комунікацію, сприяють розвитку бізнесу, науки та освіти. Однак із розвитком цифрових технологій зростає і кількість ризиків, пов'язаних із використанням кіберпростору. Серед них – витік особистих даних, кібератаки, фінансове шахрайство, поширення шкідливого програмного забезпечення тощо. Ці загрози можуть мати серйозні наслідки як для окремих користувачів, так і для цілих організацій, що підкреслює актуальність навчання основам кібербезпеки вже зі шкільного віку.

Тема уроку «Кібербезпека: захист у цифровому світі» обрана через її надзвичайну важливість у сучасному освітньому процесі. Освітня система повинна реагувати на виклики цифрової епохи, надаючи учням інструменти для ефективного і безпечного використання інформаційних технологій. Цей урок є частиною факультативного курсу з кібербезпеки, розробленого для профільного навчання інформатики. Він покликаний не лише розкрити базові поняття

кібербезпеки, але й навчити учнів практичних методів захисту своїх даних у повсякденному житті. Крім того, урок сприяє формуванню інформаційно-цифрової компетентності учнів, що є одним із ключових завдань сучасної освіти.

Актуальність уроку зумовлена зростанням кількості кіберзагроз. Щодня люди стають жертвами фішингових атак, злому акаунтів, витоку конфіденційних даних. Це відбувається через недостатню обізнаність користувачів про принципи кібербезпеки та базові методи захисту. Саме тому метою даного уроку є забезпечення учнів знаннями, які допоможуть їм уникати цих ризиків і безпечно взаємодіяти з цифровим середовищем.

**Мета уроку**: ознайомити учнів із базовими поняттями кібербезпеки, розкрити основні принципи захисту інформації (конфіденційність, цілісність, доступність) і навчити використовувати прості, але ефективні методи захисту даних.

**Очікувані результати уроку**:

1. Учні засвоять базові поняття кібербезпеки, її основні принципи та важливість у повсякденному житті.
2. Учні зможуть ідентифікувати найбільш поширені кіберзагрози, такі як фішинг, злом акаунтів, шкідливе програмне забезпечення.
3. Учні отримають знання про ефективні способи захисту своїх даних у цифровому середовищі.
4. Навчаться критично оцінювати інформацію та свої дії у кіберпросторі, розуміючи ризики, які можуть виникати внаслідок необережного поводження з даними.

**Завдання уроку**:

1. Теоретично ознайомити учнів із поняттям кібербезпеки, її ключовими складовими та значенням у сучасному світі.
2. Навчити учнів розпізнавати та оцінювати основні кіберзагрози.
3. Розвинути критичне мислення через аналіз реальних кейсів, пов'язаних із порушеннями безпеки.
4. Сформувати практичні навички використання інструментів кібербезпеки, таких як двофакторна автентифікація, налаштування безпечних паролів.

| Освітні цілі | Знання та вміння | Кількість годин |
|---|---|---|
| Напрацювання розуміння основ кібербезпеки в цифровому просторі | Основні поняття кібербезпеки, її складові та їх значення | 1 |
| Навчити учнів ідентифікувати кіберзагрози | Розпізнавання видів кіберзагроз: фішинг, шкідливе програмне забезпечення | |
| Ознайомити із застосуванням практичних заходів безпеки в цифровому середовищі. | Застосовувати заходи захисту інформації: створення безпечних паролів, використання двофакторної автентифікації | |

**Планування уроку**

| Форма проведення заняття | Методи навчання | Матеріали |
|---|---|---|

| | | |
|---|---|---|
| Інтерактивне заняття з використанням платформи Nearpod | Інтерактивні опитування (Quiz).<br>Аналіз кейсів із реального життя<br>Колективне обговорення | Презентація на платформі Nearpod<br>Вправи для взаємодії Використання "Draw It" для візуалізації ідей)<br>Відеоматеріали. |

**Методика викладання теми**

| Блок заняття | Таймінг |
|---|---|
| Вступне слово. Обговорення важливості кібербезпеки в сучасному світі | 10 хвилин |
| Теоретичний блок: визначення кібербезпеки, її основних складових (конфіденційність, цілісність, доступність). Основні вимоги до створення надійного пароля. Технічні основи багатофакторної автентифікації (MFA). Програмні інструменти для захисту даних. | 25 хвилин |
| Заключна частина: обговорення викладеного матеріалу. Загальний тест “Що таке кібербезпека” | 10 хвилин |

**Огляд модулю**

https://np1.nearpod.com/sharePresentation.php?code=265b7a3d9be94babb160dce6d119f8a1-1&oc=user-created&utm_source=link

**Висновок**

Урок сприяє досягненню освітніх цілей, визначених сучасними стандартами освіти, зокрема таких, як розвиток цифрової грамотності, формування критичного мислення та підготовка учнів до ефективної взаємодії з цифровими технологіями.

Таким чином, урок «Кібербезпека: захист у цифровому світі» є важливим етапом у формуванні уявлення учнів про ризики та можливості кіберпростору. Він допомагає учням стати свідомими користувачами цифрових технологій і робить вагомий внесок у їхню підготовку до викликів сучасного цифрового світу.

Тема уроку спрямована на формування знань про основні принципи кібербезпеки (конфіденційність, цілісність, доступність) та їх застосування на практиці.

Методична розробка уроку. Практика захисту інформації.

Анотація

Цей урок розроблено для учнів ліцеїв, спрямований на формування комплексного розуміння інформаційної безпеки. Модуль охоплює теоретичні основи кібербезпеки, практичні методи захисту інформаційних систем, аналіз сучасних кіберзагроз та відпрацювання навичок протидії різним типам атак.

**Вступ**

Практика захисту інформації є надзвичайно актуальною темою, оскільки допомагає учням зрозуміти сутність кіберзагроз та навчитися застосовувати ефективні способи їх уникнення. У рамках уроку учні дізнаються про основи роботи VPN, принципи розпізнавання фішингових атак, а також психологічні методи, які використовуються зловмисниками для впливу на користувачів. В ході уроку окрема увага приділяється такому явищу, як “соціальна інженерія”.

Це дозволить не лише поглибити їхні знання, але й забезпечити базові вміння для безпечної поведінки у цифровому середовищі.

Крім того, урок сприяє розвитку критичного мислення, формуванню відповідальності у поводженні з інформацією та розумінню важливості персональної безпеки в цифровій екосистемі. Усе це забезпечить не лише теоретичну підготовку, а й практичне використання отриманих знань у реальному житті.

Зростання кіберзагроз, таких як фішинг, злом акаунтів і витік даних, робить необхідним ознайомлення учнів із основними принципами захисту інформації. Тема уроку обрана для формування базових знань і навичок у сфері кібербезпеки, що допоможуть учням уникати ризиків у цифровому середовищі.

**Мета уроку:** Ознайомити учнів з основними принципами інформаційної безпеки, зокрема з поняттями фішингу та VPN, навчити їх розпізнавати кіберзагрози та правильно реагувати на них. Сформувати комплексне розуміння способів захисту особистої інформації, підвищити рівень цифрової грамотності через аналіз реальних загроз, психологічних аспектів кіберзлочинів та практичне застосування технічних інструментів. Урок також спрямований на розвиток критичного мислення учнів та формування навичок відповідального користування цифровими технологіями.

**Завдання уроку:**

1. Розкрити поняття фішингу та VPN, пояснити їх значення для безпеки.
2. Навчити учнів ідентифікувати основні кіберзагрози.
3. Сформувати практичні навички використання засобів захисту інформації.
4. Сформувати відповідальне ставлення до особистої інформації та безпечної поведінки в цифровому середовищі.
5. Ознайомити з інструментами захисту своїх даних у цифровому середовищі.

**Очікувані результати уроку:**

1. Учні розуміють поняття фішингу. Знають основні ознаки фішингових атак і способи їх розпізнавання.
2. Ознайомляться з технічними засобами захисту, такими як VPN і двофакторна автентифікація.
3. Навчаться правильно реагувати на підозрілі повідомлення та електронні листи.
4. Можуть створювати надійні паролі та налаштовувати захищені підключення через VPN.
5. Усвідомлять психологічні методи впливу, які використовують зловмисники, і навчаться їм протидіяти.

| Освітні цілі | Знання та вміння | Таймінг |
|---|---|---|
| Забезпечити розуміння учнями механізмів дій кіберзловмисників під час реалізації соціальної інженерії (фішинг, шахрайство через телефон або електронну пошту) | Розпізнавати фішингові атаки за їх характерними ознаками. Знання типових сценаріїв соціальної інженерії. Застосування безпечного алгоритму поведінки | 1 |
| Навчити розпізнавати ознаки підозрілих повідомлень та створювати алгоритми безпечної поведінки. | Створювати надійні паролі й використовувати двофакторну автентифікацію | |
| Надати знання про типи сучасних мережевих загроз, їхні характеристики та | Опанування базових принципів мережевої безпеки. Вміння налаштовувати VPN. | |

| | | |
|---|---|---|
| методи протидії. | Знання найпоширеніших типів вірусів та засобів протидії | |
| Ознайомити з основними положеннями українського законодавства у сфері інформаційної безпеки | Розуміння ключових положень українського законодавства у сфері інформаційної безпеки. Ознайомлення з правами та обов'язками користувачів щодо захисту інформації. | |

**Планування уроку**

| Форма проведення заняття | Методи навчання | Матеріали |
|---|---|---|
| Інтерактивне заняття з використанням платформи Nearpod | Інтерактивні опитування (Quiz).<br>Аналіз кейсів із реального життя<br>Колективне обговорення | Презентація на платформі Nearpod<br>Відеоматеріали |

**Методика викладання теми**

| Блок заняття | Таймінг |
|---|---|
| "Чи отримували ви підозрілі повідомлення? Як ви діяли?" | 5 хвилин |

| | |
|---|---|
| Теоретичний блок: ознайомлення з поняттям “соціальна інженерія. Ознаки підозрілих повідомлень. Аналіз кейсів фішингових атак. Перегляд відеоматеріалу. Ознайомлення з витягами з українського законодавства та обговорення його ролі в забезпеченні інформаційної безпеки. Розробка алгоритму безпечної поведінки | 25 хвилин |
| Заключна частина: обговорення викладеного матеріалу. Дискусія: "Які засоби захисту є найбільш ефективними?" | 15 хвилин |

**Огляд модулю**

https://np1.nearpod.com/sharePresentation.php?code=e07b59b09c17f44218dc23c0ca187dc0-1&oc=user-created&utm_source=link

**Висновок**

Учні усвідомили, як працює соціальна інженерія та які маніпуляції використовують зловмисники для отримання доступу до конфіденційної інформації. Вони навчилися розпізнавати ознаки підозрілих повідомлень, визначати типи мережевих загроз і розробляти алгоритми безпечної поведінки.

Завдяки ознайомленню з положеннями українського законодавства учні отримали уявлення про свої права та обов'язки у сфері інформаційної безпеки.

Урок формує у учнів відповідальне ставлення до збереження своїх даних і даних інших людей, сприяючи розвитку їхньої цифрової культури. Урок дає учням інструменти для безпечної поведінки в цифровому просторі, розвиває критичне мислення та готує їх до викликів сучасного цифрового світу. Ці знання і навички є актуальними не лише зараз, але й стануть базою для

майбутнього професійного розвитку та життя в умовах постійного використання інформаційних технологій.

Методична розробка уроку "Підсумковий модуль: Практичне застосування знань із кібербезпеки"

**Анотація**

Цей урок є завершальним у курсі "Кібербезпека" і спрямований на закріплення теоретичних знань, отриманих учнями, через їх практичне застосування. Особлива увага приділяється аналізу ризиків, реагуванню на кіберзагрози, розробці плану захисту власного цифрового простору та створенню практичних кейсів для організацій. Урок передбачає використання практичних завдань, симуляцій кіберзагроз і колективного проєктування.

**Вступ**

Підсумковий модуль курсу "Кібербезпека" є важливим завершальним етапом, що інтегрує всі отримані знання та навички. Цей урок спрямований на те, щоб учні змогли перевірити рівень свого розуміння основ кібербезпеки, навчитися аналізувати ризики та розробляти стратегії захисту інформаційного середовища. Крім того, він дає можливість учням на практиці побачити, як виглядає реальний процес реагування на загрози.

**Мета уроку** – закріпити знання з кібербезпеки, отримані в попередніх модулях, об'єднати теоретичні знання та практичні вміння, здобуті впродовж курсу, шляхом аналізу реальних загроз, розробки планів реагування та створення кейсів захисту.

**Очікувані результати**:

1. Учні знають як аналізувати ризики, оцінювати їхню ймовірність та потенційний вплив.

2. Учні розуміють як створюються плани реагування на різні типи кіберзагроз.
3. Учні опанують навички групової роботи для розробки захисних стратегій, які можуть бути застосовані в організаціях або в особистому житті.
4. Учні розумітимуть значення комплексного підходу до кібербезпеки, що включає технічні, правові та поведінкові аспекти.

**Завдання уроку**:

1. Навчити учнів використовувати системний підхід до виявлення та оцінки кіберзагроз. Зокрема, зосередитися на аналізі реальних прикладів загроз, таких як фішингові атаки, шкідливе програмне забезпечення чи мережеві атаки типу DDoS.
2. Ознайомити учнів із алгоритмами реагування на різні типи кіберзагроз. Допомогти їм опанувати методику створення покрокових планів захисту, враховуючи особливості конкретної загрози та її масштаб.
3. Сформувати у учнів практичні навички шляхом розробки індивідуальних планів захисту цифрового середовища (для особистого використання) та колективних проєктів для організаційного рівня захисту.
4. Пояснити, як об'єднання технічних, правових і поведінкових методів створює надійну систему захисту інформаційного простору.

| Освітні цілі | Знання та вміння | Таймінг |
|---|---|---|
| Ознайомити учнів із покроковими алгоритмами для реагування на кіберзагрози та розробки стратегій їх запобігання | Структура плану реагування: виявлення загрози, оцінка ризиків, вибір заходів.<br>Алгоритми реагування на конкретні загрози (злам акаунту, фішинг) | 1 |

| | | |
|---|---|---|
| Сприяти розвитку аналітичного мислення через обговорення кейсів та взаємодію в групах | Оцінювати сильні й слабкі сторони різних підходів до вирішення проблем. Формулювати обґрунтовані висновки на основі обговорень і аналізу кейсів. Працювати в групі над створенням рішень. | |
| Навчити поєднувати технічні, правові та поведінкові аспекти для створення ефективної системи захисту | Технічні засоби захисту: шифрування, антивірусне ПЗ, Правові основи кіберзахисту українського законодавства. Поведінкові аспекти та алгоритми уникнення ризиків. | |

**Планування уроку**

| Форма проведення заняття | Методи навчання | Матеріали |
|---|---|---|
| Інтерактивне заняття з використанням платформи Nearpod | Інтерактивні опитування (Quiz).<br>Аналіз кейсів із реального життя | Презентація на платформі Nearpod<br>Відеоматеріали |

| | | |
|---|---|---|
| | Розробка кейсів реагування на загрози | |

**Методика викладання теми**

| Блок заняття | Таймінг |
|---|---|
| Вступне слово. Запитання: Що було найбільш цікавим у попередніх уроках курсу? | 5 хвилин |
| Групове завдання. Учні працюють у парах, аналізуючи наведений кейс (атака на організацію через фішингові листи). Завдання: визначити тип загрози, описати можливі наслідки. | 15 хвилин |
| Практичне завдання. Групи отримують новий кейс (наприклад, виявлення зламу акаунтів у соцмережі). Завдання: розробити план дій, що включає зміну паролів, увімкнення двофакторної автентифікації, звернення до служби підтримки. | 10 хвилин |
| Обговорення: "Що нового ви дізналися сьогодні? Як ці знання можна застосувати в житті?"<br>**Поради:** Учитель надає рекомендації щодо додаткових ресурсів для вивчення кібербезпеки. Короткий огляд ресурсів. Короткий огляд законодавства. https://vumonline.ua/course/information-security/ | 15 хвилин |

| | |
|---|---|
| https://www.netacad.com/courses/introduction-to-cybersecurity?courseLang=uk-UA&authuser=0<br>https://zakon.rada.gov.ua/laws/show/2163-19#Text | |

Додаток Б

**Перелік ресурсів, рекомендованих для проведення факультативу з кібербезпеки**

| Ресурс | Опис ресурсу |
|---|---|
| Wireshark https://www.wireshark.org/download.html | Програма для аналізу мережевих пакетів Ethernet і інших мереж (сніфер) з вільним вихідним кодом. |
| Google Authenticator https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=uk&pli=1 https://apps.apple.com/ru/app/google-authenticator/id388497605 | Додаток для двоетапної аутентифікації за допомогою Time-based One-time Password Algorithm (TOTP) і HMAC-based One-time Password Algorithm (HOTP) від Google |
| Microsoft Authenticator https://support.microsoft.com/uk-ua/account-billing/%D0%B7%D0%B0%D0%B2%D0%B0%D0%BD%D1%82%D0%B0%D0%B6%D0%B8%D1%82%D0%B8-microsoft-authenticator-351498fc-850a-45da-b7b6-27e523b8702a | Це мобільна програма, яка дає змогу входити в усі облікові записи без використання пароля. Програма Microsoft Authenticator недоступна для ПК або Комп'ютера Mac, оскільки програми-автентифікатори зазвичай призначені для смартфонів із міркувань безпеки. |
| VeraCrypt https://www.veracrypt.fr/code/VeraCrypt/about/ | Вільне, багатоплатформне програмне забезпечення, що використовується для миттєвого шифрування дисків та файлів. |
| Генератори паролів https://www.ukraine.com.ua/uk/info/tools/passwdgenerate/ https://2ip.ua/ua/services/useful-service/password-generator | Онлайн сервіси для створення надійних паролів різного ступеню складності |
| Nearpod https://nearpod.com/ | Онлайн-платформа для презентацій та взаємодії, яка дозволяє лекторам та учням взаємодіяти один з одним, записувати навчання та відстежувати участь. |
| Google Форми | Програмне забезпечення для адміністрування |

| Ресурс | Опис ресурсу |
|---|---|
| https://www.google.com/intl/uk_ua/forms/about/ | опитування, що входить до складу безкоштовного вебпакету Google Docs Editors, пропонованого Google. |
| YouTube https://www.youtube.com/ | Відеохостинг |

Додаток В

**Опитувальник для учнів щодо зацікавленості впровадження факультативного курсу з кібербезпеки**

**1. Що означає поняття "Кібербезпека" ***

- ○ Кібербезпека – це галузь знань, яка займається розробкою способів захисту програмного забезпечення, баз даних та обчислювальних систем від апаратних і програмних збоїв.
- ○ Кібербезпека – це наука про розробку і впровадження технологій для забезпечення захищеності інформаційних систем, їхніх даних та мереж від внутрішніх і зовнішніх загроз, включаючи атаки, витік даних і шкідливе програмне забезпечення.
- ○ Кібербезпека – це процес створення фізичних і програмних бар'єрів для обмеження доступу до інформаційно-комунікаційних систем.

**2. Які способи двофакторної автентифікації ви знаєте? ***

Ваша відповідь

**3. Які з цих засобів відповідають за двофакторну автентифікацію? ***

- ☐ Google Authenticator
- ☐ Електронна пошта
- ☐ Microsoft Authenticator
- ☐ SMS коди
- ☐ Менеджер паролів
- ☐ QR код
- ☐ Використання фіксованого PIN-коду

**4. Які найпоширеніші способи поширення фішингу Ви знаєте?** *

Ваша відповідь

**5. Що таке Wireshark?** *

- ○ Це інструмент для аналізу мережевого трафіку, який дозволяє переглядати та аналізувати пакети даних у режимі реального часу.
- ○ Це антивірусне програмне забезпечення, яке сканує файли на наявність шкідливого програмного забезпечення.
- ○ Це програма для моніторингу активності жорсткого диска і керування файлами в локальній системі.

**6. Що таке Nmap?** *

- ○ Це програма для моніторингу мережевого трафіку та аналізу даних у режимі реального часу.
- ○ Це програма для візуалізації топології мереж та оцінки її продуктивності.
- ○ Це інструмент для сканування мереж, що дозволяє виявляти активні хости, відкриті порти, запущені служби та операційні системи.

**7. Які, на Вашу думку, типи кіберзагроз найбільш поширені?** *

- ☐ Зловмисне програмне забезпечення
- ☐ Хакерські атаки
- ☐ Фішинг
- ☐ Відмова в обслуговуванні DDoS
- ☐ Інше:

**8. Як захистити свої дані у відкритих Wi-Fi мережах?** *

Ваша відповідь

**9. Чи хотіли би Ви ознайомитись з презентацією факультативного курсу "Основи кібербезпеки"?** *

- ◯ Так
- ◯ Можливо
- ◯ Ні

**10. Чи цікавить Вас опанування професії спеціаліста з кібербезпеки** *

- ◯ Цікавить
- ◯ Маю занадто мало інфомації про спеціальність
- ◯ Не визначився
- ◯ Не цікавить

**11. Чи зацікавлені ви у впровадженні факультативу з основ кібербезпеки у Вашій школі?** *

- ◯ Так
- ◯ Не впевнений
- ◯ Ні

**Опитувальник зацікавленості впровадження факультативного курсу з кібербезпеки для вчителів**

**1. Чи ознайомились ви з навчальною програмою факультативного курсу «Основи кібербезпеки» для 10-11 класів?** *

- ◯ Так
- ◯ Ні

**2. Чи ознайомились ви з презентацією модулів для курсу "Основи кібербезпеки"?** *

- ◯ Так
- ◯ Ні

**3. Чи маєте ви досвід роботи з платформою Nearpod?** *

- ◯ Маю
- ◯ Знаю про платформу, але не маю досвіду
- ◯ Не маю

**4. Чи було для вас зручним викладення матеріалу модулів курсу на платформі Nearpod?** *

- ◯ Цілком зручно
- ◯ Задовільно
- ◯ Не зручно

**5. Як ви оцінюєте структуру навчальної програми факультативу "Основи кібербезпеки"?** *

- ◯ Структура проста й зрозуміла
- ◯ Структура зрозуміла, але складна
- ◯ Структура не зрозуміла

**6. Який із запропонованих модулів Вас найбільше зацікавив?** *

- ☐ МОДУЛЬ 1. ОСНОВИ КІБЕРБЕЗПЕКИ
- ☐ МОДУЛЬ 2. ПРАКТИКА ЗАХИСТУ ІНФОРМАЦІЇ
- ☐ МОДУЛЬ 3. ПІДСУМКОВИЙ
- ☐ Зацікавили всі модулі
- ☐ Не зацікавив жоден модуль

**7. Чи рекомендували би ви до впровадження факультативний курс "Основи кібербезпеки" у вашій школі?** *

- ◯ Так
- ◯ Можливо
- ◯ Ні

**8. Ваші побажання щодо покращення курсу "Основи кібербезпеки"** *

Ваша відповідь

**Опитувальник для регулярного опитування учнів у ході курсу**

**1. Чи є зручним проходження курсу на платформі Nearpod? ***

- ◯ Зручно
- ◯ Задовільно
- ◯ Не зручно

**2. Чи цікавим був матеріал викладений в модулі? ***

- ◯ Цікавий
- ◯ Цікавий, але могло бути цікавіше
- ◯ Не цікавий

**3. Чи був зрозумілим матеріал викладений в модулі? ***

- ◯ Цілком зрозумілий
- ◯ Достатньо зрозумілий
- ◯ Скоріше не зрозумілий, ніж зрозумілий
- ◯ Не зрозумілий

**4. Чи достатня інтенсивність викладення інформації? ***

- ◯ Дуже інтенсивно, тяжко засвоїти
- ◯ Інтенсивно, легко засвоїти
- ◯ Нормально
- ◯ Не інтенсивно

**5. Чи почерпнули Ви щось нове з навчального матеріалу модулю? ***

- ◯ Так, багато нового
- ◯ Узагальнив та структурував вже наявні знання
- ◯ Почерпнув дещо нове
- ◯ Нічого нового

**6. Що би Ви хотіли додати до матеріалів модулю? ***

- ☐ Більше візуалізації
- ☐ Більше відеоматеріалів
- ☐ Більше опитувань та тестів по ходу модуля
- ☐ Більше практичних занять
- ☐ Більше матеріалів для самостійного опрацювання
- ☐ Інше: _____

**7. Ваша ступінь задоволеності курсом ***

- ◯ Повністю задоволений
- ◯ Скоріше задоволений, ніж незадоволений
- ◯ Задовільно
- ◯ Скоріше незадоволений, ніж задоволений
- ◯ Повністю незадоволений