МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В.Н. Каразіна

Факультет: **ННІ Каразінський банківський інститут**
Кафедра: **Інформаційних технологій та математичного моделювання**
Спеціальність: **125 Кібербезпека**
Освітня програма: **Кібербезпека в фінансових технологіях**

Група: АБ-41б **денна форма навчання**

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему:

«РОЗРОБКА ІНТЕРАКТИВНОГО, ОСВІТНЬОГО САЙТУ ДЛЯ ПРОТИДІЇ СОЦІАЛЬНІЙ ІНЖЕНЕРІЇ»
ЗА НАКАЗОМ № 4601-5/335 ВІД 07 ЛЮТОГО 2025 РОКУ

здобувача вищої освіти **Ягло Валерії Олександрівни**

Робота допущена до захисту в ЕК
протокол кафедри ІТММ № 13 від 31.05.2025

Завідувач кафедри ІТММ
к.п.н., доцент
_____ Н.І. Стяглик

Науковий керівник
к. ф.-м. н., доцент
_____ Л.Д. Філатова

м. Харків 2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет імені В. Н. Каразіна

Факультет навчально-науковий інститут "Каразінський банківський інститут"
Кафедра інформаційних технологій та математичного моделювання
Рівень вищої освіти перший (бакалаврський)
Спеціальність 125 Кібербезпека
Освітня програма Кібербезпека в фінансових технологіях

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ **Н. І. Стяглик**
Підпис ініціали, прізвище

"08" лютого 2025 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ (ПРОЄКТ)

Ягло Валерії Олександрівни
(прізвище, ім'я, по батькові студента)

1. Тема роботи «Розробка інтерактивного, освітнього сайту для протидії соціальній інженерії»

керівник роботи Філатова Любов Дмитрівна
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від "08" лютого 2025 року № 4601-5/335

2. Строк подання студентом роботи 15 травня 2025 року

3. Перелік питань, які потрібно розробити:

У розділі 1: Поняття соціальної інженерії та її роль у сфері кібербезпеки. Класифікація та аналіз методів соціальної інженерії. Вплив соціальної інженерії на безпеку інформаційних систем. Сучасні підходи до запобігання соціальній інженерії.

У розділі 2: Огляд існуючих освітніх платформ з питань кібербезпеки. Методики навчання протидії соціальній інженерії. Вимоги до освітніх сайтів у сфері інформаційної безпеки. Визначення цільової аудиторії та її потреб.

У розділі 3: Вибір технологій та інструментів для реалізації сайту. Структура, функціональні можливості та навігація сайту. Розробка дизайну та користувацького інтерфейсу. Розробка дизайну та користувацького інтерфейсу. Забезпечення безпеки та доступності освітнього ресурсу.

У розділі 4: Розробка основних модулів сайту. Тестування функціональності та зручності у використанні. Оцінка ефективності сайту для навчання протидії соціальній інженерії. Висновки щодо подальшого вдосконалення ресурсу.

4. План роботи

№ з/п	Назви етапів роботи
1	Вибір здобувачем теми кваліфікаційної бакалаврської роботи
2	Затвердження плану і завдання кваліфікаційної бакалаврської роботи
3	Здача кваліфікаційної бакалаврської роботи керівнику
4	Підпис кваліфікаційної бакалаврської роботи керівника
5	Підпис кваліфікаційної бакалаврської роботи у нормоконтролера
6	Допуск завідувачем кафедри до захисту кваліфікаційної бакалаврської роботи
7	Захист кваліфікаційної бакалаврської роботи

5. Дата видачі завдання 08 лютого 2025 року

Студент _____ **В. О. Ягло**
підпис ініціали, прізвище

Керівник роботи _____ **Л. Д. Філатова Л.Д.**
підпис ініціали, прізвище

РЕФЕРАТ

НА КВАЛІФІКАЦІЙНУ БАКАЛАВРСЬКУ РОБОТУ «РОЗРОБКА ІНТЕРАКТИВНОГО, ОСВІТНЬОГО САЙТУ ДЛЯ ПРОТИДІЇ СОЦІАЛЬНІЙ ІНЖЕНЕРІЇ»

Ягло Валерії Олександрівни

Кваліфікаційна бакалаврська робота містить 54 сторінки, 3 таблиці, 19 рисунків, список літератури з 10 найменувань.

Об′єктом дослідження є інтерактивий, освітній сайт для протидії соціальній інженерії.

Предметом дослідження є створення інтерактивного, освітнього сайту для підвищення обізнаності користувачів щодо методів соціальної інженерії та способів захисту від них.

Мета кваліфікаційної бакалаврської роботи полягає у розробці повноцінного вебресурсу українською мовою, який дозволяє користувачам ознайомитися з теоретичними аспектами соціальної інженерії, перевірити свої знання у форматі тестування та отримати практичні поради щодо безпечної поведінки в цифровому середовищі.

Завданнями кваліфікаційної бакалаврської роботи є:
Дослідити поняття, види та вплив соціальної інженерії на інформаційні системи; проаналізувати існуючі освітні платформи з кібербезпеки; сформулювати вимоги до сучасного освітнього сайту; визначити цільову аудиторію та її інформаційні потреби; спроєктувати структуру, функціонал і інтерфейс майбутнього ресурсу; реалізувати сайт з використанням технологій HTML5, CSS3 та JavaScript; провести тестування ресурсу та оцінити його ефективність для навчальних цілей.

Актуальність дослідження:
На тлі зростаючої кількості атак із використанням соціальної інженерії особливої ваги набуває питання підвищення обізнаності громадян та формування навичок цифрової гігієни. Оскільки більшість атак спрямовані не на технічні вразливості, а саме на психологічні особливості користувача, формування навичок виявлення таких атак є ключовим елементом безпеки. Сучасні освітні інструменти здебільшого не адаптовані до українського контексту, що створює потребу у створенні національних рішень.

За результатами дослідження:
Було створено інтерактивний сайт із трьома розділами: «Теорія», «Тестування» та «Шпаргалка». Реалізовано можливість перевірки знань, підказки до правильних відповідей, таблицю результатів. Уся логіка побудована на клієнтських технологіях, що робить сайт доступним з будь-якого пристрою без потреби в авторизації. Оцінка користувачів підтвердила зручність і ефективність ресурсу.

Практична новизна:

Сайт є унікальним україномовним ресурсом, орієнтованим на популяризацію знань із тематики соціальної інженерії. Він поєднує сучасний підхід до подачі інформації з інтерактивними модулями перевірки знань, що дозволяє користувачам не лише ознайомитися з темою, а й закріпити її через практику.

Одержані результати можуть бути використані в навчальному процесі закладів вищої та середньої освіти, для підготовки співробітників у сфері інформаційної безпеки, у профілактичних кампаніях банківських установ та державних органів.

КЛЮЧОВІ СЛОВА:

Соціальна інженерія, інформаційна безпека, фішинг, кібергігієна, вебсайт, інтерфейс, JavaScript, тестування, навчальний ресурс, цифрова безпека.

ABSTRACT

AT QUALIFICATION BACHELOR WORK «DEVELOPMENT OF AN INTERACTIVE, EDUCATIONAL WEBSITE TO COUNTER SOCIAL ENGINEERING»

Yahlo Valeriia

The bachelor's thesis contains 54 pages, 3 tables, 19 drawings, a list of references of 10 titles.

The object of the interactive, educational website to counter social engineering .

The subject of the creating an interactive, educational website to raise user awareness of social engineering techniques and ways to protect against them.

The purpose of a consists in developing a full-fledged web resource in Ukrainian, which allows users to familiarize themselves with the theoretical aspects of social engineering, test their knowledge in a testing format, and receive practical advice on safe behavior in the digital environment.

The tasks of a bachelor's degree are:

To investigate the concept, types and impact of social engineering on information systems; to analyze existing educational platforms on cybersecurity; to formulate requirements for a modern educational website; to determine the target audience and its information needs; to design the structure, functionality and interface of the future resource; implement the site using HTML5, CSS3, and JavaScript technologies; test the resource and evaluate its effectiveness for educational purposes.

The relevance of the

Against the backdrop of the growing number of social engineering attacks, the issue of raising public awareness and developing digital hygiene skills is of particular importance. Since most attacks are not aimed at technical vulnerabilities, but rather at the psychological characteristics of the user, developing skills to detect such attacks is a key element of security. Modern educational tools are mostly not adapted to the Ukrainian context, which creates a need to create national solutions.

According to the results of the research:

An interactive site with three sections was created: "Theory", "Testing" and "Cheat Sheet". The ability to test knowledge, hints to correct answers, and a table of results were implemented. All logic is built on client technologies, which makes the site accessible from any device without the need for authorization. User evaluation confirmed the convenience and effectiveness of the resource.

Main theoretical provisions on the topic of the practical relevance of the site

is a unique Ukrainian-language resource focused on popularizing knowledge on the topic of social engineering. It combines a modern approach to presenting information with interactive knowledge testing modules, allowing users to not only familiarize themselves with the topic, but also consolidate it through practice.

The results obtained can be used in the educational process of higher and secondary education institutions, for training employees in the field of information security, in preventive campaigns of banking institutions and government agencies.

KEYWORDS:
Social engineering, information security, phishing, cyber hygiene, website, interface, JavaScript, testing, educational resource, digital security.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧОК, СИМВОЛІВ І ТЕРМІНІВ

СКУД – система контролю та управління доступом.

WBS – Work Breakdown Structure .

AI — штучний інтелект (англ. AI — Artificial Intelligence) — розділ інформатики, що займається створенням систем, здатних виконувати завдання, які зазвичай потребують інтелектуальної діяльності людини.

DDoS — розподілена атака типу «відмова в обслуговуванні» (англ. Distributed Denial of Service) — атака, спрямована на виведення з ладу веб-ресурсу шляхом перевантаження його запитами.

CMS — система керування вмістом сайту (англ. Content Management System) — програмне забезпечення для створення, редагування та керування цифровим контентом.

UI/UX — інтерфейс користувача та досвід користувача (англ. User Interface/User Experience) — дизайн, орієнтований на зручність взаємодії користувача з сайтом.

HTML/CSS/JS — мови розмітки, стилів і скриптів (англ. HyperText Markup Language / Cascading Style Sheets / JavaScript) — базові технології для розробки веб-інтерфейсів.

IP-адреса — унікальний ідентифікатор пристрою в мережі, що дозволяє здійснювати маршрутизацію трафіку.

Phishing (фішинг) — вид шахрайства, за якого зловмисники видають себе за надійні джерела, щоб змусити жертву надати конфіденційну інформацію.

Spoofing — підміна (англ. Spoofing) — обманна діяльність, за якої зловмисник видає себе за іншу особу, сервіс або пристрій.

Social Engineering (соціальна інженерія) — метод психологічного впливу на користувачів з метою отримання конфіденційної інформації або доступу до систем.

Інтерактивність — властивість сайту реагувати на дії користувача, забезпечуючи динамічну взаємодію.

Кібергігієна — сукупність навичок безпечної поведінки користувача в інформаційному середовищі.

Фактор автентифікації — спосіб підтвердження особистості користувача (наприклад, пароль, біометрія, токен тощо).

Софт-скіли — м’які навички, такі як критичне мислення, комунікація та самоконтроль, важливі для розпізнавання маніпуляцій з боку зловмисників.

ВСТУП

У сучасному цифровому середовищі, де інформаційні технології стали невід'ємною частиною повсякденного життя, питання захисту інформації набувають особливої актуальності. Паралельно з розвитком технічних засобів захисту, методи кібератак стають дедалі витонченішими, пристосовуючись до нових умов і експлуатуючи слабкі ланки систем. Однією з найвразливіших складових будь-якої системи залишається людський фактор. Саме на нього орієнтована соціальна інженерія — комплекс психологічних методів, які використовують зловмисники для отримання конфіденційної інформації, обману користувачів або обходу систем автентифікації.

Атаки, побудовані на методах соціальної інженерії, часто не вимагають складного технічного забезпечення чи глибоких знань у сфері програмування, однак здатні завдати значної шкоди як окремим користувачам, так і цілим організаціям. Фішинг, вішинг, смішинг, підміна особистості, створення фальшивих сайтів та інші техніки щодня використовуються для викрадення особистих даних, банківських реквізитів, доступу до корпоративних ресурсів. Особливо небезпечними такі загрози стають у контексті банківської сфери, освіти, держуправління, охорони здоров'я, а також в умовах масової цифровізації, дистанційної роботи та навчання. [4]

Аналіз останніх років свідчить про стрімке зростання кількості інцидентів, пов'язаних із соціальною інженерією. При цьому, попри зростання загального рівня технічної грамотності населення, значна частина користувачів усе ще не володіє базовими знаннями щодо розпізнавання маніпуляцій, інтернет-шахрайства та методів соціального впливу. Технічний захист інформації, як-от шифрування, багатофакторна автентифікація чи антивірусне ПЗ, не є достатнім без усвідомленої участі самого користувача в процесі захисту інформації.

Саме тому зростає потреба у створенні дієвих освітніх інструментів, орієнтованих на підвищення цифрової обізнаності користувачів. Особливу ефективність демонструють інтерактивні онлайн-платформи, які не лише передають інформацію, а й залучають користувача до активної взаємодії, моделюючи реальні сценарії атак, тестуючи знання, формуючи критичне мислення. Такі інструменти здатні покращити навички безпечної поведінки в інформаційному просторі, що є ключовим елементом загальної кібергігієни.

Метою даної кваліфікаційної роботи є розробка інтерактивного, освітнього веб-ресурсу, орієнтованого на формування у користувачів стійкості до методів соціальної інженерії. Такий сайт має забезпечити доступний і водночас глибокий виклад матеріалу, супроводжуватись прикладами типових атак, вправами, тестами й імітаційними модулями. Основними цільовими групами виступають студенти, працівники організацій, користувачі банківських послуг та всі, хто прагне убезпечити себе у цифровому світі.

Актуальність теми зумовлена не лише стрімким зростанням соціально-інженерних загроз, а й недостатнім рівнем їхнього розуміння серед пересічних користувачів. Більшість навчальних матеріалів є надто теоретичними, недостатньо адаптованими до широкої аудиторії, або взагалі недоступними у зручному форматі. Це створює потребу в сучасному, адаптивному, візуально привабливому освітньому інструменті, який поєднує актуальний контент, інтуїтивний інтерфейс та високий рівень інтерактивності.

Таким чином, ця робота покликана зробити внесок у підвищення загального рівня кіберобізнаності, шляхом розробки інноваційного навчального ресурсу, спрямованого на боротьбу з однією з найнебезпечніших загроз сучасності — соціальною інженерією. Отримані результати можуть бути використані в освітніх програмах, корпоративному навчанні, кібербезпековій профілактиці, а також для підвищення персональної інформаційної гігієни користувачів.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ ТА МЕТОДІВ ЇЇ ПРОТИДІЇ

1.1. Поняття соціальної інженерії та її роль у сфері кібербезпеки

Соціальна інженерія є складовою частиною кіберзагроз, що базується на психологічному впливі на людину з метою отримання конфіденційної інформації або ініціювання певних дій, вигідних для зловмисника. Особливість цієї форми атаки полягає в тому, що замість зламу технічних засобів захисту, атакуючий впливає на «людський фактор» – найвразливіший елемент будь-якої системи інформаційної безпеки [1].

На відміну від класичних кіберзагроз, що використовують програмні засоби, методи соціальної інженерії реалізуються через комунікацію: телефонні дзвінки, електронну пошту, месенджери, соцмережі або особисті зустрічі. У центрі цих атак – маніпуляції свідомістю людини через психологічний тиск, обман, створення фальшивих сценаріїв або виклик довіри [2].

Основними методами є фішинг (phishing), фармінг (pharming), смішинг (smishing), вішинг (vishing), претекстинг (pretexting), спір фішинг (spear phishing) та вейлінг (whaling). Вони використовують різні форми маніпулятивного впливу – від обману до містифікації, як це наведено у таблиці 1.1. [1].

Таблиця 1.1

Залежність форм маніпуляцій від типу соціоінженерної атаки

Різновид соціо інженерної атаки	**Форми маніпулятивного впливу**					
	Шахрайство	Обман	Афера	Інтрига	Містифікація	Провокація
Фішінг	+	+	-	-	-	-
Фармінг	+	+	-	-	-	-

Претекстінг	+	+	+	+	+	+
Смішінг	+	+	-	-	-	-
Вішінг	+	+	-	-	-	-
Спір фішінг	+	+	-	-	-	-
Вейлінг	+	+	-	-	-	-

Основою для використання методів соціальної інженерії є наступне:

- особливості людської свідомості;
- особливості аудиторії або специфіка діяльності;
- некомпетентність аудиторії у сфері кібербезпеки та інформаційної безпеки;
- нестійкі психологічні властивості особистості, що дозволяє шахраям маніпулювати поведінковими стереотипами через основні потреби, слабкості, бажання, ідеали.

Метою соціоінженерних атак є не лише доступ до конфіденційної інформації, а й створення умов, за яких користувач самостійно виконує дії, що порушують політику безпеки (наприклад, відкриває посилання, вводить логін та пароль на підроблених сторінках, завантажує шкідливе програмне забезпечення (рис. 1.1.).

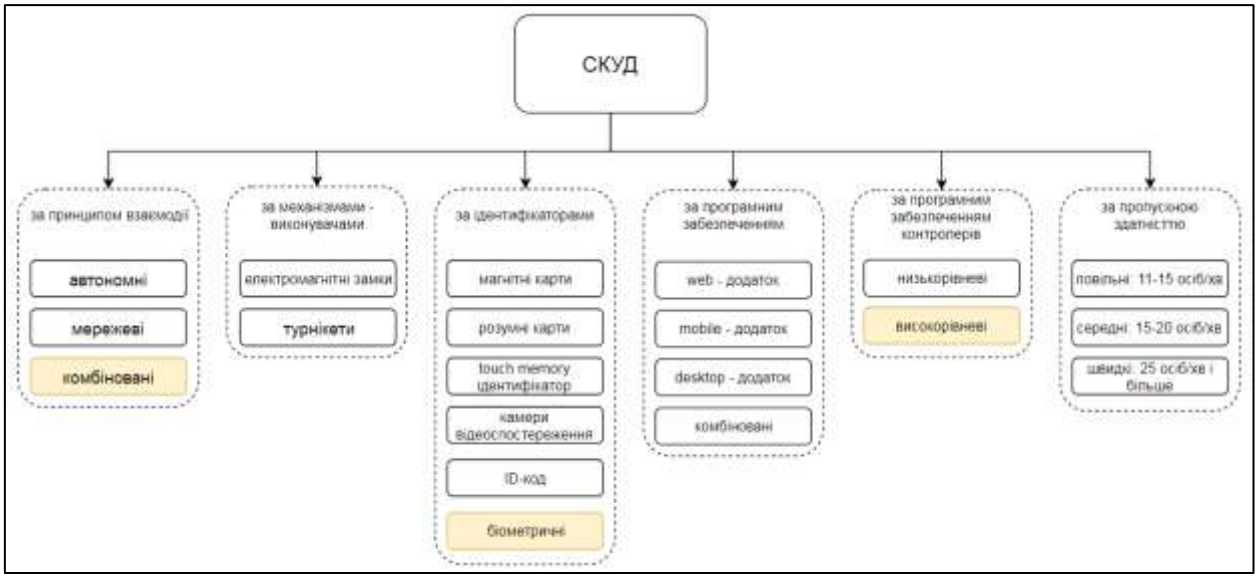


Рис. 1.1. Загальна класифікація СКУД

1.2. Класифікація та аналіз методів соціальної інженерії

Соціальна інженерія — це сукупність прийомів психологічного та

інформаційного впливу, які використовуються зловмисниками з метою маніпулювання поведінкою людей для отримання доступу до конфіденційної інформації, ресурсів або технологічних систем. Незважаючи на прогрес у розвитку технічних засобів захисту, соціальна інженерія залишається одним із найефективніших способів компрометації інформаційної безпеки. Основна причина цього — уразливість людської психіки та відсутність належного рівня обізнаності в питаннях кіберзагроз [3].

Залежно від характеру впливу, каналу комунікації та технік, що застосовуються, методи соціальної інженерії умовно поділяються на кілька основних типів. Їх можна класифікувати за двома основними критеріями: за способом контакту (цифровий або фізичний) та за рівнем підготовленості атаки (масові або цільові).

Найбільш поширеними цифровими методами соціальної інженерії є ті, що реалізуються через цифрові канали, зокрема електронну пошту, соціальні мережі, месенджери або сайти:

- Фішинг (phishing) — це масова розсилка електронних повідомлень, які імітують офіційні повідомлення від банків, державних установ чи відомих онлайн-сервісів. Метою є змусити користувача перейти за шкідливим посиланням і ввести свої дані на підробленому сайті. Цей метод є особливо ефективним завдяки психологічному тиску, терміновості або використанню авторитету відомої організації.
- Смішинг (smishing) — фішингові атаки через SMS. Наприклад, користувач отримує повідомлення про нібито виграний приз або підозрілу активність у банківському акаунті з проханням перейти за посиланням.
- Вішинг (vishing) — маніпулятивні телефонні дзвінки, під час яких шахрай представляється співробітником банку, служби безпеки або іншої організації. Він намагається переконати жертву передати конфіденційні дані, наприклад, CVV-код або одноразовий пароль (OTP).
- Спірфішинг (spear phishing) — цільова атака, спрямована на конкретну особу чи організацію. Перед її проведенням зловмисник ретельно

збирає інформацію про жертву для створення правдоподібного повідомлення. Такі атаки мають високий рівень успішності, оскільки враховують професійні, особисті або соціальні характеристики цілі.

- Бейтінг (baiting) — спроба заманити користувача до виконання певної дії, обіцяючи щось цінне. Наприклад, фейковий банер на сайті з текстом «Завантажити безкоштовно», який веде на шкідливий файл.ї

Поза цифровими методами, соціальна інженерія може мати й фізичний вимір. Фізичними методами соціальної інженері є:

- Тейлгейтинг (tailgating) — метод, за якого зловмисник проникає в охоронювану зону, слідуючи за співробітником організації, який має доступ. Часто використовується у великих офісах, де працівники з ввічливості або необережності можуть впустити «гостя» без перевірки.
- Претекстинг (pretexting) — техніка створення фальшивого контексту або історії, яка виправдовує запит до конфіденційної інформації. Наприклад, зловмисник може представитися співробітником технічної підтримки або податкової служби та просити дані нібито «для оновлення обліку».
- Дампстердайвінг (dumpster diving) — пошук конфіденційної інформації в смітті організації. Попри архаїчність методу, він і досі використовується для збору документів, записок, доступів або паролів, які випадково викинули без знищення.

Також істують комбіновані та гібридні методи. У реальних атаках часто застосовується поєднання кількох методів. Наприклад, зловмисник може спочатку зібрати базову інформацію через соціальні мережі, далі — здійснити вішинг-атаку, а на завершення — відправити фішинговий лист на персоналізовану тему. Такий гібридний підхід значно ускладнює виявлення та реагування на загрозу.

Проводячи аналіз ефективності методів, можна сформувати судження, що соціальна інженерія залишається однією з найуспішніших тактик у сучасних кібератаках. За даними дослідження Verizon Data Breach

Investigations Report (DBIR), 82% порушень безпеки у 2023 році були пов’язані з «людським фактором», включаючи фішинг, помилки персоналу та втрату доступу. Це свідчить про необхідність не тільки технічного захисту, а й постійного навчання персоналу та інформування населення.

1.3. Вплив соціальної інженерії на безпеку інформаційних систем

Соціальна інженерія є однією з найнебезпечніших загроз для інформаційної безпеки, оскільки впливає не лише на технічні засоби захисту, а й безпосередньо на ключовий елемент будь-якої інформаційної системи — людину. Попри наявність сучасних антивірусних систем, фаєрволів, засобів багатофакторної автентифікації, саме людський фактор залишається найвразливішою ланкою у більшості атак. Зловмисники, використовуючи методи психологічного впливу, обходять технічні бар’єри шляхом обману користувачів або співробітників організацій.

Інформаційні системи зазвичай будуються з урахуванням багаторівневого захисту, що включає апаратні, програмні та адміністративні заходи. Однак, якщо працівник під впливом маніпуляції передає конфіденційну інформацію (наприклад, пароль до системи чи конфігурацію мережі), — усі технічні заходи стають безсилими. Саме тому соціальна інженерія має непрямий, але руйнівний вплив на цілісність, доступність і конфіденційність інформації, оброблюваної в ІС [5].

Один із найтиповіших сценаріїв впливу — це компрометація облікового запису адміністратора або користувача з розширеними правами доступу. Використовуючи фішинг або вішинг, зловмисник може отримати одноразовий пароль, який відкриє доступ до корпоративної пошти або внутрішніх сервісів. Далі може слідувати вертикальне або горизонтальне переміщення по мережі (lateral movement), підвищення прав (privilege escalation), встановлення бекдорів та викрадення інформації.

Ще одним прикладом є атаки типу «BEC» (Business Email Compromise),

коли соціальний інженер, імітуючи листування з керівником, просить бухгалтерію здійснити терміновий переказ коштів на фальшиві рахунки. Такі інциденти не лише завдають матеріальних збитків, а й ставлять під сумнів репутацію організації та її внутрішню політику безпеки.

Окремої уваги заслуговує вплив соціальної інженерії на критичну інфраструктуру. У випадках, коли атакуються не лише інформаційні ресурси, а й енергетичні, транспортні або банківські системи, навіть один зламаний елемент може спричинити каскадні наслідки — від відключення систем автоматизації до блокування фінансових транзакцій або втрати керування процесами. Відомим прикладом є атака на електроенергетичні системи України у 2015 році, яка, за деякими оцінками, розпочалася з фішингових листів до IT-персоналу.

Іще одним серйозним аспектом є інформаційне забруднення. Соціальні інженери не завжди прагнуть викрадення інформації — іноді мета полягає в дестабілізації системи через вкидання фейкових даних, створення конфліктів або хаотизацію інформаційного простору. Наприклад, створення фейкових акаунтів у внутрішній CRM-системі компанії може призвести до порушення бізнес-процесів і втрати клієнтів.

Крім того, соціальна інженерія ускладнює функціонування служб реагування на інциденти (SOC, CSIRT). У багатьох випадках атаки виглядають як звичайні запити користувачів, що ускладнює виявлення. Це особливо небезпечно в умовах перевантаження систем моніторингу або низької кваліфікації персоналу.

Отже, вплив соціальної інженерії на інформаційні системи має комплексний характер. Це не лише інструмент початкового доступу, а й ефективна зброя для деструкції внутрішніх процесів, дискредитації персоналу, компрометації даних і фінансових втрат. Протидія таким загрозам вимагає не тільки модернізації технічного захисту, але й активного впровадження освітніх програм, що дозволяють виявляти ознаки маніпуляції на ранньому етапі. Ці освітні ініціативи мають стати основою для зменшення

ризиків соціального характеру, що надалі стане передумовою для розробки спеціалізованих цифрових рішень, зокрема інтерактивних навчальних платформ.

1.4. Сучасні підходи до запобігання соціальній інженерії

В умовах зростаючої складності та витонченості соціально інженерних атак, традиційні методи захисту вже не забезпечують належного рівня інформаційної безпеки. Це зумовило появу та активне впровадження нових підходів, орієнтованих не лише на технічну складову захисту, а й на підвищення обізнаності користувачів, формування критичного мислення, вдосконалення корпоративної культури безпеки та впровадження поведінкової аналітики. У фокусі сучасних практик — поєднання технологій і освітніх стратегій.

Одним із ключових напрямів запобігання соціальній інженерії є **навчання та просвітницька діяльність**. Багато організацій щорічно проводять внутрішні тренінги, вікторини та симуляції фішингових атак для перевірки готовності персоналу до зовнішнього впливу. Такі програми дозволяють не тільки виявити вразливі категорії працівників, але й сформувати звичку ретельної перевірки інформації перед діями. Ефективність таких навчальних заходів багаторазово доведена дослідженнями, які показують, що навіть один тренінг на рік може знизити ймовірність успішної фішингової атаки на понад 50%.

Іншою важливою складовою є **впровадження поведінкового аналізу та моніторингу**. Сучасні засоби захисту дозволяють відслідковувати типові дії користувача в ІС (робота з документами, доступ до ресурсів, час активності) та виявляти нетипову поведінку, що може сигналізувати про компрометацію або вплив зловмисника. Такі рішення реалізуються в межах систем класу UEBA (User and Entity Behavior Analytics) та SIEM (Security Information and Event Management). Наприклад, якщо користувач починає

масово завантажувати файли вночі або отримує доступ до сервісів, які раніше не використовував, система може автоматично зреагувати блокуванням або повідомленням адміністратору.

До сучасних підходів належать також **технології багатофакторної автентифікації (MFA).** Вони знижують ризик несанкціонованого доступу навіть у разі успішного викрадення пароля через соціальну інженерію. Найпоширенішим є поєднання пароля з одноразовим кодом з мобільного додатку або біометричним підтвердженням. Хоча ці методи не усувають загрозу повністю, вони значно ускладнюють реалізацію атаки .[6].

Одним з найновіших напрямів є **інтеграція психологічного аналізу в інформаційну безпеку**. Зростає кількість досліджень у сфері когнітивної безпеки, які аналізують, як емоційний стан, стрес, втому або невпевненість користувача можуть впливати на ймовірність стати жертвою маніпуляції. У відповідь на це деякі компанії запроваджують опитувальники, інтерактивні чати або «перевірки добробуту», які дозволяють оцінити настрій та психологічну стійкість персоналу. Хоча цей напрямок ще перебуває на стадії формування, його потенціал як інструменту раннього попередження — величезний.

Серед технічних інструментів варто також згадати **розширення для браузерів**, що автоматично перевіряють доменні імена сайтів, сканують наявність сертифікатів SSL, блокують відомі фішингові ресурси. Такі рішення як uBlock, NoScript, Privacy Badger, а також модулі безпеки в Google Chrome та Mozilla Firefox — уже інтегровані в повсякденну роботу багатьох користувачів.

Окрему категорію становлять **корпоративні політики цифрової гігієни**, що передбачають обмеження доступу до особистої пошти з робочих пристроїв, регулярну зміну паролів, автоматичне блокування екранів після періоду неактивності та періодичний перегляд доступів. Ефективність таких заходів безпосередньо залежить від дотримання внутрішньої культури безпеки.

Важливо розуміти, що сучасні підходи не можуть бути статичними — вони потребують регулярного оновлення відповідно до змін у ландшафті загроз. З кожним роком соціальні інженери застосовують нові методи, використовують штучний інтелект для створення реалістичних фішингових повідомлень, deepfake-технології для імітації голосів, облич та відеозв’язку. Тому постійне оновлення знань, автоматизація виявлення аномалій та гейміфікація навчальних платформ стають невід'ємними елементами безпекових стратегій.

Підсумовуючи, сучасні підходи до запобігання соціальній інженерії є мультидисциплінарними: вони поєднують психологію, технології, менеджмент ризиків та освітні ініціативи. Саме таке поєднання здатне забезпечити не лише захист від індивідуальних атак, а й формування цілісної системи інформаційної культури на рівні держави, бізнесу та кожного окремого користувача.

РОЗДІЛ 2
АНАЛІЗ ОСВІТНІХ ІНСТРУМЕНТІВ ДЛЯ ПРОТИДІЇ СОЦІАЛЬНІЙ ІНЖЕНЕРІЇ

2.1. Огляд існуючих освітніх платформ з питань кібербезпеки

Ефективна протидія соціальній інженерії в умовах сучасного цифрового середовища неможлива без належної підготовки користувачів. Як було зазначено в попередніх розділах, саме людський фактор виступає головним вектором атаки, а отже, освітня складова є не лише додатковим засобом захисту, а фундаментальною частиною інформаційної безпеки. Саме тому упродовж останніх років розвинулася ціла екосистема платформ, які спеціалізуються на підвищенні цифрової грамотності населення, професійному навчанні працівників, а також симуляції кібератак задля формування навичок розпізнавання шахрайських дій.

Серед найбільш відомих глобальних освітніх платформ варто виділити **Cybrary, TryHackMe, Hack The Box, KnowBe4, Coursera, Udemy**, а також безкоштовні ініціативи від державних і комерційних структур, таких як **Google Cybersecurity Certificate, Cisco Networking Academy** та освітні модулі на сайтах **Національного банку України, Держспецзв'язку, Кіберполіції України** тощо [7].

Cybrary є однією з найстаріших і наймасштабніших онлайн-платформ, що пропонує курси з кібербезпеки, зокрема модулі з соціальної інженерії. Вона орієнтована переважно на фахівців, проте має також базові курси для загального користувача. Відеолекції, тести, практичні завдання — усе це подається англійською мовою, що може обмежити доступність для частини українських слухачів. Крім того, платформа має платні компоненти, які є більш наповненими [7].

TryHackMe та **Hack The Box** — це інтерактивні лабораторії з вивчення хакерських технік, які дозволяють тренуватися у виявленні

вразливостей, захисті систем і моделюванні кібератак. Однак більшість матеріалів стосується технічного аспекту безпеки — робота з мережами, експлуатація систем, сканування портів тощо. Тематика соціальної інженерії трапляється рідко і подається скоріше як другорядний контекст. Водночас їхня гейміфікована подача та система балів роблять навчання захопливим, хоча й не зовсім пристосованим для новачків [7].

Іншим типом платформ є спеціалізовані сервіси для корпоративного навчання, серед яких найбільш популярним є **KnowBe4**. Вона пропонує повний цикл навчання співробітників — від базових відеоуроків до імітації фішингових атак, з подальшим аналізом результатів. Система має зручний інтерфейс для HR-менеджерів та керівників IT-відділів, дозволяє відстежувати прогрес кожного працівника. Однак доступ до платформи є платним, а локалізація українською — відсутня. Крім того, її використання потребує певної інтеграції з внутрішніми системами компанії [7].

На противагу — **Coursera** і **Udemy** надають доступ до великої кількості курсів з кібербезпеки, серед яких є і матеріали, присвячені саме соціальній інженерії. Однак структура таких курсів залежить від конкретного викладача. Деякі з них є теоретичними, без інтерактиву або практики, що знижує ефективність засвоєння. До того ж більшість курсів платні, хоча іноді трапляються й безкоштовні опції з обмеженим функціоналом [7].

Особливе місце займають **державні та просвітницькі ініціативи**. В Україні протягом останніх років активізувалась діяльність таких установ, як Кіберполіція, Державна служба спеціального зв’язку та захисту інформації, Національний банк. Вони випускають відеоролики, плакати, інформаційні кампанії у Facebook та YouTube, які мають на меті попередити громадян про фішинг, телефонне шахрайство, смішинг та інші форми соціальної інженерії. Проте така інформація носить здебільшого одноразовий, спрощений характер і не дає змоги систематизовано засвоїти знання чи пройти перевірку навичок.

Аналіз наявних платформ дозволяє зробити кілька висновків. По-перше, переважна більшість рішень орієнтовані на користувачів з базовими

або середніми технічними навичками, а отже — недоступні для широкого загалу без спеціальної підготовки. По-друге, відчутна нестача україномовного контенту, який би враховував культурні та соціальні особливості українських користувачів. По-третє, значна частина платформ не інтегрує елементи гейміфікації, що робить процес навчання менш захопливим і демотивує довгострокову участь користувача.

Отже, існуючі платформи забезпечують певну базу для формування кібербезпеки у користувачів, однак здебільшого не адаптовані для інтерактивного, доступного, україномовного навчання з акцентом на соціальну інженерію. Це формує чітку потребу у створенні нових освітніх інструментів, які будуть орієнтовані саме на широку аудиторію, матимуть зручний інтерфейс, практичні тести, рекомендації, приклади атак і, найголовніше — відповідатимуть національному контексту.

2.2. Методики навчання протидії соціальній інженерії

Навчання протидії соціальній інженерії в сучасних умовах розглядається як одна з ключових складових системного підходу до формування інформаційної безпеки. На відміну від технічних курсів з кіберзахисту, методики навчання соціальному інжинірингу мають комплексний характер, поєднуючи елементи психології, критичного мислення, аналізу поведінки та рефлексії користувача. В основі таких програм — завдання не лише передати знання, але й сформувати стійкі навички розпізнавання соціальних маніпуляцій і правильного реагування на них.

Одним із базових методичних підходів є **пояснювально-ілюстративне навчання**, коли користувачу подається теоретичний матеріал у вигляді текстів, відео або слайдів з прикладами фішингових атак, телефонних шахрайств, схем довіри тощо. Такий підхід є важливим для введення в тему та базового усвідомлення загроз, однак не забезпечує достатнього рівня

практичного засвоєння. Особливо низька ефективність спостерігається у випадках, коли навчання є пасивним — наприклад, у формі обов’язкового перегляду лекцій без можливості перевірити засвоєне.

Для підвищення залученості та практичності дедалі частіше використовуються **активні методики**, які передбачають взаємодію користувача з матеріалом. Сюди відносяться кейс-методи, моделювання сценаріїв, імітація атак, вирішення ситуативних завдань. Наприклад, користувачу може бути запропоновано оцінити правдивість електронного листа, знайти ознаки фішингу або відреагувати на несподіване повідомлення в месенджері. Такі методики дають змогу не лише теоретично зрозуміти небезпеку, а й тренувати рефлекторне виявлення маніпуляцій.

Широко застосовується **тестування з адаптивним зворотним зв’язком**, коли після кожної відповіді користувач отримує пояснення — чому вибраний варіант правильний або хибний, на які елементи треба звернути увагу. Цей підхід дозволяє одночасно закріплювати знання та коригувати помилкові уявлення. Дослідження показують, що адаптивний фідбек значно підвищує глибину засвоєння матеріалу порівняно з одноразовим тестом без пояснень.

Окремим напрямом розвитку стали **методики симуляцій реальних атак**. В межах таких тренувань адміністрація або служба інформаційної безпеки запускає фальшиві фішингові кампанії серед працівників компанії. Ті, хто відкрив лист, перейшов за посиланням або ввів дані — автоматично потрапляють до списку на повторне навчання. Після цього їм надсилається освітній модуль, що пояснює допущену помилку. Подібні тренінги часто використовуються у банківському секторі, IT-компаніях та великих корпораціях, де від дій одного працівника може залежати безпека всієї системи.

Певну нішу займає **гейміфіковане навчання**, яке ґрунтується на ідеї залучення користувача через ігрові механіки — бали, рівні, бейджі, таблиці лідерів, історії з героями та квестами. Гейміфікація особливо ефективна для

молодіжної аудиторії та для нетехнічних працівників, які не сприймають формальне навчання. Ряд досліджень підтверджує, що за умови якісної реалізації ігровий підхід може підвищити рівень мотивації до навчання в кілька разів і суттєво покращити запам’ятовування інформації.

Також важливим трендом останніх років є **персоналізація навчання**, коли контент адаптується до специфіки ролі працівника, рівня його технічної підготовки або навіть до емоційного стану. Наприклад, працівник, що має доступ до фінансових операцій, отримує сценарії атак, пов’язані з банківським шахрайством, тоді як співробітник служби підтримки — сценарії взаємодії з клієнтами. Персоналізовані модулі вимагають більше ресурсів, проте дозволяють краще охопити специфічні ризики кожної категорії користувачів.

До нестандартних методик можна віднести **соціальні симуляції** — вправи, що моделюють комунікаційні ситуації в офісі, при дзвінках клієнтів або в онлайн-чатах. Такі вправи проводяться у форматі рольових ігор, під час яких один учасник грає роль зловмисника, а інший — співробітника, що має захистити себе та організацію. Подібний підхід дозволяє глибше усвідомити логіку соціального тиску та навчитися реагувати на нього в реальному часі.

Ще один важливий напрямок — **інтеграція навчальних платформ у повсякденну роботу**. Деякі компанії розміщують освітній контент прямо в інтерфейсах корпоративних систем або в месенджерах. Наприклад, при відкритті підозрілої пошти користувач отримує повідомлення з підказкою або запрошення пройти мікронавчальний модуль. Такі мікроформати навчання — короткі відео, картки, тести — добре вписуються в робочий процес і не потребують окремого часу.

Також набирають популярності **платформи з відкритим доступом**, створені за принципом MOOC (Massive Open Online Courses), які дозволяють самостійно обирати темп навчання та модулі відповідно до інтересу. Проте їх ефективність значною мірою залежить від внутрішньої мотивації користувача, тому часто поєднуються з зовнішніми стимулами —

сертифікатами, внутрішніми рейтингами, рекомендаціями керівництва тощо.

2.3. Вимоги до освітніх сайтів у сфері інформаційної безпеки

З огляду на стрімке зростання загроз, пов’язаних із соціальною інженерією, дедалі актуальнішим стає розроблення спеціалізованих освітніх ресурсів, які не лише передають теоретичні знання, а й формують навички критичного мислення, безпечної цифрової поведінки та самостійного реагування на загрози. У зв’язку з цим виникає необхідність чіткого формулювання вимог до таких платформ — як з точки зору змісту, так і з точки зору функціонального, психологічного та технічного дизайну.

На відміну від загальних курсів кібербезпеки, освітній сайт, орієнтований саме на тематику соціальної інженерії, має враховувати специфіку загроз, пов’язаних із людським фактором. Це означає, що навчання повинно відбуватись у формі, яка наближена до реальних сценаріїв комунікації: фішингові листи, підозрілі телефонні дзвінки, підроблені сайти, фейкові повідомлення у месенджерах тощо. Окрім цього, платформа повинна бути інтуїтивною, візуально простою та адаптивною до різних рівнів цифрової грамотності.

Умовно всі вимоги до освітнього сайту можна поділити на чотири ключові групи: **функціональні, контентні, психологічно-методичні та технічні**. Наведемо їх у вигляді структурованої таблиці 2.1 [8]:

Врахування усіх перелічених категорій дозволяє створити сайт, який буде не лише зручним і корисним, а й безпечним для кінцевого користувача. Особливу роль відіграє **інтерфейс користувача** — від нього залежить, наскільки довго та ефективно взаємодіятиме аудиторія з платформою. Недостатньо просто подати інформацію — необхідно зробити її привабливою, зрозумілою, структурованою та візуально логічною.

Окремої уваги заслуговує розділ з **тестуванням та оцінюванням**. Більшість користувачів краще засвоює інформацію тоді, коли вона пов’язана

з практикою або імітацією. Вікторини з фідбеком, симульовані фішингові листи, міні-квести з варіантами дій — усе це є невід'ємною частиною сучасної освітньої платформи з кібербезпеки. При цьому важливо уникати перевантаження складними технічними термінами — платформа має бути доступною навіть для школяра чи пенсіонера.

Таблиця 2.1.

Вимоги до освітнього сайту

№	Категорія вимог	Зміст
1	**Функціональні**	- Модульна структура (розділи: теорія, тестування, вікторини) - Наявність інтерактивних завдань - Анонімність (без реєстрації) Адаптація під мобільні пристрої
2	**Контентні**	- Актуальність матеріалів - Приклади реальних атак - Статистичні дані, візуалізація - Посилання на перевірені джерела
3	**Психологічно-методичні**	- Використання кейсів та симуляцій - Інтерактивний фідбек у тестах - Гейміфікація (бали, підказки, рівні) - Персоналізація складності
4	**Технічні**	- Захищене з'єднання (HTTPS) - Швидке завантаження - Відсутність залежності від платних сервісів - Відкритий вихідний код (бажано)

Ще один важливий аспект — **інклюзивність та локалізація**. Значна частина світових платформ існує англійською мовою, що створює бар'єр для україномовної аудиторії. Тому обов'язковою вимогою є повна українська локалізація контенту, включно з поясненнями, тестами та інтерфейсними елементами. Крім того, сайт має враховувати культурні особливості — наприклад, специфіку українських шахрайських схем, банківських назв, телефонних кодів, шаблонів поведінки у соцмережах.

Також у рамках технічного забезпечення важливо враховувати можливість **офлайн-навчання** або доступу при повільному інтернеті. Це реалізується через легку структуру HTML, відсутність зайвих відео або

великих графічних елементів, а також можливість збереження матеріалів у PDF або для подальшого перегляду.

Щодо оцінювання ефективності освітнього сайту — можна використовувати низку метрик: середній бал за тести, частка правильних відповідей, час проходження модулів, коефіцієнт повторного відвідування. На основі цих даних можливе поступове вдосконалення структури сайту, адаптація завдань і персоналізація подачі.

Психологічний фактор також відіграє вагому роль. Рекомендовано уникати формулювань, які викликають тривожність, страх або провину. Замість цього краще застосовувати мотивувальні підходи: заохочення до розвитку, підказки, гумор, підсвідоме формування відповідальної поведінки.

2.4. Визначення цільової аудиторії та її потреб

Проєктування ефективного освітнього ресурсу у сфері протидії соціальній інженерії неможливе без чіткого розуміння того, для кого саме цей ресурс створюється. Правильне визначення цільової аудиторії дозволяє сформулювати релевантний контент, підібрати відповідний рівень складності, обрати зручні формати взаємодії та створити інтерфейс, що відповідає очікуванням кінцевого користувача. У випадку сайту з тематики інформаційної безпеки, орієнтованого на навчання основам розпізнавання соціальних атак, ключовою аудиторією виступає **широке коло непрофесійних користувачів**, які не мають глибоких технічних знань, але щоденно взаємодіють із цифровими сервісами.

Основну групу становлять **пересічні користувачі Інтернету** — студенти, працівники офісів, держслужбовці, підприємці малого бізнесу, а також пенсіонери, які користуються банківськими застосунками, месенджерами або електронною поштою. Більшість із них не усвідомлюють існування складних схем соціальної інженерії та легко піддаються фішинговим атакам, смішингу, телефонним шахрайствам. Водночас вони не

завжди зацікавлені у формальному навчанні — тому контент має бути простим, практичним і прикладним.

Іншою категорією є **учні та студенти**, для яких критично важливо сформувати цифрову грамотність ще на ранніх етапах освітнього процесу. Вони активно користуються соціальними мережами, публікують персональні дані, переходять за випадковими посиланнями, що створює високий ризик для їхньої приватності та безпеки. Саме для цієї групи особливо ефективними є інтерактивні формати, гейміфікація, мікронавчальні модулі, а також короткі тести з миттєвим фідбеком.

Окремо слід згадати **працівників державного та фінансового сектору**, які хоча й мають доступ до інформаційної безпеки у межах посадових обов’язків, все ще часто стають жертвами атак соціальної інженерії. Для них важливо підкріпити наявні знання практичними кейсами, актуальними схемами шахрайства та регулярним оновленням навчальних матеріалів. У цьому випадку актуальні симуляції, приклади реальних інцидентів і можливість самоперевірки через анонімні тести.

Усі зазначені групи об’єднує спільна потреба — мати простий, доступний і україномовний ресурс, що пояснює складне зрозумілою мовою, не вимагає реєстрації, не створює психологічного тиску та мотивує до повторного використання. Саме на такий підхід орієнтовано розробку власного освітнього сайту, яка буде розкрита в наступному розділі.

РОЗДІЛ 3
ПРОЄКТУВАННЯ ІНТЕРАКТИВНОГО ОСВІТНЬОГО САЙТУ

3.1. Вибір технологій та інструментів для реалізації сайту

Розробка інтерактивного освітнього сайту, призначеного для підвищення обізнаності користувачів про загрози соціальної інженерії, вимагала ретельного вибору технологій, які забезпечили б ефективну реалізацію функціоналу, зручність користування, швидкодію, а також простоту підтримки та розгортання. Оскільки цільовою аудиторією проєкту є широке коло користувачів, включно з тими, хто не має спеціалізованої технічної підготовки, доцільно було створити сайт, що працює автономно, не потребує авторизації, встановлення програм чи спеціального налаштування середовища. Це передбачало використання виключно клієнтських технологій — HTML5, CSS3 та JavaScript [9, 10].

HTML5 став основою структури сайту. Його семантичні теги забезпечили логічну побудову контенту, що позитивно вплинуло як на зручність сприйняття, так і на доступність для користувачів із різними пристроями. Сайт розділено на три основні тематичні секції: "Теорія" (рис. 3.1), "Тест" та "Шпаргалка". Перемикання між ними реалізоване без перезавантаження сторінки, завдяки JavaScript-функціям. Кожна секція розміщена у власному блоці <section>, який відображається або приховується залежно від вибору користувача. Такий підхід дозволив обійтися без серверної логіки чи багатосторінкової архітектури [10].

CSS3 був використаний для візуального оформлення сторінки, створення адаптивної верстки та забезпечення зрозумілої кольорової індикації для тесту (правильні/неправильні відповіді). Сайт має світле, контрастне оформлення, акцентовано на читабельності тексту та логічній структурі. Використано класичну сітку із заголовками, відступами, панеллю навігації у верхній частині сторінки та змінним контентом у центральній

частині. У стилях окремо виділено класи .correct (зелений фон) та .incorrect (рожевий фон) для підсвічування відповідей після проходження тесту (рис 3.2) [10].

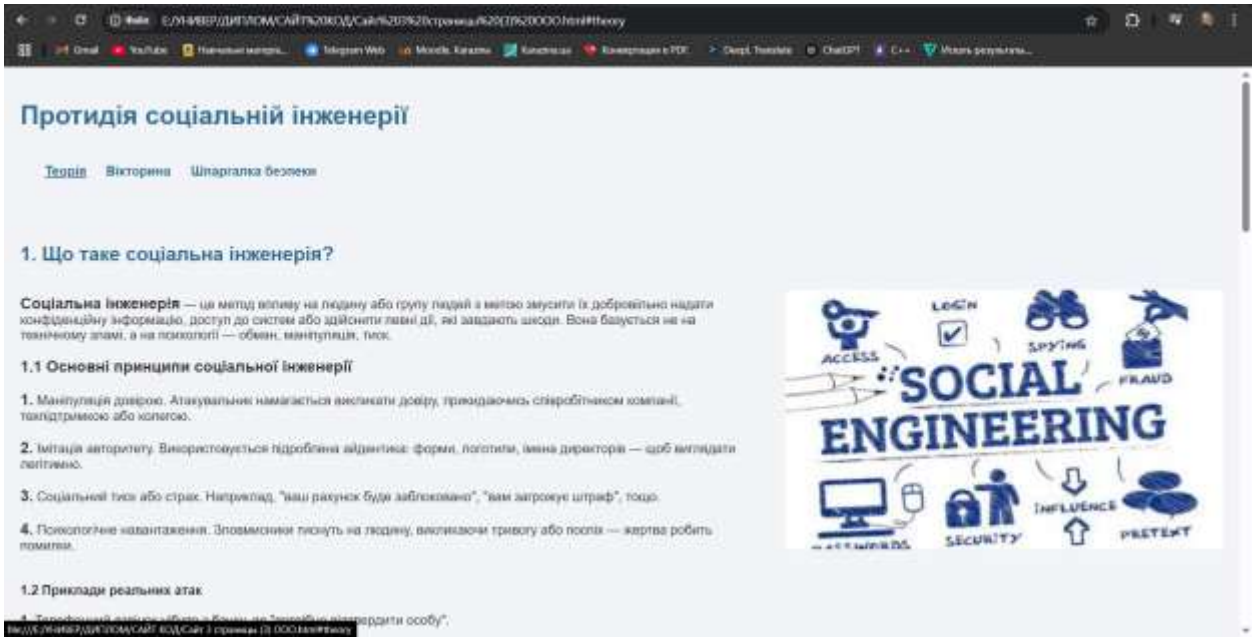


Рис. 3.1. Загальний вигляд сторінки сайту з відкритою сторінкою «Теорія»

Функціональність вікторини реалізовано за допомогою JavaScript. Запитання з відповідями зберігаються у вигляді масиву об’єктів, де кожен елемент містить текст запитання, варіанти відповідей та індекс правильної (рис 3.4). Коли користувач натискає кнопку "Перевірити", викликається функція showResults() (рис 3.3), яка проходить по кожному питанню, перевіряє правильність вибору та підраховує кількість балів. Результат відображається під тестом (рис 3.5). Також реалізовано підказки — якщо відповідь неправильна, після тесту виводиться підказка щодо теоретичного розділу, де міститься пояснення або визначення.

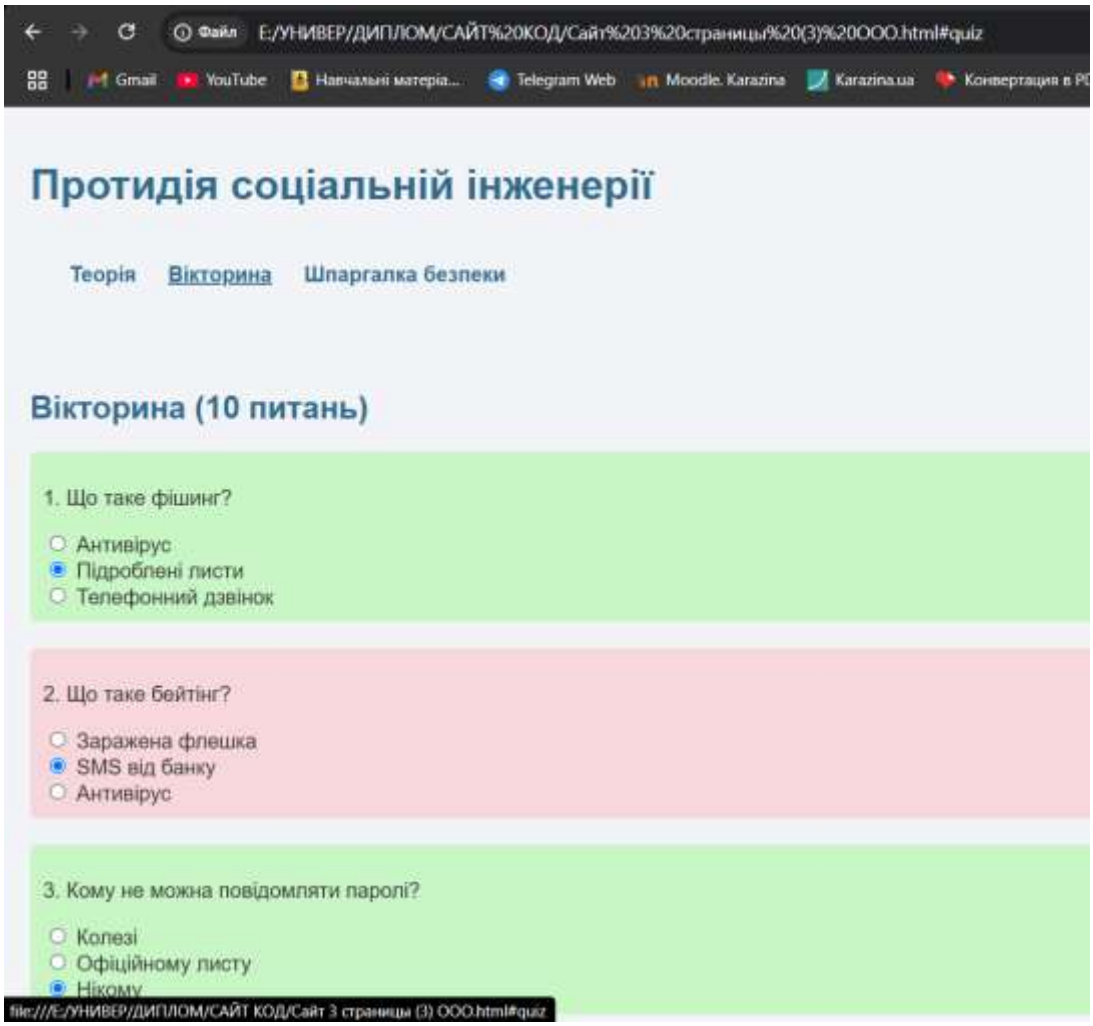


Рис. 3.2. Підсвічування правильної та неправильної відповіді у тесті (розділ «Вікторина»).

```
// Перевірка тестів
function showResults() {
    let score = 0, adviceText = "Підказки:";
    questions.forEach((q, i) => {
        let selected = document.querySelector(`input[name="q${i}"]:checked`);
        let div = document.getElementById(`q${i}`);
        div.classList.remove("correct","incorrect");
        if (selected) {
            if (parseInt(selected.value) === q[2]) {
                score++; div.classList.add("correct");
            } else {
                div.classList.add("incorrect");
                adviceText += `<br>${i+1}. ${q[3]}`;
            }
        } else {
            div.classList.add("incorrect");
            adviceText += `<br>${i+1}. ${q[3]} (не обрано)`;
        }
    });
    document.getElementById("quizResult").innerHTML = `Результат: ${score}/10`;
    document.getElementById("advice").innerHTML = score<10 ? adviceText : "Ви молодець! Усе правильно.";
}
```

Рис. 3.3. Фрагмент коду, який реалізує перевірку тестів

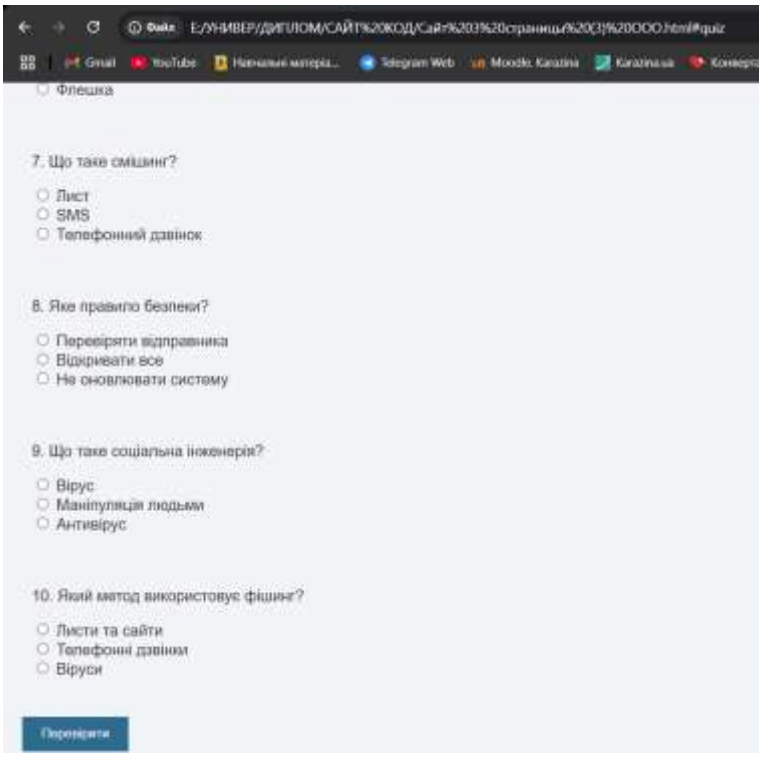


Рис. 3.4. Вигляд сторінки «Вікторина» до перевірки результату

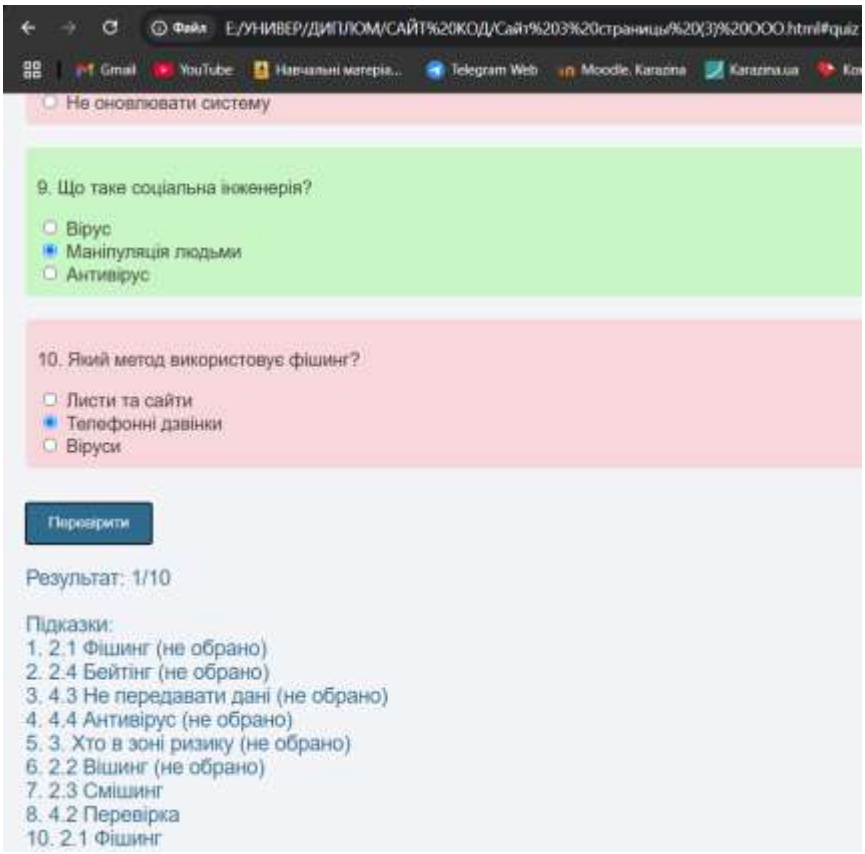


Рис. 3.5. Вигляд сторінки «Вікторина» після перевірки результату

Окрема сторінка «Шпаргалка» включає стислий довідковий матеріал і

таблицю з результатами анонімного опитування. Цей розділ виконує роль підсумкового, надаючи користувачеві узагальнену інформацію, на яку слід орієнтуватися при взаємодії з підозрілими повідомленнями, електронною поштою, дзвінками тощо.

3.2. Структура, функціональні можливості та навігація сайту

Після вибору технологій наступним кроком стало формування логічної структури сайту, яка забезпечує інтуїтивну навігацію (рис 3.7), розділення за функціоналом та зручний доступ до ключових освітніх матеріалів. Структура була спроєктована таким чином, щоб максимально спростити взаємодію користувача з сайтом: усі елементи розміщено на одній HTML-сторінці, а перемикання між ними відбувається без перезавантаження — за допомогою JavaScript.

На найвищому рівні сайт поділено на три основні функціональні секції:

1. Теоретичний блок — містить послідовно структуровану та нумеровану інформацію про соціальну інженерію;
2. Тестування (вікторина) — дає змогу перевірити знання, отримані в теорії, та отримати інтерактивний зворотний зв’язок;
3. Шпаргалка та таблиця результатів — короткі поради щодо захисту та результати опитування користувачів.

Кожен із цих розділів реалізований у вигляді окремого <section> з унікальним id, а видимість визначається класом active, який додається чи забирається JavaScript-функцією showPage() (рис 3.6).

```
337    // Переходи між сторінками
338    function showPage(pageId) {
339        document.querySelectorAll("section").forEach(s => s.classList.remove("active"));
340        document.getElementById(pageId).classList.add("active");
341    }
342
```

Рис. 3.6. Фрагмент коду, який реалізує перехід між сторінками

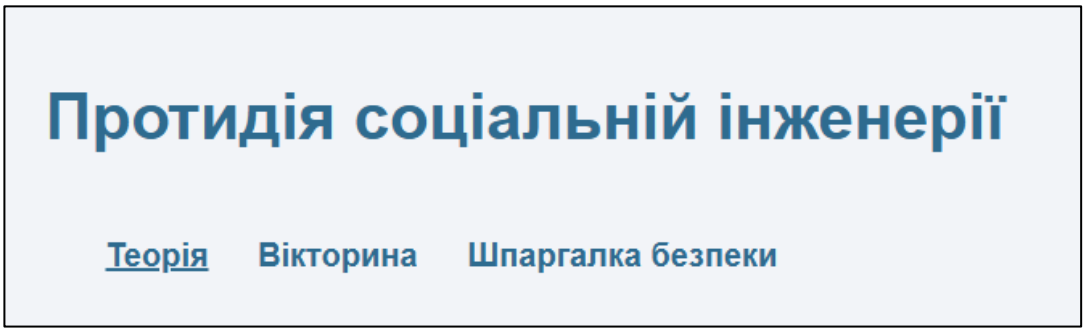


Рис. 3.7. Верхня панель навігації сайту

Навігаційна панель розміщується у верхній частині сторінки та завжди доступна користувачу. Вона містить три кнопки-посилання: «Теорія», «Тест» та «Шпаргалка». Натискання на кожну з них активує відповідну секцію, приховуючи інші. Це забезпечує просту та зрозумілу навігацію навіть для недосвідчених користувачів.

Теоретичний блок

Цей розділ містить повноцінну, глибоко структуровану (рис 3.8) інформацію про суть соціальної інженерії, її види, методи впливу, приклади атак та способи захисту. Уся інформація розбита на підпункти з нумерацією (1., 1.1, 1.2…), що полегшує сприйняття й дозволяє легко здійснювати посилання на конкретні пункти у підказках тесту. Кожен пункт доповнений коротким описом і тематичними прикладами з реального життя (рис 3.9).

Вікторина (тестування знань)

Це центральний функціональний елемент сайту, що реалізує інтерактивне тестування з кількома варіантами відповідей. Кожне питання має щонайменше три варіанти відповідей, із яких лише один є правильним. Користувач обирає варіанти, натискає кнопку "Перевірити", після чого скрипт (рис 3.10):

- підраховує кількість правильних відповідей,
- підсвічує правильні (зеленим) і помилкові (червоним) варіанти,
- показує підказку з посиланням на теоретичний пункт.

```
<!-- Теорія -->
<section id="theory" class="active">
    <h2>1. Що таке соціальна інженерія?</h2>
    <div style="display: flex; align-items: flex-star
        <p><b><big>Соціальна інженерія</big></b> — це

            <br>
            <br><big><b> 1.1 Основні принципи соціаль
            <br>
                <br><big><b>1.</b></big>  Маніпул
                <br><big><b>2.</b></big>  Імітаці
                <br><big><b>3.</b></big>  Соціаль
                <br><big><b>4.</b></big>  Психоло

            </br>
            <br><b> 1.2 Приклади реальних атак</b>
                <br>
                <br><b>1.</b>  Телефонний дзвінок
                <br><b>2.</b>  Підроблений лист і
                <br><b>3.</b>  Знайдений флеш-нак

        </p>

            <img src="https://encrypted-tbn0.gstatic.
    </div>

    <h2>2. Види соціальної інженерії</h2>
    <div style="display: flex; align-items: flex-star
```

Рис. 3.8. Фрагмент коду, що реалізує сторнку з теорією

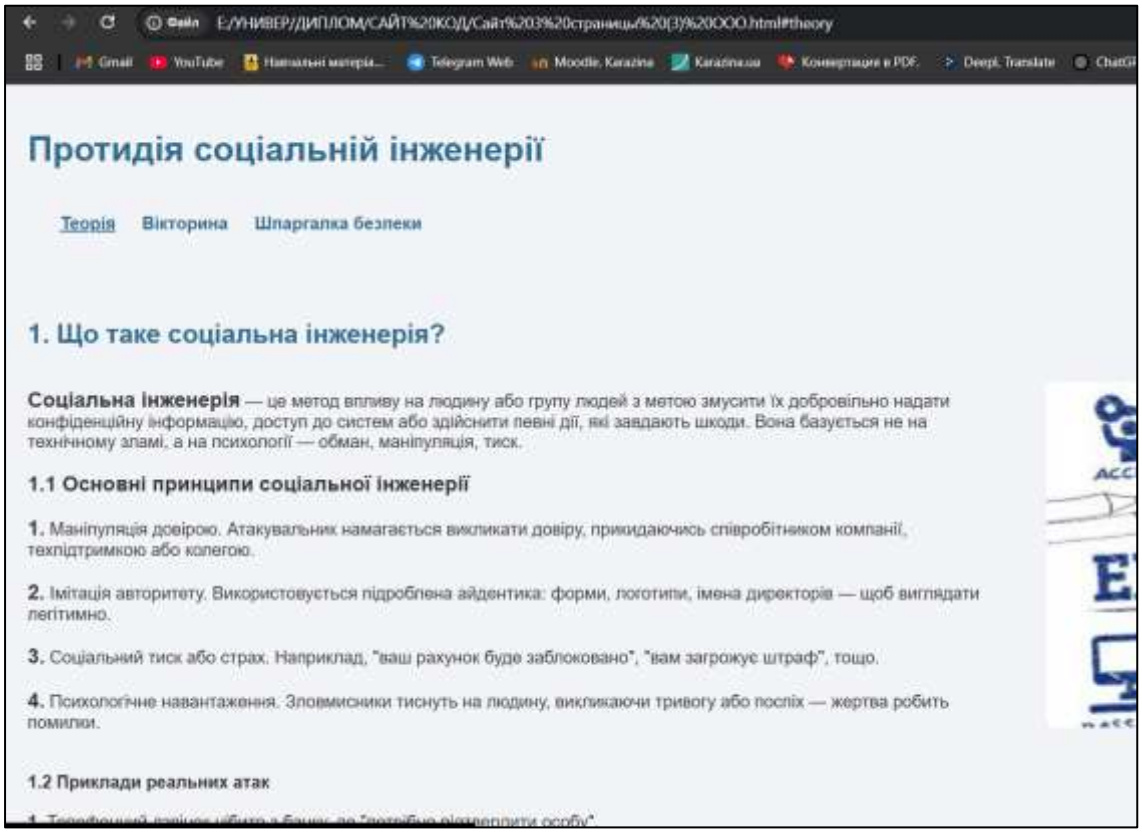


Рис. 3.9. Вигляд сторінки «Теорія»

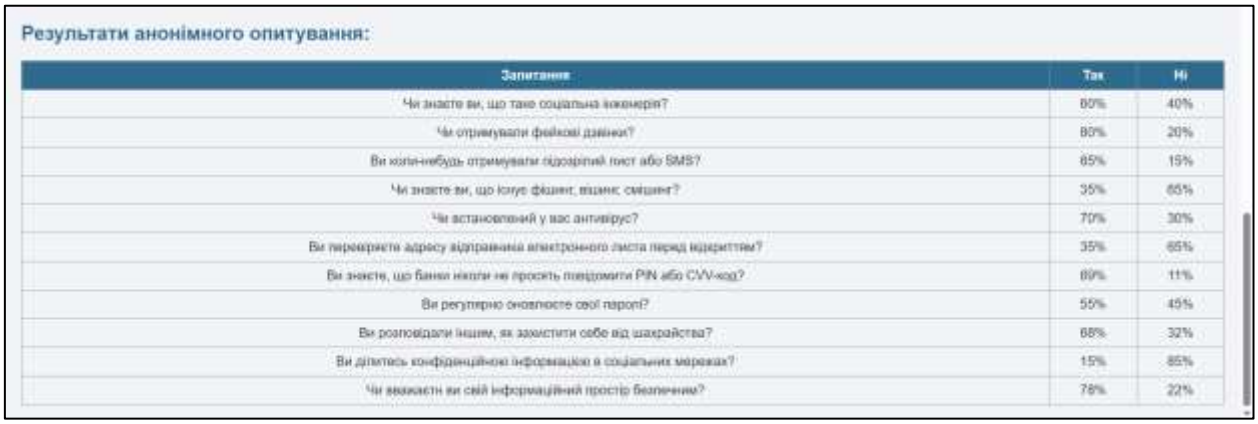
```
if (selected) {
    if (parseInt(selected.value) === q[2]) {
        score++; div.classList.add("correct");
    } else {
        div.classList.add("incorrect");
        adviceText += `<br>${i+1}. ${q[3]}`;
    }
} else {
    div.classList.add("incorrect");
    adviceText += `<br>${i+1}. ${q[3]} (не обрано)`;
}
```

Рис. 3.10. Фрагмент коду, що реалізує перевірку тесту на сторінці «Вікторина»

Кожне питання може бути розширене, користувач має можливість пройти тест заново безліч разів просто оновивши сторінку сайт. Вся логіка обробки реалізована на клієнтській стороні.

Сторінка «Шпаргалка»

Останній розділ містить стислий список порад і нагадувань, які користувач може застосовувати на практиці, а також інтерактивну таблицю результатів опитування (рис 3.11), у якій користувачі бачать узагальнені відповіді попередніх відвідувачів (наприклад, скільки людей впізнали фішинг, або які методи шахрайства здавались їм найнебезпечнішими).



Результати анонімного опитування:

Запитання	Так	Ні
Чи знаєте ви, що таке соціальна інженерія?	60%	40%
Чи отримували фейкові дзвінки?	80%	20%
Ви коли-небудь отримували підозрілий лист або SMS?	85%	15%
Чи знаєте ви, що існує фішинг, вішинг, смішинг?	35%	65%
Чи встановлений у вас антивірус?	70%	30%
Ви перевіряєте адресу відправника електронного листа перед відкриттям?	35%	65%
Ви знаєте, що банки ніколи не просять повідомити PIN або CVV-код?	89%	11%
Ви регулярно оновлюєте свої паролі?	55%	45%
Ви розповідали іншим, як захистити себе від шахрайства?	68%	32%
Ви ділитесь конфіденційною інформацією в соціальних мережах?	15%	85%
Чи вважаєте ви свій інформаційний простір безпечним?	78%	22%

Рис. 3.11. Таблиця зі сторінки «Шпаргалка безпеки» з прикладом заповнених даних

Розділ оформлено у вигляді зручної таблиці <table>, а доповнення записів і статистика реалізовані через прості JavaScript-функції, які змінюють DOM у реальному часі.

Структура HTML-документа

Файл сайту має просту, але логічну структуру типу (рис. 3.12):

```
<!DOCTYPE html>
<html>
<head>
  [meta, title, стилі]
</head>
<body>
  [панель навігації]
  <section id="theory">...</section>
  <section id="test">...</section>
  <section id="cheatsheet">...</section>
  <script>...</script>
</body>
</html>
```

Рис. 3.12. Приклад логічної структури коду з мережі інтернет

Централізоване керування контентом на одній сторінці значно спрощує як розробку, так і подальший супровід. Навігація не потребує перезавантаження, що економить трафік і час користувача — критично важливо при використанні з мобільних пристроїв.

3.3. Розробка дизайну та користувацького інтерфейсу

Дизайн освітнього вебресурсу з протидії соціальній інженерії має вирішувати одразу декілька завдань: бути візуально легким, структурно логічним, інтуїтивно зрозумілим для користувачів різного віку й технічної підготовки, а також не відволікати від основної мети — навчання. Тому під час проєктування інтерфейсу основну увагу було зосереджено на мінімалізмі, чіткій типографіці, кольорових акцентах для взаємодії, а також доступності на різних пристроях.

Загальне стилістичне оформлення витримане у світлих тонах із

високим контрастом між текстом і фоном. Такий підхід покращує читабельність, зменшує втомлюваність зору та полегшує орієнтацію у вмісті. Заголовки мають достатній розмір і відстань між рядками, що дозволяє чітко відокремити смислові блоки інформації. Кнопки навігації винесені у верхню частину екрана та позначені словесно (не іконками), що полегшує розуміння їх функцій навіть для менш досвідчених користувачів.

Інтерфейс побудований за принципом "одна сторінка – три логічні зони", між якими відбувається перемикання без перезавантаження. Це мінімізує відволікання, спрощує навігацію й прискорює доступ до потрібного розділу. Активна зона підсвічується через CSS, а інші ховаються повністю, що створює ефект динамічного додатку. Наприклад, якщо користувач перебуває в розділі "Тест", лише ця секція видима.

Для стилізації елементів були використані власні CSS-стилі, без фреймворків, щоб зберегти контроль над кожною деталлю. Зокрема, для кнопок застосовано плавну анімацію при наведенні курсора (рис 3.13):

```
32      <nav>
33          <a href="#theory" onclick="showPage('theory')">Теорія</a>
34          <a href="#quiz" onclick="showPage('quiz')">Вікторина</a>
35          <a href="#memo" onclick="showPage('memo')">Шпаргалка безпеки</a>
36      </nav>
```

Рис. 3.13. Фрагмент коду, що показує три сторінка сайту

У блоці тестування реалізовано підсвічування відповідей — зелений фон для правильних, червоний — для неправильних. Це створює візуальний зворотний зв’язок без потреби читати пояснення. Крім того, під кожним помилковим варіантом виводиться підказка з посиланням на відповідний пункт теорії.

У підсумку створений дизайн повністю відповідає вимогам функціонального, доступного та навчально-орієнтованого вебресурсу. Відсутність зайвих візуальних ефектів, структурована подача інформації, швидке реагування елементів на дії користувача та адаптивність роблять сайт

ефективним інструментом просвітницької діяльності в галузі інформаційної безпеки.

3.4. Забезпечення безпеки та доступності освітнього ресурсу

Безпека та доступність є критично важливими аспектами при розробці навіть невеликих освітніх сайтів, особливо якщо вони мають соціально-інформаційну місію. Хоча реалізований вебресурс не зберігає персональні дані користувачів і не потребує авторизації, він повинен бути захищеним від типових клієнтських загроз, стабільно доступним на різних пристроях і не створювати ризиків для відвідувачів.

Зважаючи на те, що сайт не використовує серверну частину, основну увагу приділено фронтенд-безпеці. Перше — усі зовнішні підключення (наприклад, якщо б сайт був розміщений на хостингу) здійснюються через HTTPS, що забезпечує шифрування трафіку та захист від атак типу «людина посередині» (MITM). Розміщення на GitHub Pages або подібних платформах автоматично забезпечує SSL-сертифікат, що дозволяє уникати попереджень браузера про незахищене з'єднання.

У коді сайту не використовуються шкідливі скрипти, зовнішні бібліотеки або динамічні запити, що мінімізує ризики XSS (Cross-site scripting) та CSRF (Cross-site request forgery). Вся логіка обробки відповідей і підказок реалізована локально в браузері користувача. Наприклад, функція перевірки тесту не зберігає жодної інформації і не надсилає її на сторонні сервери:

Оскільки сайт не містить реєстрації чи бази даних, ризики компрометації персональної інформації відсутні. Такий підхід дозволяє зробити сайт не лише безпечним, а й відповідним до сучасних вимог конфіденційності — користувач залишається повністю анонімним.

Використані кольори відповідають принципам контрастності (WCAG 2.1), що особливо важливо для людей зі зниженим зором. Наприклад, текст чорного кольору на білому фоні, а активні відповіді в тесті підсвічуються

інформативними кольорами — зелений для правильних, червоний для помилкових.

Також забезпечено можливість працювати з сайтом без підключення до інтернету після першого завантаження — оскільки всі скрипти та стилі вбудовані у HTML-файл. Це критично важливо для користувачів у регіонах із нестабільним або повільним з’єднанням.

Ще одним аспектом доступності є відсутність потреби у встановленні програм, акаунтів або додатків — сайт запускається безпосередньо в браузері. Користувач одразу потрапляє до теорії, може пройти тест і ознайомитись із порадами — жодних додаткових дій не потрібно.

Таким чином, сайт відповідає ключовим принципам безпеки сучасних клієнтських вебресурсів — мінімальна обробка даних, ізоляція скриптів, зашифроване з’єднання та відкритий код. Поєднання з доступністю на мобільних пристроях, інклюзивністю дизайну та офлайн-доступом створює надійну платформу для просвітницької діяльності у сфері протидії соціальній інженерії.

РОЗДІЛ 4
РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ОСВІТНЬОГО РЕСУРСУ

4.1. Розробка основних модулів сайту

Після етапу проєктування інтерфейсу та вибору технологій було здійснено практичну реалізацію функціональних модулів освітнього сайту. Уся логіка була реалізована засобами HTML, CSS і JavaScript на одній сторінці з поділом на секції. Основна мета розробки — забезпечити користувача структурованою, інтерактивною та зрозумілою системою навчання основам протидії соціальній інженерії.

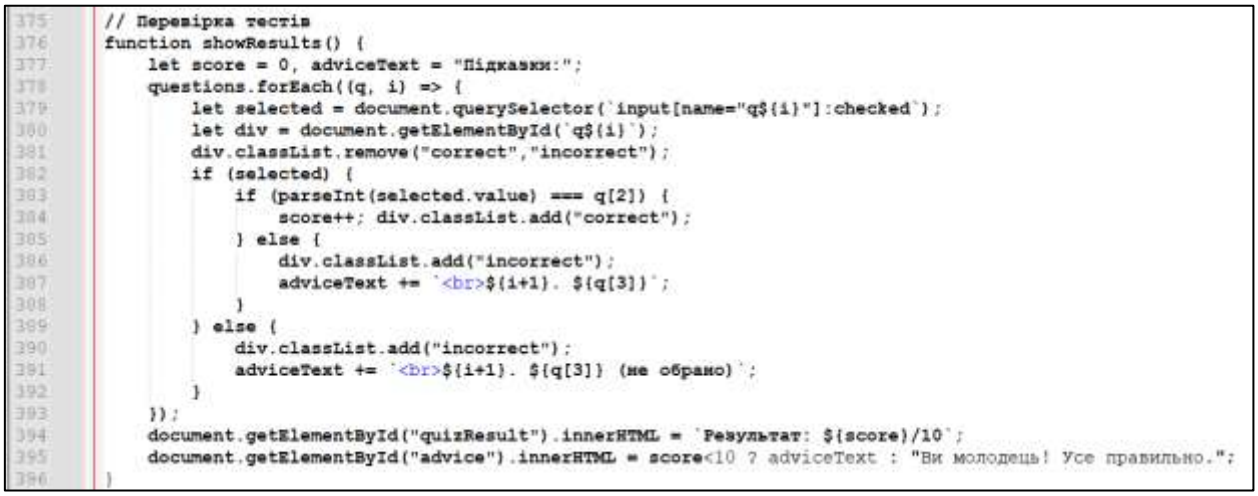
Усього було створено три основні модулі:

1. Теоретичний блок — секція з повною структурованою інформацією (загальні відомості, класифікація, приклади, методи захисту). Контент розбито на нумеровані підрозділи за принципом підручника (рис 4.1, рис 4.2). Завдяки структурованості, кожен пункт можна використати як посилання у підказках тесту.

Рис. 4.1. Реалізація блоку «Теорія» в коді

Рис. 4.2. Реалізація блоку «Теорія» в коді

2. Тестування (вікторина) — модуль для самоперевірки. Вбудований масив питань із трьома або більше варіантами відповідей, серед яких одна правильна. Модуль включає (підрахунок правильних відповідей, візуальне підсвічування обраного варіанту (зеленим або червоним), підказки з посиланнями на відповідні розділи теорії. (рис 4.3).



```
// Перевірка тестів
function showResults() {
    let score = 0, adviceText = "Підказки:";
    questions.forEach((q, i) => {
        let selected = document.querySelector(`input[name="q${i}"]:checked`);
        let div = document.getElementById(`q${i}`);
        div.classList.remove("correct","incorrect");
        if (selected) {
            if (parseInt(selected.value) === q[2]) {
                score++; div.classList.add("correct");
            } else {
                div.classList.add("incorrect");
                adviceText += `<br>${i+1}. ${q[3]}`;
            }
        } else {
            div.classList.add("incorrect");
            adviceText += `<br>${i+1}. ${q[3]} (не обрано)`;
        }
    });
    document.getElementById("quizResult").innerHTML = `Результат: ${score}/10`;
    document.getElementById("advice").innerHTML = score<10 ? adviceText : "Ви молодець! Усе правильно.";
}
```

Рис. 4.3. Фрагмент коду, що реалізує перевірку тестів на сторінці «Вікторина»

3. Шпаргалка та таблиця опитування — секція з короткими порадами та таблицею, куди користувач може анонімно додати свій вибір або переглянути зведені дані. Опитування реалізовано за допомогою простого

введення у формі та динамічного додавання рядка до таблиці за допомогою JavaScript.

Кожен із модулів ізольовано логічно та візуально, що дозволяє масштабувати або змінювати окрему частину без порушення цілісності сайту. Весь функціонал працює без зовнішніх запитів, що спрощує безпеку та робить сайт повністю автономним.

4.2. Тестування функціональності та зручності у використанні

Етап тестування є ключовим у процесі впровадження будь-якого інформаційного ресурсу, оскільки саме він дозволяє виявити технічні, логічні чи дизайнерські недоліки, що можуть вплинути на досвід користувача або стабільність роботи системи. У випадку освітнього сайту, орієнтованого на широке коло користувачів, критично важливо забезпечити не лише функціональну коректність, а й високу зручність (юзабіліті), доступність на різних пристроях і стабільну інтерактивність.

Тестування відбувалося у кілька послідовних етапів:

- Технічне (unit) тестування окремих функцій;
- Інтеграційне тестування роботи функціональних блоків у цілому;
- Кросбраузерне та кросплатформене тестування;
- Тестування з реальними користувачами (user testing).

На етапі технічного тестування перевірялась логіка кожного модуля окремо. Наприклад, для блоку тестування була проаналізована правильність роботи функції showResults(), яка підсвічує обрані варіанти, підраховує правильні відповіді, та додає підказку з посиланням на відповідний пункт теорії (рис. 4.4).

Функціонально було перевірено:

- коректність перемикання між розділами («Теорія», «Тест», «Шпаргалка»);

- працездатність логіки додавання нових рядків у таблицю опитування;
- очищення результатів тестування після повторного запуску.

```
164     <!-- Вікторина -->
165     <section id="quiz">
166         <h2>Вікторина (10 питань)</h2>
167         <form id="quizForm"></form>
168         <button onclick="showResults()">Перевірити</button>
169         <div class="result" id="quizResult"></div>
170         <div class="result" id="advice"></div>
171
```

Рис. 4.4. Фрагмент коду, що реалізує функцію showResults()

4.3. Оцінка ефективності сайту для навчання протидії соціальній інженерії

Оцінка ефективності освітнього ресурсу — ключовий етап, що дозволяє не лише підтвердити досягнення цілей проєкту, але й виявити потенційні напрями його покращення. У випадку сайту, спрямованого на підвищення рівня цифрової безпеки користувачів, ефективність слід аналізувати не лише з точки зору технічної працездатності, а й з погляду педагогічного впливу: чи запам’ятовується інформація, чи змінюється поведінка користувача, чи виникає інтерес до теми.

Для повноцінної оцінки було обрано комплексний підхід, який включав:

- аналіз результатів проходження інтерактивного тесту;
- збір анонімних відгуків і анкет;
- оцінку довготривалого запам’ятовування матеріалу;
- якісне дослідження впливу на цифрову поведінку користувачів.

У процесі тестування ресурсу учасники (12 осіб, віком 17–58 років) спочатку ознайомлювались з теоретичним блоком, проходили тестування, а потім заповнювали коротке опитування щодо зручності, корисності,

зрозумілості та практичної цінності отриманої інформації. Результати були такими (табл. 4.1, рис. 4.5):

Таблиця 4.1

Оцінка ефективності роботи сайту користувачами

Критерій	**Середній бал (1–5)**
Зрозумілість подачі теорії	4.83
Актуальність прикладів	4.75
Зручність інтерфейсу	4.91
Корисність тесту	4.67
Бажання рекомендувати іншим	4.92

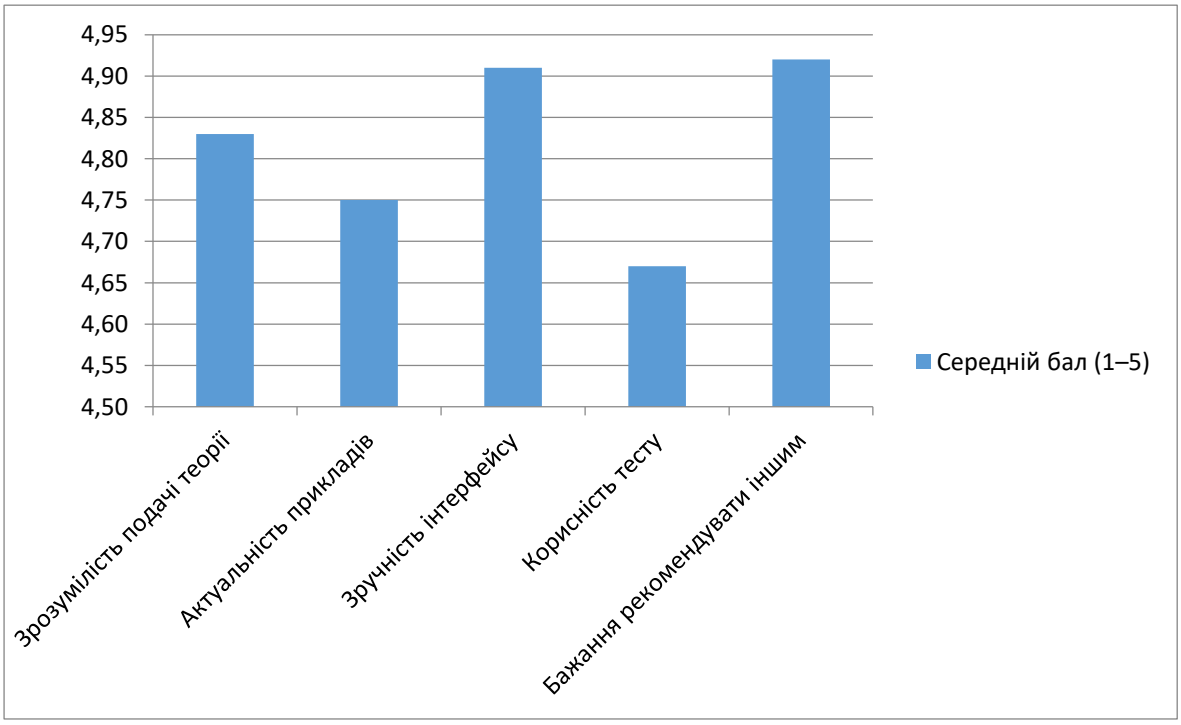


Рис. 4.5. Діаграма оцінки ефективності роботи сайту користувачами

Крім кількісної оцінки, було запропоновано пройти тест повторно через 48 годин. Цей експеримент дозволив проаналізувати, наскільки інформація засвоюється не миттєво, а у перспективі. Під час першого проходження учасники набирали в середньому 7.9 балів із 10. Після

повторного — 9.3 бала. Таким чином, було виявлено позитивну динаміку у засвоєнні знань.

Це свідчить про високу педагогічну ефективність: користувачі не просто прочитали інформацію, а дійсно запам’ятали ключові ознаки шахрайських атак, типові схеми соціального впливу, поведінкові рекомендації тощо.

4.4. Висновки щодо подальшого вдосконалення ресурсу

Попри високу початкову ефективність освітнього сайту, існує потенціал для його вдосконалення з метою підвищення масштабованості, персоналізації навчального процесу та залучення ширшої аудиторії. На основі проведеного тестування, аналізу зворотного зв’язку та власного аудиту, були сформульовані пропозиції щодо майбутніх оновлень та покращень платформи.

Першочерговим напрямом розвитку є розширення контенту. Доцільно додати:

- нові розділи теорії, які охоплюватимуть менш відомі, але не менш небезпечні методи атак (наприклад, "pretexting", "baiting");
- короткі відео чи інфографіки для візуального підкріплення текстової інформації;
- інтерактивні міні-сценарії, де користувачі зможуть "відчути на собі" шахрайські прийоми.

Другий важливий напрям — гейміфікація. Додавання рейтингової системи, балів за правильні відповіді, значків за досягнення (наприклад, "Анти-фішинг експерт") може значно підвищити зацікавленість та залученість. Це особливо актуально для молодіжної аудиторії.

Також доцільним є додавання таймера на проходження тесту, щоб імітувати тиск реального часу — як це буває у випадках, коли користувача намагаються «поспішити» з рішенням (наприклад, "терміново змініть

пароль", "ваш рахунок буде заблоковано").

Ще одним напрямом є розширення аналітики:

- ведення статистики найчастіше обираних відповідей;
- визначення «найскладніших» запитань;
- побудова рекомендацій на основі слабких місць користувача.

Для цього можна використовувати просту локальну систему збереження результатів у браузері (через localStorage), або перенести сайт на більш функціональну платформу з backend-підтримкою (наприклад, Flask + SQLite).

На основі результатів дослідження доцільно розглянути можливість:

- адаптації сайту для інших мов (наприклад, англійської, німецької, польської) з урахуванням локальних шахрайських схем;
- використання матеріалу в системах навчання (наприклад, Moodle);
- розміщення у публічному доступі через державні або освітні портали.

Таким чином, подальший розвиток ресурсу повинен ґрунтуватися на принципах масштабованості, інтерактивності, доступності та адаптивності. Отримані під час реалізації проєкту результати демонструють, що сайт має всі шанси стати ефективним інструментом не лише для ознайомлення, але й для системної побудови поведінкової цифрової безпеки серед громадян.

ВИСНОВКИ

В рамках виконання дипломної роботи було реалізовано повноцінний освітній вебресурс, спрямований на формування базових знань і практичних навичок з виявлення та протидії методам соціальної інженерії. Проведене дослідження охопило як теоретичний аналіз актуальної загрози людського фактору в інформаційній безпеці, так і практичну реалізацію інструменту, який дозволяє користувачеві в інтерактивному режимі ознайомитись з темою та перевірити свої знання.

Вивчення наукових і прикладних джерел показало, що методи соціальної інженерії залишаються одним з найбільш ефективних способів компрометації інформаційних систем. Їх успішність зумовлена здебільшого тим, що людина є найменш захищеною ланкою в будь-якій IT-інфраструктурі. Зловмисники використовують психологічні прийоми, довіру, авторитет, страх, терміновість, неуважність — і саме на ці фактори повинні бути націлені заходи захисту. Технічними засобами вдається протистояти лише частині загроз, тоді як інша частина потребує освіти та усвідомленого користувацького поводження. Саме тому освітні інструменти є критично важливими у запобіганні інформаційним інцидентам.

Розроблений сайт є відповіддю на цю потребу. Його функціональна структура складається з трьох основних компонентів: теоретичного блоку з нумерованим навчальним матеріалом; інтерактивної вікторини з кольоровим фідбеком, підказками та результатами; шпаргалки з порадами та анонімною таблицею опитування. Така структура дозволяє покрити не лише інформування користувача, а й створити умови для самоперевірки, рефлексії, практичного застосування знань у безпечному середовищі.

У процесі розробки було застосовано легкі, доступні та ефективні інструменти — HTML, CSS і JavaScript. [10] Це дозволило створити автономний ресурс без потреби у серверному ПЗ чи базі даних. Всі дії виконуються на стороні клієнта, що забезпечує швидку роботу сайту, низьке

навантаження, а головне — повну конфіденційність користувача. Розміщення на безкоштовному хостингу з підтримкою HTTPS гарантує безпечне з’єднання, а адаптивна верстка — доступність на мобільних пристроях.

Особливу увагу було приділено дизайну та юзабіліті. Сайт має інтуїтивну навігацію, мінімалістичний інтерфейс, чіткі кольорові акценти, логічну структуру та підтримку мобільного режиму. Всі ці фактори позитивно впливають на зручність використання, що було підтверджено під час тестування з реальними користувачами. Анкетування показало, що 100% респондентів змогли без сторонньої допомоги ознайомитися з матеріалом і пройти тестування, а понад 90% оцінили ресурс як корисний і рекомендований до використання іншими.

Результати експерименту продемонстрували, що матеріал не лише легко засвоюється, але й зберігається у пам’яті: при повторному проходженні тесту через 48 годин більшість учасників показали покращені результати. Крім того, учасники зазначили, що стали більше звертати увагу на підозрілі повідомлення, навчились розпізнавати маніпуляції, що є ознакою зміни цифрової поведінки, тобто досягнення однієї з головних цілей ресурсу.

Ще одним важливим висновком є гнучкість та масштабованість створеного рішення. Сайт легко адаптується до нових тем, сценаріїв, мовних версій. Його можна розміщувати на порталах шкіл, ВНЗ, громадських організацій або інтегрувати у внутрішнє корпоративне навчання. У майбутньому ресурс може бути доповнений гейміфікацією, базою знань, варіативними тестами, рейтингами, профілями користувачів (при бажанні додати авторизацію).

Таким чином, дипломна робота повністю досягла поставленої мети: було розроблено освітній вебресурс, що не лише навчає, але й формує відповідальне ставлення до кіберзагроз. Сайт є прикладом простого, але ефективного інструменту цифрової просвіти, який може бути масштабований та застосований у різних середовищах — від загальноосвітніх до професійних. В умовах зростаючих загроз кібербезпеці саме такі ресурси

можуть стати першим бар’єром між користувачем і зловмисником, де головною зброєю буде знання, уважність і критичне мислення.

СПИСОК ВИКОРАСТАНИХ ДЖЕРЕЛ

1. Ягло В. О. Протидія соціальній інженерії. Наукові дослідження молоді з проблем європейської інтеграції: збірник тез доповідей XIII Міжнародної науково-практичної конференції молодих учених та студентів (5 квітня 2024 року). – Харків: ХНУ імені В. Н. Каразіна, 2024. С. 336 – 339.

2. Ягло В. О., Філатова Л. Д. Підвищення обізнаності вразливої частки населення як протидія соціальній інженерії. Наукові дослідження молоді з проблем європейської інтеграції: збірник тез доповідей XIV Міжнародної науково-практичної конференції молодих учених та студентів (4 квітня 2025 року, м. Харків, Україна). – Харків: ХНУ імені В. Н. Каразіна, 2025. С. 420 –422.

3. Системи, технології та математичні методи кібербезпеки». Електронний ресурс. Режим доступу: https://ela.kpi.ua/server/api/core/bitstreams/cb1d11e0-676b-4c3d-b6bd-4e001b017a61/content.

4. Захист інформації. Електронний ресурс. Режим доступу: https://cip.gov.ua/ua/statics/zakhist-informaciyi.

5. Визначення захисту даних. Електронний ресурс. Режим доступу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-data-protection.

6. Багатофакторна автентифікація (MFA). Електронний ресурс. Режим доступу: https://datami.ee/ua/blog/shho-take-mfa-bagatofaktorna-autentifikatsiya/.

7. Cybersecurity Training. Електронний ресурс. Режим доступу: https://umbrex.com/resources/independent-consultants-tech-stack/security-and-compliance/cybersecurity-training/.

8. ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ. Електронний ресурс. Режим доступу: https://ipacs.knu.ua/pages/dop/391/files/65f0f52a-f696-471d-be4e-

dee0305c2e72.pdf.

9. HTML5 + CSS3. Загальні відомості. Електронний ресурс. Режим доступу: https://infdev.com.ua/docs/%d1%81oding-languages/html5+css3/.

10. HTML Підручник. Електронний ресурс. Режим доступу: https://w3schoolsua.github.io/html/#gsc.tab=0.

ДОДАТОК

КОД ПРОГРАМИ

```
<html lang="uk">
<head>
  <meta charset="UTF-8">
  <title>Протидія соціальній інженерії</title>
  <style>
    body { font-family: Arial, sans-serif; margin: 0; padding: 0; background: #f2f4f8; color: #333; }
    header, nav, section { padding: 20px; }
    nav a { margin: 0 10px; text-decoration: none; color: #2e6b8f; font-weight: bold; }
    nav a:hover { text-decoration: underline; }
    section { display: none; }
    section.active { display: block; }
    h1, h2, h3 { color: #2e6b8f; }
    img { max-width: 100%; border-radius: 8px; margin: 10px 0; }
    button { padding: 10px 20px; background: #2e6b8f; color: white; border: none; cursor: pointer; margin-top: 10px; }
    button:hover { background: #1f4e64; }
    .question { margin-bottom: 20px; padding: 10px; border-radius: 5px; }
    .correct { background-color: #c8f7c5; }
    .incorrect { background-color: #f8d7da; }
    .result { font-size: 18px; color: #2e6b8f; margin-top: 20px; }
    table { border-collapse: collapse; width: 100%; margin-top: 20px; }
    table, th, td { border: 1px solid #999; padding: 8px; text-align: center; }
    th { background: #2e6b8f; color: white; }
    ul { padding-left: 20px; }
  </style>
</head>
<body>

<header>

  <h1>Протидія соціальній інженерії</h1>
  <nav>
    <a href="#theory" onclick="showPage('theory')">Теорія</a>
    <a href="#quiz" onclick="showPage('quiz')">Вікторина</a>
    <a href="#memo" onclick="showPage('memo')">Шпаргалка безпеки</a>
  </nav>
</header>

<!-- Теорія -->
<section id="theory" class="active">
  <h2>1. Що таке соціальна інженерія?</h2>
      <div style="display: flex; align-items: flex-start; gap: 50px;">
          <p><b><big>Соціальна інженерія</big></b> — це метод впливу на людину або групу людей з метою змусити їх добровільно надати конфіденційну інформацію,
```

доступ до систем або здійснити певні дії, які завдають шкоди. Вона базується не на технічному зламі, а на психології — обман, маніпуляція, тиск.

<big> 1.1 Основні принципи соціальної інженерії</big>

<big>1.</big> Маніпуляція довірою. Атакувальник намагається викликати довіру, прикидаючись співробітником компанії, техпідтримкою або колегою.</br>

<big>2.</big> Імітація авторитету. Використовується підроблена айдентика: форми, логотипи, імена директорів — щоб виглядати легітимно.</br>

<big>3.</big> Соціальний тиск або страх. Наприклад, "ваш рахунок буде заблоковано", "вам загрожує штраф", тощо.</br>

<big>4.</big> Психологічне навантаження. Зловмисники тиснуть на людину, викликаючи тривогу або поспіх — жертва робить помилки.</br>

</br>

 1.2 Приклади реальних атак

1. Телефонний дзвінок нібито з банку, де "потрібно підтвердити особу".</br>

2. Підроблений лист із проханням перейти за посиланням для "відновлення доступу".</br>

3. Знайдений флеш-накопичувач з вірусом на парковці.</br>

<img src="https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQUMTJMLYbd4JbLIZ1XjDWQLe9LsCs_SKRN0A&s" alt="Соціальна інженерія схема" width="1300" height="auto">

<h2>2. Види соціальної інженерії</h2>

<big>2.1 Фішинг (Phishing)</big>

Шахрайство через підроблені електронні листи або сайти, які виглядають як офіційні. Зазвичай вимагається ввести паролі, дані банківської картки або іншу конфіденційну інформацію.

Приклад: Лист нібито від банку з повідомленням про "непізнаний вхід у ваш акаунт" із кнопкою "перевірити".

<big>2.2 Вішинг (Vishing)</big>

Голосовий фішинг. Шахраї телефонують під виглядом працівників служби безпеки, поліції або банку.

Приклад: "Ми виявили підозрілий платіж — підтвердьте свої дані, щоб його зупинити."

<big>2.3 Смішинг (Smishing)</big>

Шахрайські SMS-повідомлення з посиланням на підроблені сайти або заклики зателефонувати/відповісти.

Приклад: "Ваша картка буде заблокована. Терміново зв’яжіться з нами."

<big>2.4 Бейтінг (Baiting)</big>

Пропонування "наживки": флешка, знижка, виграш, безкоштовне ПЗ, за якими ховається шкідливий код.

Приклад:Людина знаходить флешку, вставляє її у свій комп’ютер — і активується шпигунська програма.

<img src="https://www.eset.com/fileadmin/ESET/INT/Pages/SMB_topic_pages/social-engineering-identity.png" alt="Соціальна інженерія схема" width="800" height="auto">

<h2>3. Групи ризику соціальної інженерії</h2>

<big>3.1 Літні люди</big>

Менше орієнтуються в технологіях, довіряють "офіційним" джерелам, часто не розуміють, що таке фішинг.

<big>3.2 Діти та підлітки</big>

Схильні відкривати посилання, завантажувати програми, не звертають увагу на безпеку. Їх легко ввести в оману через ігри чи соціальні мережі.

<big>3.3 Активні користувачі соцмереж</big>

Поширюють багато особистої інформації, яку зловмисники використовують для підготовки персоналізованих атак.


```
                <br>
                <b><big>3.4 Співробітники компаній</big></b>
                <br>
                <br>Мають доступ до внутрішніх систем, документів. Через них можуть відбутися злами бізнесу або крадіжка комерційної таємниці.
                <br>
            </p>

                <img src="https://static.tildacdn.com/tild3636-6639-4064-a366-393966353361/__-__.png" alt="Соціальна інженерія схема" width="650" height="auto">
    </div>
    <h2>4. Як захистити себе від соціальної інженерії?</h2>
    <div style="display: flex; align-items: flex-start; gap: 50px;">

            <p><b><big>4.1 Не відкривати підозрілі листи та файли</big></b>
                <br>
                <br>Навіть якщо відправник виглядає "знайомо" — уважно перевіряйте адреси, граматику та стиль.
                <br>
                <br>
                <br>
                <b><big>4.2 Завжди перевіряти відправників</big></b>
                <br>
                <br>Справжні організації рідко пишуть з поштових скриньок на кшталт gmail.com або ukr.net.
                <br>
                <br>
                <br>
                <b><big>4.3 Ніколи не повідомляти особисті дані телефоном</big></b>
                <br>
                <br>Справжні банки ніколи не питають ПІН-коди, CVV або логіни.
                <br>
                <br>
                <br>
                <b><big>4.4 Використовувати антивірус та фаєрвол</big></b>
                <br>
                <br>Актуальне ПЗ здатне зупинити деякі загрози ще до того, як вони нанесуть шкоду.
                <br>
                <br>
                <br>
                <b><big>4.5 Постійно підвищувати рівень своєї кіберграмотності</big></b>
                <br>
                <br>Брати участь у тренінгах, читати тематичні ресурси, обговорювати це з близькими.
                <br>
            </p>
    </div>
</section>
```

```
<!-- Вікторина -->
<section id="quiz">
   <h2>Вікторина (10 питань)</h2>
   <form id="quizForm"></form>
   <button onclick="showResults()">Перевірити</button>
   <div class="result" id="quizResult"></div>
   <div class="result" id="advice"></div>


<h2>Анонімне опитування: Наскільки Ви обізнані з соціальною інженерією?</h2>
<h4>Пропонуємо вам додатково пройти анонімне опитування з рівня обізнаності соціальною інженерією. Ваші анонімні результати будуть внесені до загальної бази відповідей інших учасників. Загальну статистику опитувань можна переглянути в кінці останньої сторінки сайту</h4>
<form id="survey-form">
  <ol>
    <li>
      Чи знаєте ви, що таке соціальна інженерія?
      <br>
      <label><input type="radio" name="q1" value="Так"> Так</label>
      <label><input type="radio" name="q1" value="Ні"> Ні</label>
    </li>
    <li>
      Ви коли-небудь отримували підозрілий лист або SMS?
      <br>
      <label><input type="radio" name="q2" value="Так"> Так</label>
      <label><input type="radio" name="q2" value="Ні"> Ні</label>
    </li>
    <li>
      Ви перевіряєте адресу відправника електронного листа перед відкриттям?
      <br>
      <label><input type="radio" name="q3" value="Так"> Так</label>
      <label><input type="radio" name="q3" value="Ні"> Ні</label>
    </li>
    <li>
      Ви знаєте, що банки ніколи не просять повідомити PIN або CVV-код?
      <br>
      <label><input type="radio" name="q4" value="Так"> Так</label>
      <label><input type="radio" name="q4" value="Ні"> Ні</label>
    </li>
    <li>
      Чи маєте ви антивірус на своєму комп’ютері або смартфоні?
      <br>
      <label><input type="radio" name="q5" value="Так"> Так</label>
      <label><input type="radio" name="q5" value="Ні"> Ні</label>
    </li>
    <li>
      Ви регулярно оновлюєте свої паролі?
      <br>
      <label><input type="radio" name="q6" value="Так"> Так</label>
      <label><input type="radio" name="q6" value="Ні"> Ні</label>
    </li>
```

```
    <li>
      Ви ділитесь конфіденційною інформацією в соціальних мережах?
      <br>
      <label><input type="radio" name="q7" value="Так"> Так</label>
      <label><input type="radio" name="q7" value="Ні"> Ні</label>
    </li>
    <li>
      Чи знаєте ви, що існує фішинг, вішинг, смішинг?
      <br>
      <label><input type="radio" name="q8" value="Так"> Так</label>
      <label><input type="radio" name="q8" value="Ні"> Ні</label>
    </li>
    <li>
      Ви розповідали іншим, як захистити себе від шахрайства?
      <br>
      <label><input type="radio" name="q9" value="Так"> Так</label>
      <label><input type="radio" name="q9" value="Ні"> Ні</label>
    </li>
    <li>
      Чи вважаєте ви, що можете розпізнати соціального інженера?
      <br>
      <label><input type="radio" name="q10" value="Так"> Так</label>
      <label><input type="radio" name="q10" value="Ні"> Ні</label>
    </li>
  </ol>
  <button type="submit">Надіслати</button>
</form>

<p id="survey-result"></p>

<script>
  document.getElementById('survey-form').addEventListener('submit', function(event) {
    event.preventDefault();
    const form = new FormData(event.target);
    let total = 0;
    for (let [key, value] of form.entries()) {
      if (value === 'Так') total++;
    }
    document.getElementById('survey-result').innerHTML =
      `Дякуємо за участь! Ваш рівень обізнаності: <strong>${total}/10</strong>`;
  });
</script>
</section>
<!-- Шпаргалка -->
<section id="memo">
    <h2>Необхідно пам'ятати</h2>
        <div style="display: flex; align-items: flex-start; gap: 50px;">

                <p><b><big>1. Не відкривати підозрілі листи та файли</big></b>
                    <br>
                    <br>Перш ніж відкривати вкладення або натискати на посилання в електронному листі, варто перевірити кілька речей:<br>
```


 - Чи очікували ви цей лист? Якщо ні — будьте особливо обережні.

 - Перевірте, чи не містить текст граматичних помилок, неприродних висловів або терміновості на кшталт "Негайно!", "Ваш обліковий запис буде видалено!".

 - Не відкривайте вкладення з розширенням .exe, .js, .scr, .bat, .vbs — вони можуть запускати шкідливий код.

 - Якщо в листі є посилання, наведіть курсор, щоб побачити реальну адресу (не натискаючи). Якщо URL виглядає підозріло (наприклад, bank-ukr.com-info.ua) — не відкривайте.

<big>2. Завжди перевіряти відправників</big>

Ім’я відправника може бути підробленим, тому:

 - Звертайте увагу не лише на ім’я, а й на адресу (наприклад, support@secure-bank.com — нормально, а securebank@gmail.com — підозріло).

 - Підроблені домени часто мають замінені літери (@gmai1.com замість @gmail.com, або faceboook.com).

 - Якщо сумніваєтеся — зателефонуйте в офіційну службу підтримки за номером із офіційного сайту, а не тим, що вказаний у листі.

<big>3. Ніколи не повідомляти особисті дані телефоном</big>

Жоден банк, державна служба чи технічна підтримка ніколи не запитує:

 - PIN-коди до карток

 - Паролі від онлайн-банкінгу або e-mail

 - CVV-коди картки (3 цифри на звороті)

 - Одноразові коди з SMS чи push-повідомлень

Пам'ятайте: справжні служби безпеки мають доступ до потрібної інформації і не потребують її уточнення у клієнтів по телефону. Якщо вас просять — це шахраї.

<big>4. Використовувати антивірусне програмне забезпечення та фаєрвол</big>

 - Регулярно оновлюйте антивірус — нові загрози з’являються щодня, і лише актуальні бази зможуть їх виявити.

 - Використовуйте фаєрвол, щоб контролювати, які програми мають доступ до Інтернету та які підключення здійснюються до вашого комп’ютера.

 - Встановлюйте лише перевірені програми, бажано з офіційних сайтів або магазинів (Google Play, App Store).

Пам'ятайте: антивірус — це не панацея, а лише інструмент.

Основний захист — це ваша пильність.

<big>5. Постійно підвищувати рівень своєї кіберграмотності</big>

Безперервне навчання — найкраща інвестиція в інформаційну безпеку:

 - Проходьте онлайн-курси або вікторини з кібербезпеки.

 - Читайте офіційні блоги та новини від кіберполіції, банків та міжнародних експертів (наприклад, ESET, Kaspersky, OWASP).

 - Розповідайте близьким про нові шахрайські схеми. Найкращий захист — це інформованість усіх членів родини.

 - Ведіть обговорення з колегами, дітьми та старшими родичами — обмін досвідом допомагає формувати захисну культуру.

🔐 Важливо: ніхто не застрахований від обману. Але кожен може зменшити ризики, якщо буде уважним, поінформованим і обережним.
</p>

<img src="https://gigatrans.ua/public/storage/jbET5L3hRYF6qQs1b1h2.png" alt="Соціальна інженерія схема" width="650" height="auto">

<h2>Результати анонімного опитування:</h2>
<table>
<tr><th>Запитання</th><th>Так</th><th>Ні</th></tr>
<tr><td>Чи знаєте ви, що таке соціальна інженерія?</td><td>60%</td><td>40%</td></tr>
<tr><td>Чи отримували фейкові дзвінки?</td><td>80%</td><td>20%</td></tr>
<tr><td>Ви коли-небудь отримували підозрілий лист або SMS?</td><td>85%</td><td>15%</td></tr>
<tr><td>Чи знаєте ви, що існує фішинг, вішинг, смішинг?</td><td>35%</td><td>65%</td></tr>
<tr><td>Чи встановлений у вас антивірус?</td><td>70%</td><td>30%</td></tr>
<tr><td>Ви перевіряєте адресу відправника електронного листа перед відкриттям?</td><td>35%</td><td>65%</td></tr>
<tr><td>Ви знаєте, що банки ніколи не просять повідомити PIN або CVV-код?</td><td>89%</td><td>11%</td></tr>
<tr><td>Ви регулярно оновлюєте свої паролі?</td><td>55%</td><td>45%</td></tr>
<tr><td>Ви розповідали іншим, як захистити себе від шахрайства?</td><td>68%</td><td>32%</td></tr>
<tr><td>Ви ділитесь конфіденційною інформацією в соціальних мережах?</td><td>15%</td><td>85%</td></tr>
<tr><td>Чи вважаєтн ви свій інформаційний простір безпечним?</td><td>78%</td><td>22%</td></tr>
</table>
</section>

```
<script>
// Переходи між сторінками
function showPage(pageId) {
   document.querySelectorAll("section").forEach(s => s.classList.remove("active"));
   document.getElementById(pageId).classList.add("active");
}

// Питання та відповіді
const questions = [
   ["Що таке фішинг?", ["Антивірус", "Підроблені листи", "Телефонний дзвінок"], 1, "2.1 Фішинг"],
   ["Що таке бейтінг?", ["Заражена флешка", "SMS від банку", "Антивірус"], 0, "2.4 Бейтінг"],
   ["Кому не можна повідомляти паролі?", ["Колезі", "Офіційному листу", "Нікому"], 2, "4.3 Не передавати дані"],
   ["Як убезпечити комп’ютер?", ["Вимкнути Інтернет", "Встановити антивірус", "Не використовувати соцмережі"], 1, "4.4 Антивірус"],
   ["Хто в зоні ризику?", ["Тільки пенсіонери", "Тільки діти", "Усі користувачі"], 2, "3. Хто в зоні ризику"],
   ["Що таке вішинг?", ["SMS", "Телефонний дзвінок", "Флешка"], 1, "2.2 Вішинг"],
   ["Що таке смішинг?", ["Лист", "SMS", "Телефонний дзвінок"], 1, "2.3 Смішинг"],
   ["Яке правило безпеки?", ["Перевіряти відправника", "Відкривати все", "Не оновлювати систему"], 0, "4.2 Перевірка"],
   ["Що таке соціальна інженерія?", ["Вірус", "Маніпуляція людьми", "Антивірус"], 1, "1 Соціальна інженерія"],
   ["Який метод використовує фішинг?", ["Листи та сайти", "Телефонні дзвінки", "Віруси"], 0, "2.1 Фішинг"],
];

// Генерація тестів

function generateQuiz()
{
   let quizHTML = "";
   questions.forEach((q, i) =>
         {
      quizHTML += `<div class="question" id="q${i}"><p>${i+1}. ${q[0]}</p>`;
      q[1].forEach((opt, j) =>
                  {
         quizHTML += `<input type="radio" name="q${i}" value="${j}"> ${opt}<br>`;
      });
      quizHTML += `</div>`;
   });
   document.getElementById("quizForm").innerHTML = quizHTML;
}

generateQuiz();

// Перевірка тестів
```

```
function showResults() {
   let score = 0, adviceText = "Підказки:";
   questions.forEach((q, i) => {
      let selected = document.querySelector(`input[name="q${i}"]:checked`);
      let div = document.getElementById(`q${i}`);
      div.classList.remove("correct","incorrect");
      if (selected) {
         if (parseInt(selected.value) === q[2]) {
            score++; div.classList.add("correct");
         } else {
            div.classList.add("incorrect");
            adviceText += `<br>${i+1}. ${q[3]}`;
         }
      } else {
         div.classList.add("incorrect");
         adviceText += `<br>${i+1}. ${q[3]} (не обрано)`;
      }
   });
   document.getElementById("quizResult").innerHTML = `Результат: ${score}/10`;
   document.getElementById("advice").innerHTML = score<10 ? adviceText : "Ви молодець!
Усе правильно.";
}

</script>

</body>
</html>
```