Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА
на тему:
«ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ОЦІНЮВАННЯ
РІВНЯ КІБЕРГІГІЄНИ ОСОБИ»

Виконав: студент 2 курсу, групи 1БС-22м
спеціальності 125 Кібербезпека
_____Анастасія ФЕДОРОВА
Керівник: к.т.н., доцент каф.ЗІ
_____Леонід КУПЕРШТЕЙН
«11»_____12_____2023 р.
Опонент: к.т.н., доцент каф.ПЗ
_____Олена КОВАЛЕНКО
«13»_____12_____2023 р.

Допущено до захисту
Завідувач кафедри ЗІ
д.т.н., проф.
_____Володимир ЛУЖЕЦЬКИЙ
«15»_____12_____2023 р.

Вінниця ВНТУ – 2023 року

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Рівень вищої освіти II (магістерський)
Галузь знань – 12 Інформаційні технології
Спеціальність – 125 Кібербезпека
Освітньо-професійна програма – Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Завідувач кафедри ЗІ,
д. т. н., проф.
Володимир ЛУЖЕЦЬКИЙ
«19» 09 2023 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Федоровій Анастасії Вячеславівні

1. Тема роботи: «Інформаційна технологія оцінювання рівня кібергігієни особи»

керівник роботи: Куперштейн Леонід Михайлович, к. т. н., доцент, затверджені наказом ректора ВНТУ від «18» вересня 2023 № 247.

2. Строк подання студентом роботи: «13» грудня 2023р.

3. Вихідні дані до роботи:

- засіб повинен запускатись в операційній системі Windows;
- засіб повинен надавати достовірну оцінку рівня кібергігієни особи;
- засіб повинен враховувати різні напрямки кібергігієни.

4. Зміст текстової частини: Вступ. 1. Аналіз предметної області. 2. Розробка інформаційної технології. 3. Інформаційна технологія оцінки рівня кібергігієни особи. 4. Тестування засобу оцінки рівня кібергігієни. 5. Економічна частина. Висновки. Перелік використаних джерел. Додатки.

5. Перелік ілюстративного матеріалу: Архітектура системи оцінки рівня кібергігієни особи (плакат А4). Алгоритм роботи системи оцінки рівня кібергігієни (плакат А4). Система процесів інформаційної технології (плакат А4). Схема роботи модуля автентифікації/авторизації (плакат А4). Схема роботи модуля керування (плакат А4). Схема роботи модуля обробки результатів (плакат А4).

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Куперштейн Л. М., доц. кафедри ЗІ	19.09	
2	Куперштейн Л. М., доц. кафедри ЗІ	19.09	
3	Куперштейн Л. М., доц. кафедри ЗІ	19.09	
4	Ратушняк О.Г. к. т. н., доц.	19.09	

7. Дата видачі завдання «1» вересня 2023 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської дипломної роботи	Строк виконання етапів роботи	Прим.
1	Аналіз завдання. Вступ	01.09.2023 – 10.09.2023	
2	Аналіз літературних джерел за напрямком магістерської кваліфікаційної роботи	10.09.2023 – 15.09.2023	
3	Науково-технічне обґрунтування	16.09.2023 – 22.09.2023	
4	Розробка технічного завдання	23.09.2023 – 29.09.2023	
5	Розробка рішень	30.09.2023 – 12.10.2023	
6	Практична реалізація, інтеграція, результати	14.10.2023 – 10.11.2023	
7	Розробка розділу тестування і обґрунтування доцільності розробки	11.11.2023 – 17.11.2023	
8	Аналіз виконання ТЗ, висновки	18.11.2023 – 24.11.2023	
9	Оформлення пояснювальної записки	25.11.2023 – 30.11.2023	
10	Попередній захист та доопрацювання МКР	28.11.2023 – 01.12.2023	
11	Перевірка магістерської роботи на наявність плагіату	02.12.2023 – 10.12.2023	
12	Представлення МКР до захисту	11.12.2023 – 14.12.2023	
13	Захист МКР	14.12.2023 – 21.12.2023	

Студент _____ Анастасія ФЕДОРОВА

Керівник роботи _____ Леонід КУПЕРШТЕЙН

АНОТАЦІЯ

Федорова А.В. Інформаційна технологія оцінювання рівня кібергігієни особи. Магістерська кваліфікаційна робота зі спеціальності 125 – Кібербезпека, освітня програма – Безпека інформаційних і комунікаційних систем. Вінниця: ВНТУ, 2023.

Укр.мовою. Бібліогр.: рис.18, табл.3.

Магістерська кваліфікаційна робота присвячена розробці інформаційної технології оцінювання рівня кібергігієни особи та програмного засобу, що реалізує вказану технологію. В рамках роботи було проведено аналіз існуючих систем та засобів оцінювання рівня кібергігієни. Розроблено програмний засіб.

Ілюстративна частина складається з 6 плакатів.

В економічному розділі оцінено витрати на розробку технології та програмного засобу.

Ключові слова: кібергігієна, інформаційна безпека.

ABSTRACT

Fedorova A.V. Information technology for assessing a person's level of cyber hygiene. Master's thesis on specialty 125 - Cybersecurity, educational program - Security of information and communication systems. Vinnytsia: VNTU, 2023. Bibliographer: fig.18, tabl.3.

Ukrainian language.

The master's thesis is devoted to the development of information technology for assessing the level of cyber hygiene of a person and the software that implements the specified technology. As part of the work, an analysis of existing systems and tools for assessing the level of cyber hygiene was carried out. A software tool has been developed.

The illustrative part consists of 6 posters.

The economic section estimates the costs of technology and software development.

Keywords: cyber hygiene, information security.

ЗМІСТ

ВСТУП

Технологічний прогрес торкнувся кожної галузі нашого життя. Наразі комп'ютери або інші технології використовуються на кожному підприємстві, майже кожна людина так чи інакше пов'язує виконання своїх посадових обов'язків з технікою. В цьому, безперечно, є безліч позитивних аспектів, але в той же час це збільшує кількість інцидентів інформаційної безпеки.

На початку роботи на будь-якому підприємстві працівник проходить інструктаж з охорони праці, але, на жаль, надзвичайно рідко в них підіймають тему кібергігієни. Саме через це можливий витік важливої інформації з причини нерозуміння проблеми працівником, адже, як відомо, найслабша ланка системи – це людина.

Описані раніше факти створюють проблему для роботодавців не нехтувати рівнем кібергігієни особи, яка є кандидатом на посаду, та ретельно перевіряти знання систематично. Інструкторам з проведення інструктажів охорони праці також важливо мати можливість аналізувати рівень кібергігієни в компанії та проводити роботу над слабими місцями.

Актуальність. На сьогоднішній день, коли в країні проходить активна інформаційна війна, питання кібергігієни повинно вивчатись максимально уважно, адже від цього залежить не лише безпека конкретної людини, але мова також йде про безпеку підприємств та цілої нації. Нехтування основними правилами поведінки в кіберпросторі може призвести до негативних наслідків, таких як витік важливої інформації, яку може використати зловмисник в своїх цілях, втрата таємної інформації, персональних даних. Підприємство повинно мати інструмент, який дозволить оцінити рівень знань співробітника. Розробка інформаційної технології оцінювання кібергігієни особи дозволить збільшити безпеку даних підприємств та країни в цілому.

Об'єктом дослідження є процеси оцінювання рівня кібергігієни особи.

Предметом дослідження є методи та засоби оцінювання рівня кібергігієни особи.

Метою магістерської кваліфікаційної роботи є підвищення рівня кібербебезпеки підприєства за рахунок оцінки рівня кібергігієни працівників.

Для досягнення мети необхідно виконати наступні завдання:

- проаналізувати напрямки кібергігієни;
- проаналізувати аналоги для оцінювання рівня кібергігієни;
- розробити інформаційну технологію;
- розробити програмний засіб, що реалізує інформаційну технологію;
- виконати тестування програмного засобу.

Наукова новизна. Запропонована інформаційна технологія оцінювання рівня кібергігієни працівників організації, яка полягає у тестуванні працівника певної посади за відповідними напрямками кібергігієни, що дозволить забезпечити належний рівень інформаційної безпеки підприємства.

Практична цінність полягає у тому, розроблено програмний засіб, який дозволяє зібрати та проаналізувати дані про рівень кібергігієни працівників підприємств, залежно від посади та обов’язків і, при необхідності, забезпечити подальше навчання.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Аналіз напрямків кібергігієни

Будь-яка помилка завжди вартує компанії прибутку, ресурсів, затрат зайвого часу. За даними аналітиків, втрати підприємств по причині людського фактору становлять 89%, сюди входять як навмисний злив даних, так і необачність та незнання правил кібергігієни в кіберпросторі [1]. Втрати підприємств через людський фактор можуть виникати з різних причин і призводити до різних наслідків. Ось кілька типових сценаріїв, які можуть призводити до втрат[1]:

- Людські помилки: невірні рішення, неправильно введені дані, невірне виробництво або обслуговування можуть призвести до великих втрат.

- Неправильне використання ресурсів: зловживання виробничим обладнанням, матеріалами або іншими ресурсами також може спричинити втрати.

- Шахрайство та злочинні дії: крадіжки, фінансові махінації, використання конфіденційної інформації можуть призвести до значних фінансових втрат.

- Незадовільні умови праці: неправильні умови праці можуть впливати на якість виробів чи послуг.

- Непрофесійна поведінка: негативна поведінка працівників може призвести до втрати репутації підприємства, що може вплинути на його фінансові результати.

- Втрати через конфлікти: конфлікти між працівниками можуть вести до втрат продуктивності та зниження ефективності роботи.

Для управління ризиками, пов'язаними з людським фактором, підприємства можуть впроваджувати політики безпеки, навчання працівників,

контроль за доступом до конфіденційної інформації, а також встановлювати етичні стандарти та процедури для вирішення конфліктів.

Згідно закону України «Про основні засади забезпечення кібербезпеки України» визначаються наступні поняття:

Кіберпростір - середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [2].

Кібергігієна - уміння, навички користування інформаційними технологіями, спрямовані на здійснення заходів щодо своєчасного виявлення, запобігання і нейтралізації реальних і потенційних кіберзагроз [2].

Виділяють наступні види кібергігієни:

1) Кібергігієна паролів.

Основні проблеми:

- Людський фактор. Слабкі паролі: Багато користувачів вибирають слабкі паролі або використовують легко вгадувані комбінації, що знижує стійкість їх облікових записів до атак.

- Системні вразливості. Атаки перебором: Атаки перебором паролів включають в себе спроби вгадати пароль шляхом спроб усіх можливих комбінацій. Якщо пароль слабкий, такий вид атаки може бути успішним.

- Множинні облікові записи. Управління багатьма паролями: Для безпеки рекомендується використовувати унікальні паролі для кожного облікового запису. Управління багатьма паролями може бути важким завданням для користувачів.

- Втрата паролів. Спроба створити складний пароль для безпеки може призвести до того, що користувачі забувають свої паролі. Це може викликати втрату доступу до облікового запису.

- Альтернативні методи автентифікації. Деякі методи автентифікації можуть бути неефективними або занадто непорівнянною для користувачів, що може призводити до їх обходження або ігнорування.

- Атаки фішингу та соціальної інженерії. Отримання пароля шляхом обману: Користувачі можуть випадково втратити свої паролі через атаки фішингу або соціальної інженерії.

Розв'язанням цих проблем може бути поєднання використання сильних паролів, використання двофакторної аутентифікації, вдосконалення систем безпеки, які ускладнюють атаки перебором паролів, і надання користувачам зручних і безпечних інструментів для управління своїми паролями [3].

2) Кібергігієна персонального комп’ютера.

Основні проблеми:

- Віруси та шкідливі програми. Недостатній або неактуальний антивірус може вести до зараження комп'ютера вірусами та іншими шкідливими програмами.

- Оновлення та патчі. Неактуальне програмне забезпечення, відсутність регулярних оновлень та патчів може залишити комп'ютер вразливим перед загрозами.

- Фаєрвол та брандмауер. Погано налаштований фаєрвол може допустити несанкціонований доступ до комп'ютера та втрату конфіденційності.

- Сильні та унікальні паролі. Використання легко вгадуваних чи слабких паролів може зробити комп'ютер легкою мішенню для зловмисників.

- Управління конфіденційністю. Неакуратне управління особистими даними та відсутність відповідних налаштувань можуть призвести до проблем з конфіденційністю.

- Файлова система та резервне копіювання. Недостатнє регулярне резервне копіювання може призвести до втрати важливих даних внаслідок видалення або атак.

Рішення цих проблем включає в себе регулярне оновлення програмного забезпечення, використання надійного антивірусу та фаєрволу, уважність в мережі, використання сильних паролів та двохфакторної аутентифікації, а також ефективне управління конфіденційністю та регулярне резервне копіювання даних [3].

3) Кібергігієна мобільного пристрою.

Основні проблеми:

- Втрата чи крадіжка пристрою. Якщо пристрій втрачено або вкрадено, це може призвести до небажаного доступу до особистої інформації та даних.

- Недостатня аутентифікація. Використання слабкого пароля чи відсутність заходів блокування може стати причиною незаконного доступу до пристрою.

- Неактуальне програмне забезпечення. Невчасне або відсутнє оновлення операційної системи та інших додатків може залишити пристрій вразливим перед новими загрозами безпеки.

- Атаки на мережі та зловмисне ПЗ. Зловмисники можуть використовувати фішинг та інші методи для видалення конфіденційної інформації чи встановлення шкідливого програмного забезпечення на мобільний пристрій.

- Неперевірені додатки. Встановлення додатків з ненадійних джерел може призвести до встановлення шкідливого програмного забезпечення на пристрій.

Для вирішення цих проблем рекомендується використовувати паролі та методи аутентифікації, встановлювати оновлення програмного забезпечення, уникаючи громадських Wi-Fi без забезпечення додаткового захисту, освітювати користувачів, встановлювати додатки лише з надійних джерел та ретельно контролювати доступ до особистих даних [3].

4) Кібергігієна електронної пошти.

Основні проблеми:

- Фішинг та спам. Спам та фішингові листи можуть містити шкідливі посилання або призвести до витоку конфіденційної інформації.

- Шкідливі файли. Вкладення в електронних листах можуть містити віруси або інше шкідливе програмне забезпечення.

- Соціальна Інженерія. Зловмисники можуть використовувати соціальну інженерію, щоб отримати доступ до особистої інформації чи облікових даних.

- Недостатня аутентифікація. Використання слабких чи легко вгадуваних паролів для електронної пошти може стати причиною несанкціонованого доступу.

- Недостатній захист листування. Недостатнє шифрування може призвести до того, що важливі дані можуть бути доступні третім особам.

- Викрадання акаунтів. Атаки на акаунти можуть вести до викрадання поштових скриньок та небажаної користі з них.

- Спільний доступ до пошти. Використання спільних акаунтів або недостатній контроль доступу можуть призвести до втрати конфіденційності.

- Небажана реклама. Небажані рекламні листи можуть порушувати приватність користувача.

Рішення цих проблем включає в себе використання антиспамових та антивірусних фільтрів, уважності користувачів при натисканні на посилання чи відкриванні вкладень, використання надійних паролів та двофакторної аутентифікації, шифрування листування та постійне навчання користувачів про потенційні загрози [3].

5) Кібергігієна соціальних мереж та месенджерів.

Основні проблеми:

- Спроби витягнути особисту інформацію. Зловмисники можуть використовувати соціальні мережі та месенджери для фішингових атак, спрямованих на отримання конфіденційної інформації.

- Спам та небажані повідомлення. Користувачі можуть стикатися з небажаними повідомленнями, рекламою та спамом в соціальних мережах та месенджерах.

- Кіберзнущання та булінг. Кіберзнущання та булінг можуть виникнути в мережах через некоректну поведінку користувачів.

- Втрата приватності. Недостатній контроль над налаштуваннями приватності може вести до неправильного використання особистої інформації.

- Віруси та шкідливе ПЗ. В соціальних мережах можуть з'являтися посилання на шкідливий контент або програми.

- Атаки на акаунти. Атаки на акаунти та витоки облікових даних можуть призвести до несанкціонованого доступу до особистих профілів.

- Спілкування з невідомими особами. Користувачі можуть невірно оцінювати ризики, спілкуючись з невідомими особами через месенджери та соціальні мережі.

- Дитяча безпека. Діти можуть стикатися з ризиками, пов'язаними з використанням соціальних мереж та месенджерів, такими як контент для дорослих або небезпечні контакти.

- Фейкові профілі та ідентичність: Існування фейкових профілів може призвести до витоку дезінформації та обману користувачів.

Розв'язання цих проблем включає в себе використання налаштувань приватності, уважне ставлення до отриманих повідомлень та запитань про особисту інформацію, надання освіти користувачам щодо онлайн-безпеки та використання функцій блокування та звітності для недоречних випадків [3].

6) Кібергігієна електронних платежів.

Основні проблеми:

- Шахрайство та атаки на карткові дані. Зловмисники можуть використовувати різні методи, такі як фішинг або злам, для отримання кредитних карткових даних та здійснення неправомірних транзакцій.

- Віруси та шкідливе ПЗ. Віруси та шкідливе програмне забезпечення можуть використовуватися для витягнення фінансової інформації або втручання в електронні платежі.

- Неактуальне ПЗ та недостатні оновлення. Використання застарілого або недостатньо оновленого програмного забезпечення може створити вразливості для кібератак та загроз безпеці.

- Недостатнє шифрування. Використання ненадійних методів шифрування може призвести до витоку особистої інформації та фінансових даних.

- Порушення приватності та використання даних. Електронні платіжні системи можуть втрачати довіру користувачів, якщо вони неправильно обробляють або передають особисті дані.

- Несанкціоновані транзакції. Зловмисники можуть намагатися використати неправомірний доступ до електронних платіжних систем для здійснення транзакцій від імені користувача.

- Проблеми з аутентифікацією. Неякісні методи аутентифікації можуть стати причиною несанкціонованих доступів до електронних платіжних рахунків.

- Купівля та продаж на ненадійних сайтах. Користувачі можуть стикатися з ризиками при взаємодії з ненадійними торговими платформами або сайтами для електронних платежів.

- Фінансові технології. Розвиток фінтех-технологій може призвести до нових видів кіберзагроз та вимагати постійного адаптування заходів кібербезпеки.

Для розв'язання цих проблем важливо використовувати безпечні електронні платіжні системи та платформи, регулярно оновлювати програмне забезпечення, використовувати надійні методи проведення транзакцій [3].

7) Кібергігієна технології Wi-Fi.

Основні проблеми:

- Ненадійне шифрування. В ненадійно налаштованих Wi-Fi мережах або з використанням застарілих протоколів може бути легше здійснити несанкціонований доступ.

- Слабкі паролі та несанкціонований доступ. Легкі для вгадування паролі можуть призвести до несанкціонованого доступу до Wi-Fi мережі.

- Зловмисні точки доступу. Зловмисники можуть створювати фейкові Wi-Fi точки, щоб привабити користувачів та отримати доступ до їх даних.

- Фішингові атаки та мережеві загрози. Зловмисники можуть використовувати Wi-Fi для проведення фішингових атак або розповсюдження шкідливого програмного забезпечення.

- Недостатній контроль за підключеннями. Недостатній контроль за підключеннями може призвести до несанкціонованого доступу та атак на мережу.

- Використання відкритих мереж. Використання невідомих або ненадійних відкритих Wi-Fi мереж може призвести до ризиків для безпеки даних.

- Недостатнє шифрування трафіку. Відсутність або ненадійне шифрування може призвести до прослуховування та витоку конфіденційної інформації.

- Неактуальне програмне забезпечення обладнання. Застаріле обладнання може бути вразливим перед новими кіберзагрозами [3].

8) Кібергігієна споживання інформації.

Основні проблеми:

- Розповсюдження фейкових та маніпулятивних змістів. Інформаційні ресурси можуть містити фейкові новини, дезінформацію або маніпуляції, що може впливати на погляди та рішення користувачів.

- Надмірна кількість інформації. Надмірна кількість інформації може ускладнити вибір та розуміння важливих питань.

- Анонімність та кібербулінг. Анонімні користувачі можуть вести агресивні дії в мережі, включаючи кібербулінг.

- Залежність від соцмереж та інформаційний баласт. Залежність від соціальних мереж та надмірне використання може впливати на психічне здоров'я та забезпечити велику кількість несправжньої інформації.

- Розповсюдження загроз здоров'ю та інші шкідливі впливи. Зміст, що розповсюджує хибні медичні поради чи загрози здоров'ю, може впливати на поведінку користувачів [4].

9) Соціальна інженерія

Соціальна інженерія — це метод атаки, коли атакуючий використовує маніпулювання людським фактором, а не технічні засоби, для отримання конфіденційної інформації, нелегітимного доступу або виконання інших шкідливих дій. Основні проблеми, пов'язані з соціальною інженерією, включають:

- Недооцінка ризиків. Багато людей можуть бути несвідомі або недооцінювати ризики, пов'язані з соціальною інженерією, і тому можуть стати легкою мішенню для атак.

- Низький рівень кібербезпеки. Багато працівників не мають достатньої підготовки в галузі кібербезпеки та соціальної інженерії, що робить їх вразливими перед атаками.

- Віра в авторитет. Люди можуть легко вірити або слідувати інструкціям, представленим впливовими особами, без перевірки їхньої достовірності.

- Експлуатація особистих даних. Зловмисники можуть використовувати інформацію, доступну в соціальних мережах, для персоналізованих атак і маніпуляцій.

- Слабкий контроль доступу. Недостатній контроль доступу до конфіденційної інформації внутрішніх систем може легко дозволити несанкціонований доступ через соціальну інженерію.

- Недостатні заходи безпеки. Брак адекватних заходів фізичної безпеки може забезпечити можливість фізичного доступу для атак, що використовують соціальну інженерію.

- Ігнорування загроз. Деякі люди можуть ігнорувати загрози безпеки, оцінюючи їх як малоймовірні або несуттєві.

- Недостатня перевірка дій. Багато систем не мають ефективних механізмів аудиту, що ускладнює виявлення та розслідування соціально-інженерних атак.

Більшість названих вище проблем досить просто вирішити шляхом надання населенню достатньої інформації, проходженням тематичних курсів та тренінгів [5].

1.2 Аналіз засобів оцінки кібергігієни

Наразі існує декілька систем для оцінки рівня кібергігієни особи. Нижче наведена порівняльна таблиця (табл. 1.1):

Таблиця 1.1 – Порівняльна таблиця засобів оцінки рівня кібергігієни

№	Назва	Тематика	Вартість	Країна розробки	Наявність сертифіката з результатами
1.	Дія.Освіта	Основи кібергігієни для держслужбовців	Безкоштовно	Україна	Так
2.	Дія.Освіта	Персональна кібергігієна, безпека в	Безкоштовно	Україна	Так

		мережі Інтернет			
3.	Дія.Освіта	Кібергігієна для дітей	Безкоштовно	Україна	Ні
4.	Дія.Освіта	Кібергігієна під час війни	Безкоштовно	Україна	Ні
5.	Здолати шахрая	58 кейсів шахрайства в мережі Інтернет	Безкоштовно	Україна	Ні
6.	Cyberacademy	Кібергігієна для підприємств	Платний інтенсив	Україна	Так
7.	Як?	Практичні поради з цифрової безпеки	Безкоштовно	Україна	Ні
8.	Цифрограм. Твоя кібергігієна	Телеграм бот з тестами на різні напрямки кібергігієни	Безкоштовно	Україна	Ні
9.	Google Jigsaw	Тест на розпізнавання фішингових листів	Безкоштовно	Україна	На
10.	Cybereducation	Базові правила безпеки в цифровому середовищі	Безкоштовно	Великобританія	Ні

11.	Єшко	Цифрова безпека	3713 грн.	Україна	Так

Розглянемо кожну детальніше:

1. Дія.Освіта (Основи кібергігієни для держслужбовців) – освітній серіал, що складається з трьох серій та націлений на вивчення базових правил кібергігієни держслужбовцями. Після повномасштабного вторгнення Росії на територію України, українські органи влади стали однією з основних цілей ворожих хакерів. Основні інструменти для цього — люди. Зловмисники користуються їхньою неуважністю: вони можуть не помітити підозрілий лист, відкрити сумнівне покликання, повірити у фейк або проігнорувати подвійну автентифікацію на смартфоні [6].

2. Дія.Освіта (Персональна кібергігієна) – освітній серіал, що складається з трьох серій та націлений на вивчення базових правил особистої кібергігієни. В освітньому серіалі з кібербезпеки розібрали психологію та прийоми онлайн-шахраїв, природу фейків, вірусів і як цьому ефективно протидіяти. Освітній серіал створено з ініціативи Мінцифри для платформи Дія.Освіта за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури України» та розроблено експертами Києво-Могилянської Академії [6].

3. Дія.Освіта (Кібергігієна для дітей) – гайд, розрахований на дитячу аудиторію, що містить в собі основні застереження та перелік рекомендацій щодо правильного користування кіберпростором [6].

4. Дія.Освіта (Кібергігієна під час війни) – гайд, розрахований на будь-яку вікову категорію, в якому описуються рекомендації щодо поведінки в кіберпросторі в умовах інформаційної війни. Цифрове середовище вже давно стало невід'ємною складовою життя людини і суспільства. Наш гайд «Онлайн-безпека під час війни» стане у пригоді широкій аудиторії — дітям, батькам і

опікунам, людям поважного віку та молоді. Оскільки в умовах повномасштабної війни росії проти нашої держави стало ще простіше скористатися вразливістю користувачів в онлайн- просторі. У ці часи потрібно подбати про свою цифрову безпеку та дотримуватися правил, які допоможуть захистити себе та своїх близьких [6].

Кібергігієна стала ще важливішою під час першої повномасштабної кібервійни. В умовах інформаційно-психологічних атак варто дотримуватися правил онлайн-безпеки, залишатися пильними та обережними.

5. Здолати шахрая – 58 кейсів у вигляді тестів, з різними напрямками шахрайства в мережі Інтернет. Онлайн-гра «Здолай шахрая!» – це гра-симуляція, де гравці потрапляють у змодельовані ситуації різних видів платіжного шахрайства та отримують інформацію про наслідки прийнятих ними рішень і поради щодо виявлення шахрайства та дієвих засобів захисту у кожній ситуації. Клацнувши на картку з зображенням монстра-шахрая, гравець проходить одну схему платіжного шахрайства та дізнається про її ознаки й методи захисту. Наразі гра складається з 56 тематичних частин, які симулюють різні види платіжного шахрайства: телефонне, банкоматне та кредитне шахрайство, угон SIM-картки, шахрайські розіграші призів, опитування та інтернет-крамниці, шахрайство на дошках оголошень, у сферах працевлаштування та заробітку в інтернеті, туризму та розваг, фішинг, шкідливе програмне забезпечення, програми-вимагачі, геймінг-шахрайство тощо [7].

6. Cyberacademy (Кібергігієна для підприємств) – курс, націлений на керівників та працівників підприємств різного напрямку діяльності (рис 1.1).

7. 

8. Рисунок 1.1 – Програма та деталі курсу

Складається з тренінгів та інтенсивів, також включає в себе роботу з кураторами та різні перевірки знань. Програма пропонує тестування рівня кібер-гігієни всіх працівників на онлайн-платформі CybExer, навчання працівників за програмою Cyber Hygiene (3 рівні), періодичну перевірку результатів навчання шляхом симуляції фішингових атак, проведення цільових тренінгів для вирішення найбільш проблемних аспектів, а також регулярну комунікаційну підтримку і стимуляцію всього персоналу [8].

9. Як? – Збірник практичних порад щодо користування пристроями на основі різних операційних систем та різноманітними месенджерами та соціальними мережами (рис 1.2) [9].

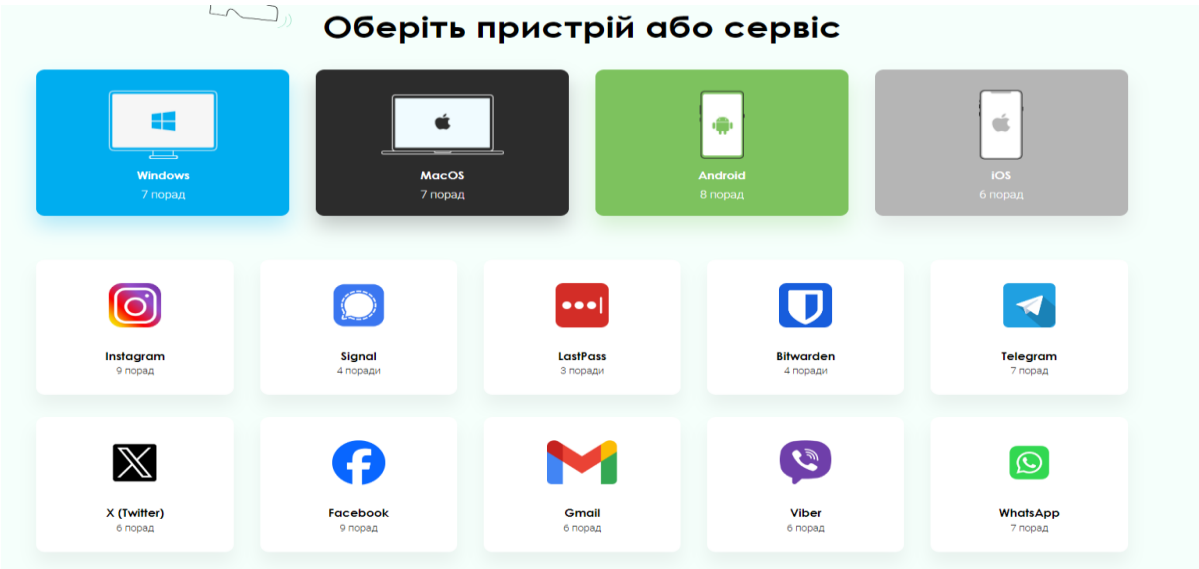

Рисунок 1.2 – Вибір тематики порад на порталі «Як?»

10. Цифрограм. Твоя кібергігієна – телеграм-бот, який спрямований на оцінку рівня кібергігієни особи, задаючи випадкові запитання з різних напрямків кібергігієни. Цей чат-бот розроблений за спільної ініціативи Міністерства цифрової трансформації України (https://t.me/mintsyfra), Міжнародної фундації виборчих систем (IFES), Координатора проектів ОБСЄ та компанії Vodafone Україна (https://t.me/vfukraine). Чат-бот також є частиною проекту Дія. Цифрова освіта (https://osvita.diia.gov.ua/) [10].

11. Google Jigsaw – офіційний сервіс компанії Google, тест з визначенням, чи являється наведений електронний лист фішинговим, чи ні (рис 1.3) [11].

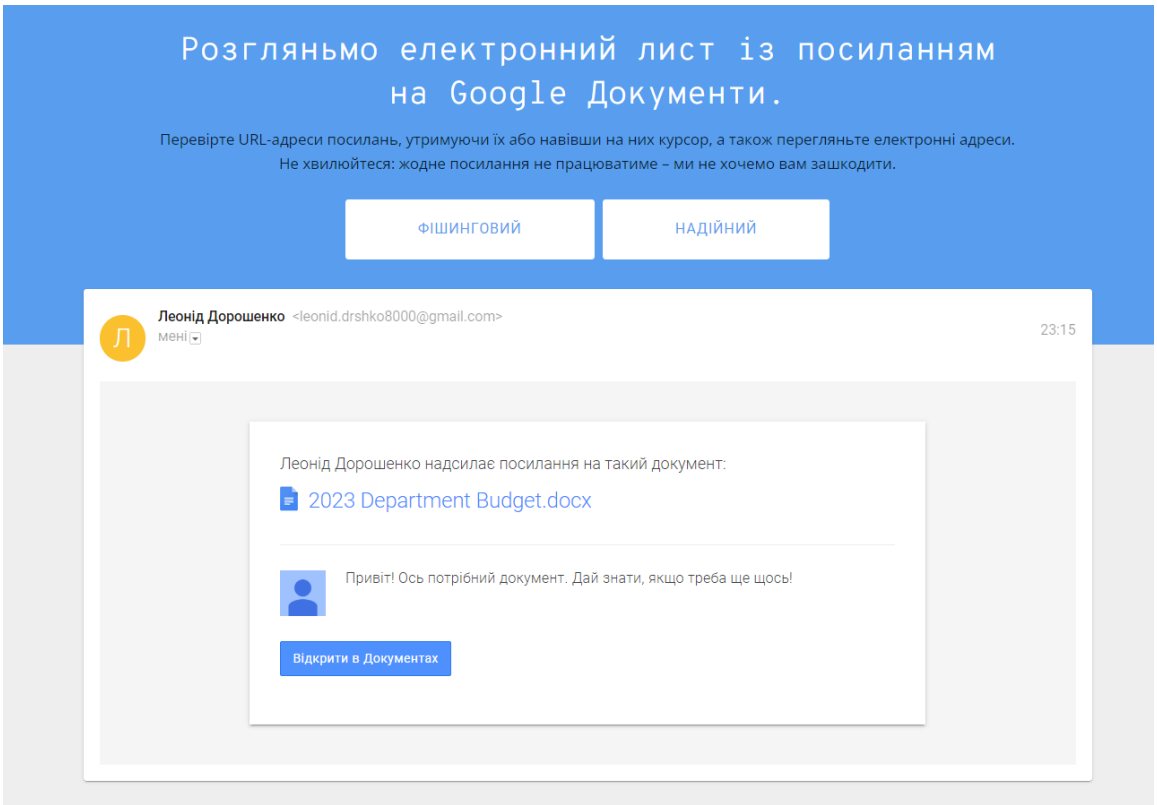

Рисунок 1.3 – Приклад запитання на порталі Google Jigsaw

12. Cybereducation (Базові правила безпеки в цифровому середовищі) – курс, який складається з 10 модулів загальною тривалістю 60 хвилин. У курсі розкриваються поняття інформаційної безпеки, найбільш важливі для пересічних користувачів. У ньому описані основні загрози в інформаційному просторі та базові методи протидії цим загрозам [12].

13. Єшко – платний курс з підтримкою кураторів та домашніми завданнями [13].

Отже, аналізуючи порівняльну таблицю, можна зробити висновок: існує досить багато засобів оцінки кібергігієни, та зовсім не розвинений напрямок кібергігієни на підприємствах, тому розробка даної системи є актуальною та корисною для загальної безпеки України.

1.3 Формалізація вимог та постановка задач

Виходячи з наведеної вище інформації, приходимо до висновку, що доцільним буде створення власної системи оцінки рівня кібергігієни особи шляхом тестування. На будь-якому підприємстві працівники проходять інструктажі з охорони праці та техніки безпеки на робочому місці. Виходячи з наведеної вище статистики втрат на підприємствах по причині людського фактору, буде доцільним додати до інструктажів дану технологію оцінювання рівня кібергігієни особи. Оскільки використання певних технологій варіюється в залежності від посади працівника, необхідно надати можливість обирати ті модулі тестування, з якими потрібно буде працювати в майбутньому. Також потрібно ввести шкалу оцінювання рівня знань, щоб аналізувати та прогнозувати подальші дії. Також це дозволить відстежувати динаміку знань користувачів, так як результати зберігатимуться у базі даних. Інструктор зможе створювати статистику по кожному працівнику та надавати йому матеріали за слабкими темами.

Реалізовано можливість створити акаунт адміністратора, за допомогою якого можна створювати нові модулі, редагувати та видаляти існуючі. Оскільки напрямки роботи підприємства можуть змінюватись та з’являтимуться нові посади, необхідно мати можливість легко додавати до системи нові теми та запитання. Після проходження тесту користувачеві виводиться результат та посилання на навчальні матеріали з темами, в яких було зроблено найбільше помилок.

2 РОЗРОБКА ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ

2.1 Структура інформаційної технології

Інформаційна технологія визначення рівня кібергігієни особи складається з декількох процесів, кожен з яких має власне функціональне призначення. Схема процесів інформаційної технології наведена на рис. 2.1.

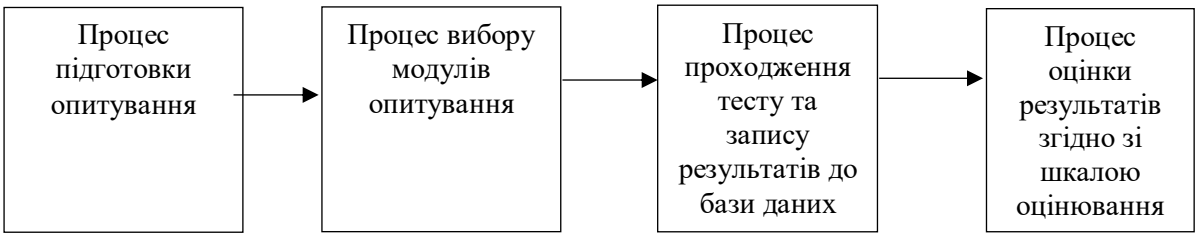

Рисунок 2.1 – Схема процесів інформаційної технології

Розглянемо окремо кожен процес.

1) Процес підготовки опитування

Перед початком опитування формується список запитань з різних напрямків кібергігієни та за допомогою режиму адміністратора вноситься в систему.

Отже, буде доступний вибір модулів, згідно з вищенаведеним списком:

- кібергігієна паролів;
- кібергігієна персонального комп’ютера;
- кібергігієна мобільних пристроїв;
- кібергігієна електронної пошти;
- кібергігієна соцмереж та месенджерів;
- кібергігієна електроних платежів;
- кібергігієна технології Wi-Fi;
- кібергігієна споживання інформації;
- соціальна інженерія.

Всі питання є тестовими або ситуаційними, що дозволяє детально охопити обізнаність працівників в певних напрямках кібергігієни.

2) Процес вибору модулів опитування.

Оскільки кожна посада має різні посадові обов'язки, доцільною є розробка можливості вибору модулів опитування. Тобто, якщо співробітник не працює с електронною поштою, то немає сенсу оцінювати рівень кібергігієни в цій темі.

Також додані запитання на специфічні та вузьконаправлені теми для актуальності системи для будь-якої посади працівника.

Список запитань та варіантів відповіді наведено в додатку А.

Також, реалізована можливість редагування модулів, додавання та видалення запитань з кожного модуля, з урахуванням швидкого розвитку технологій, це забезпечить актуальність додатку для тестування.

Нижче наведено таблицю відповідності напрямків кібергігієни з найбільш ключовими посадами на будь-якому підприємстві (табл.2.1).

Таблиця 2.1 – Відповідність посади до напрямків кібергігієни

Напрямок / Посада	Паролі	Персональний комп'ютер	Мобільні пристрої	Електронна пошти	Соцмережі та месенджерів	Електронні платежі	Технологія WI-FI	Споживання інформації	Соціальна інженерія
Бухгалтер	+	+	-	+	-	+	+	+	+
Менеджер	+	+	+	+	+	-	+	+	+
Рекрутер	+	+	+	+	+	-	+	+	+
Секретар	+	+	+	+	-	-	+	+	+
Юрист	+	+	-	+	-	-	+	+	+

3) Процес проходження тесту та запису результатів до бази даних.

Проходження тесту передбачає певну кількість випадкових запитань з кожного модуля.

База даних із запитаннями буде реалізована за допомогою SQLite, що дасть змогу легко корегувати модулі, додавати та видаляти запитання або ж додавати нові модулі за необхідністю.

Також створена база даних з матеріалами для підготовки, якщо особа пройшла тестування на недостатньому рівні, що включає в себе посилання на статі та навчальні відео. База даних навчальних матеріалів також може легко оновлюватись, система передбачає можливість додавання нових записів.

Кожне проходження тесту створюватиме окремий протокол з результатами, до якого входитимуть:

- ПІБ кандидата;
- посада кандидата;
- список пройдених запитань;
- обраний варіант відповіді на запитання;
- позначка правильності відповіді;
- кінцева оцінка рівня кібергігієни.

4) Процес оцінки результатів згідно зі шкалою оцінювання.

Для підрахунку оцінки використовується наступна математична модель:

$$O_{test} = \sum_{i=1}^{n} W_i * S_i,$$

де W_i – вага і-го модуля/напрямку кібергігієни (можуть бути різними в залежності від критичності для кожної посади), S_i – кількість правильних відповідей, що набрав працівник в і-му модулі.

Вага кожного запитання 0 або 1, де 0 це неправильна відповідь, 1 – правильна. Вага модулів для тестування конкретного працівника в сумі дорівнює 1. Тобто, якщо обрано 3 модуля, то вага кожного автоматично становить 0,33, або ж є можливість налаштовувати вагу модулів вручну. Наприклад, було обрано 3 модуля і в першому 1 правильна відповідь, в другому 3, в третьому 2. Вагу модуля налаштовано таким чином, що коефіцієнт першого становить 0,2, другого - 0,4, третього 0,4. Тоді оцінка дорівнює:

$$O_{test} = 0{,}2 * 1 + 0{,}4 * 3 + 0{,}4 * 2 = 2{,}2.$$

Максимальне ж значення при таких умовах дорівнює:

$$O_{max} = 0{,}2 * 3 + 0{,}4 * 3 + 0{,}4 * 3 = 3,$$

Тоді оцінку рівня кібергігієни у відсотковому вираженні можна представити таким чином:

$$О = \frac{О_{test}}{О_{max}} = \frac{2,2}{3} = 73,3\%$$

Тобто, в такому випадку кінцева оцінка користувача – С згідно з таблицею оцінювання (табл. 2.1), та особа недопущена до роботи, рекомендується повторне проходження тесту та вивчення навчальних матеріалів.

Після проходження тесту буде автоматично пораховано та виведено на екран користувача загальний відсоток правильних відповідей та отриманий бал.

Таблиця 2.2 – Шкала оцінювання рівня кібергігієни особи

Рівень знань	Відсоток правильних відповідей	Оцінка	Рекомендації
Низький	До 60%	D	Особа має низький рівень кібергігієни та не допущена до роботи.
Середній	60-74%	C	Особа має середній рівень кібергігієни та недопущена до роботи, рекомендується проходження курсу з інструктором та повторне проходження тесту.
Достатній	75-89%	B	Особа має достатній рівень кібергігієни та допущена на

Продовження таблиці 2.2

			посаду після проходження тренінгу з інструктором.
Високий	90-100%	A	Особа має високий рівень кібегігієни та допущена на посаду.

Якщо кандидат отримав оцінку А – він допускається до роботи з відповідними засобами, сервісами та інформаційними ресурсами. Якщо отримав оцінку В, тоді інструктор приймає рішення, згідно з критичністю посади та напрямків, в яких кандидат зробив найбільше помилок.

Кандидати с оцінками D і С не допущені до роботи та рекомендовані до перегляду навчальних матеріалів з подальшим перескладанням тесту.

Система аналізує слабкі місця знань кандидата на посаду, виходячи з порівняння ваги модулів, та виводить на екран посилання на навчальні матеріали та ресурси, які допоможуть особі краще підготуватись до наступного проходження тесту.

2.2 Розробка архітектури системи

Інформаційна технологія оцінювання рівня кібергігієни особи включає в себе комплекс методів, моделей та програмного забезпечення. Архітектура даної системи наведена на рис. 2.2.

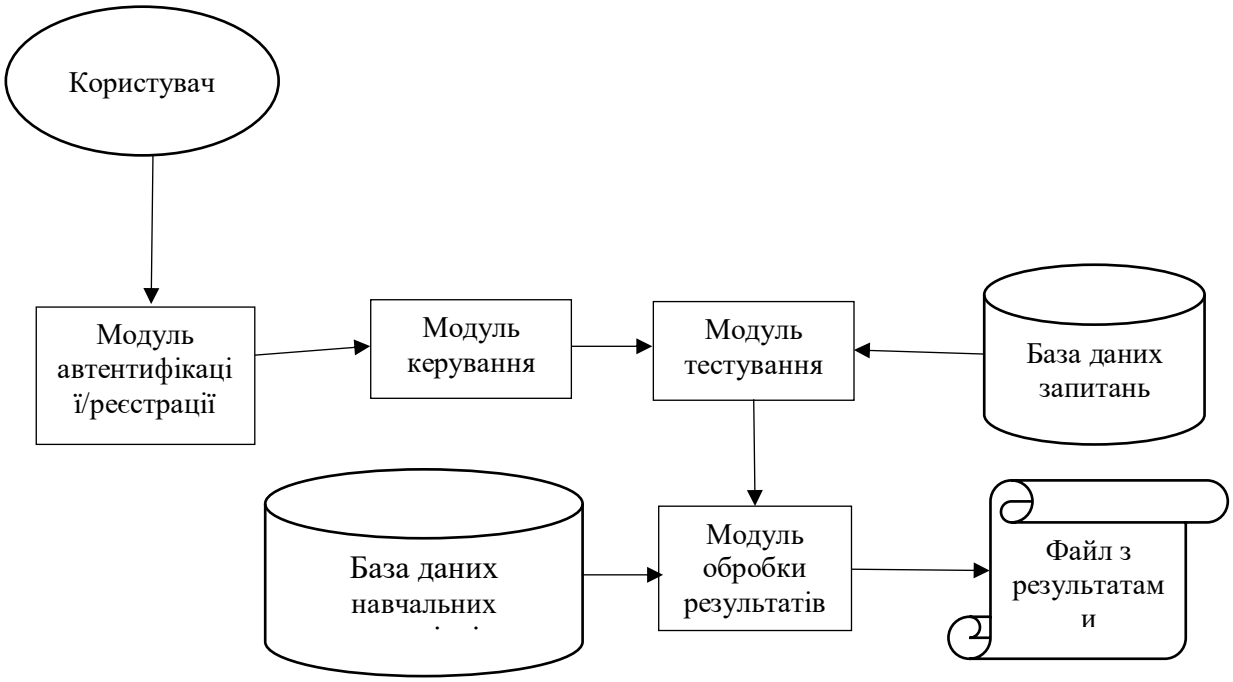

Рисунок 2.2 – Схема архітектури системи

Розглянемо кожен модуль системи окремо.

1) Модуль автентифікації/реєстрації.

Користувач вводить свій логін та пароль в графічному інтерфейсі.

Система перевіряє ці дані в базі даних. Якщо дані вірні, користувач отримує доступ до системи.

У випадку невірних даних, користувач повідомляється про помилку.

Реєстрація:

Новий користувач натискає кнопку "Реєстрація" та вводить свої особисті дані та обирає унікальний логін та пароль.

Система перевіряє, чи логін є унікальним. Якщо так, то користувач реєструється, і йому надається доступ до системи.

Рисунок 2.3 – Схема роботи модуля автентифікації/реєстрації

2) Модуль керування.

Даний модуль починає роботу одразу після запуску програмного засобу, і надає користувачеві графічний інтерфейс для взаємодії з програмним засобом. Модуль також виконує функції відображення діалогових вікон та результатів роботи програми.

Графічний інтерфейс:

Забезпечує зручний та естетичний інтерфейс для користувача.

Включає меню, кнопки та інші елементи для навігації та взаємодії з іншими модулями.

3) Модуль тестування.

Даний модуль відповідає за вибір випадкових запитань для користувача з обраних тем, представлення даних користувачу, визначення правильних відповідей та навігацію по модулям.

Модуль тестування взаємодіє з інструктором або адміністратором, який визначає категорії тестів в залежності від специфіки роботи працівника або того, з чим він буде працювати. Цей модуль дозволяє персоналізувати тести для максимально ефективного вимірювання рівня обізнаності працівників у конкретних аспектах кібергігієни.

Процес роботи модуля тестування виглядає наступним чином:

- Консультація з інструктором:

Інструктор або адміністратор визначає конкретні категорії тестів, що відповідають вимогам конкретної професії чи виду діяльності працівника.

- Вибір категорій тестів:

Інструктор вибирає з бази даних категорії тестів, які найкраще відображають основні виклики та завдання, з якими працівник може стикатися в своїй роботі.

- Опціональне визначення специфічних тестів:

Інструктор може вибрати конкретні тести або завдання, які відображають специфічні аспекти та сценарії, що важливі для даної групи працівників.

- Надсилання тестів працівнику:

Система надсилає підготовлені тести працівникові через графічний інтерфейс.

- Виконання тестів працівником:

Користувач взаємодіє з графічним інтерфейсом для вирішення тестових завдань, які можуть включати запитання, сценарії чи інші завдання кібергігієни

- Збір результатів:

Система збирає відповіді та результати від працівника.

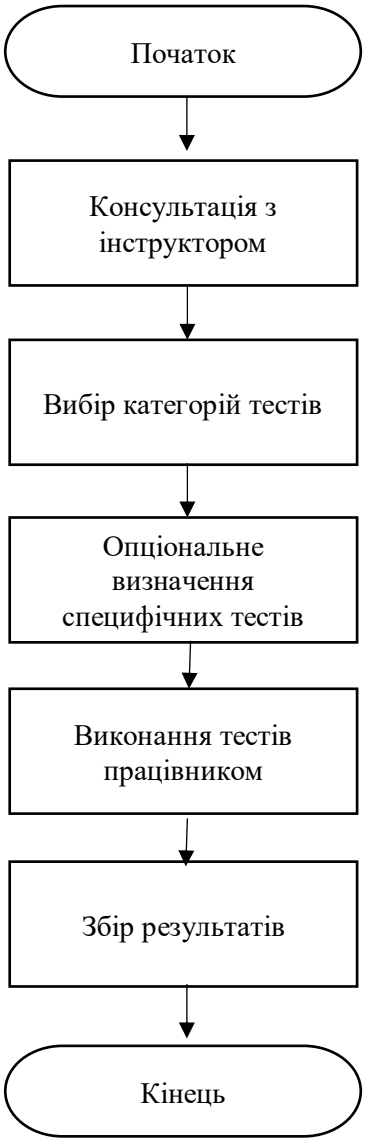

Рисунок 2.4 – Схема роботи модуля керування

Приклад:

Сфера діяльності: Банківський працівник.

Категорії тестів: Кібербезпека електроних платежів, Кібербезпека паролів.

Такий підхід дозволяє системі точно визначити, які аспекти кібергігієни є найбільш критичними для конкретного працівника та відповідно персоналізувати тести для максимально ефективного оцінювання його знань.

4) Модуль обробки результатів.

Даний модуль виконує наступні операції:

- експорт відповідей в окремий файл;
- підрахунок відсотка правильних відповідей та формування кінцевої оцінки;
- вивід результатів на екран користувача.

Якщо результати показують недостатній рівень знань, система може генерувати повідомлення або рекомендації щодо покращення знань користувача.

Модуль обробки результатів відіграє ключову роль у визначенні рівня кібергігієни працівника та визначенні напрямків для подальшого вдосконалення. Робота модуля включає в себе кілька етапів:

- Підрахунок рівня кібергігієни:

Модуль аналізує відповіді працівника на тести з врахуванням визначених категорій та ваги питань.

- Визначення напрямків помилок:

Якщо рівень кібергігієни працівника недостатній, модуль аналізує відповіді на окремі тести та визначає напрямки, в яких допущено найбільше помилок.

Напрямки можуть включати аспекти такі як захист паролів, визнання фішингових атак, використання антивірусного програмного забезпечення та інші.

- Пропозиції щодо вдосконалення:

Система генерує рекомендації та пропозиції для підвищення рівня кібергігієни працівника.

Враховуються конкретні аспекти, в яких виявлено слабкість, і пропонуються ресурси для самонавчання.

- Посилання на навчальні ресурси:

Система надає посилання на текстові, відео- або графічні матеріали, які відповідають конкретним напрямкам, в яких працівник допустив помилки.

Ці матеріали можуть бути внутрішніми навчальними ресурсами або посиланнями на зовнішні інформаційні ресурси.

- Заплановане навчання:

Система може автоматично створити заплановане навчання для працівника, розгортане в часі, щоб він мав можливість повторно та систематично вдосконалювати свої знання в певних аспектах кібергігієни.

- Звіти і статистика:

Модуль генерує звіти та статистику, яка може бути використана для відслідковування прогресу працівника та оцінки ефективності програми навчання в цілому.

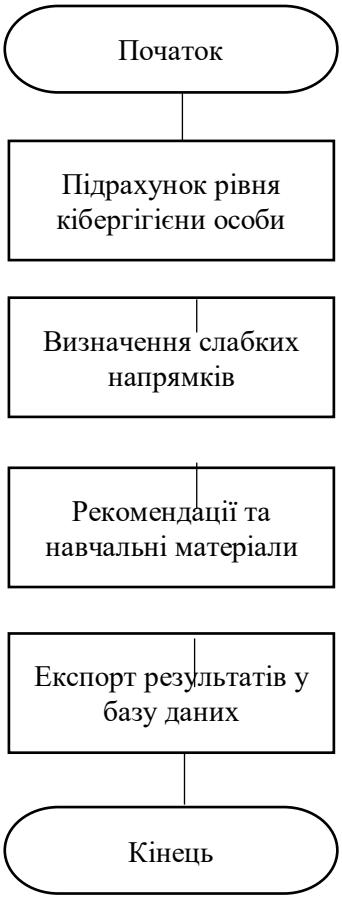

Рисунок 2.5 – Схема роботи модуля обробки результатів

Приклад:

Проходження тестів вказало на слабкість працівника в розділі "Кібербезпека паролів".

Модуль обробки результатів генерує рекомендації та пропозиції для вдосконалення знань у цьому напрямку.

Система надає посилання на відео-уроки та інтерактивні матеріали з теми "Створення безпечних паролів та їх збереження".

Пропонується запланованe навчання з цього конкретного аспекту, розподілене в часі для поступового покращення навичок.

5) База даних

Зберігання тестових завдань:

База даних утримує широкий спектр тестових завдань із кібергігієни, категоризованих для зручного вибору користувачем.

Навчальні матеріали:

Утримує навчальні ресурси, які можуть бути автоматично або рекомендовано надавати працівнику для підвищення його рівня обізнаності.

Результати оцінювання:

Записує результати тестування та оцінювання, щоб надати історію та можливість відстеження прогресу користувача в часі.

Модуль ведення бази даних (ВБД) в контексті системи для оцінки кібергігієни працівника грає важливу роль в зберіганні та обробці інформації, яка виникає під час взаємодії користувачів із системою. Давайте розглянемо принципи роботи цього модуля в контексті взаємодії з іншими модулями системи:

- Модуль автентифікації/реєстрації:

В момент реєстрації нового користувача модуль автентифікації/реєстрації взаємодіє з ВБД для додавання нового запису в таблицю "Users".

При автентифікації користувача модуль перевіряє введений логін та пароль, звертаючись до ВБД.

- Модуль керування:

Модуль керування використовує дані з таблиці "Users" для відображення інформації про користувача у графічному інтерфейсі.

- Модуль тестування:

При виборі категорій тестів модуль тестування звертається до ВБД для вибору тестів відповідно до обраних категорій, переглядаючи таблиці "TestCategories" та "Tests". Результати тестування записуються в таблицю "UserTestResults" для подальшого аналізу.

- Модуль обробки результатів:

Після завершення тестування модуль обробки результатів звертається до ВБД для аналізу даних в таблиці "UserTestResults".

Проводиться оцінка рівня кібергігієни, визначаються напрямки, в яких користувач може покращити свої навички.

За необхідності виводяться рекомендації та звертання до навчальних ресурсів, які також знаходяться в ВБД (таблиця "LearningResources").

- Модуль навчання:

Модуль навчання використовує дані з таблиці "LearningResources" для надання користувачеві відповідного навчального матеріалу.

Модуль ведення бази даних є основним елементом, з яким взаємодіють інші модулі системи. Даний підхід дозволяє системі ефективно керувати інформацією, а також реалізувати розширення та підтримку нових функцій в майбутньому.

2.3 Формування переліку запитань

Сформовано перелік запитань тесту згідно з вищенаведеними темами.

Всі запитання є запитаннями закритого типу, з однією правильною відповіддю. Частина запитань є теоретичними, інші ж – ситуаційні запитання, з якими працівник може найчастіше зустрічатись у процесі роботи на підприємстві або поза ним. Це дозволяє аналізувати основні проблеми з обізнанністю користувачів, а самі кандидати точно знатимуть, як саме їм слід вчинити у подібній ситуації. Кількість запитань при тестуванні фіксована, з кожного напрямку по 5 запитань, обраних системою випадковим чином.

Повний перелік запитань наведено у додатку Б.

1. Кібергігієна паролів

Даний модуль містить запитання на тему правильного використання паролів, адже кожен працівник незалежно від посади має безліч систем захищених паролем, як на робочому місці, так і поза ним.

Питання: Який вид паролю вважається більш безпечним?

a) Пароль123

b) !2#Gp$Xm

c) Користувач

d) 123456

Відповідь: b) !2#Gp$Xm

Питання: Як можна покращити запам'ятовування складних паролів?

a) Використання того самого паролю для різних облікових записів

b) Запис паролів на стікерах та клейках паперів

c) Використання парольних менеджерів

d) Зберігання паролів у недоступному для інших місці

Відповідь: c) Використання парольних менеджерів

Ситуація: Ваш колега залишив комп'ютер включеним і невимкненим на кілька годин. Як ви реагуєте щодо захисту паролю?

a) Нічого не роблю

b) Змінюю пароль

c) Повідомляю керівництво

d) Змінюю пароль і підказую колегові

Відповідь: b) Змінюю пароль

Ситуація: Ви отримали лист від сервісу електронної пошти про підозрілу активність у вашому обліковому записі. Що ви робите?

a) Клікаю на посилання у листі та вводжу пароль

b) Ігнорую лист

c) Заходжу на веб-сайт сервісу електронної пошти, не використовуючи посилання

d) Видаляю лист

Відповідь: c) Заходжу на веб-сайт сервісу електронної пошти, не використовуючи посилання

2. Кібергігієна мобільних пристроїв

Даний напрямок кібергігієни є надзвичайно актуальним для системи оцінювання, адже більшість посад певним чином пов'язані з використанням мобільних пристроїв.

Питання: Яким чином двофакторна аутентифікація забезпечує додатковий рівень безпеки на мобільних пристроях?

a) Забезпечує шифрування файлів

b) Вимагає двох різних мобільних пристроїв

c) Використовує два різних методи аутентифікації

d) Змінює пароль двічі на місяць

Відповідь: c) Використовує два різних методи аутентифікації

Питання: Яка загроза може виникнути при використанні відкритого Wi-Fi на мобільному пристрої?

a) Затримка в роботі додатків

b) Зменшення рівня заряду батареї

c) Витік особистих даних через непрошений доступу до мережі

d) Втрата файлів з пристрою

Відповідь: c) Витік особистих даних через непрошений доступу до мережі

Ситуація: Під час користування відкритим Wi-Fi ви помітили незвичайну активність на своєму мобільному пристрої. Як ви реагуєте?

a) Продовжу користуватися мережею, ігноруючи незвичайну активність

b) Відключу Wi-Fi і перейду на мобільний інтернет

c) Запитаю персонал кафе щодо стану їхньої мережі

d) Завершу всі сеанси та вимкну Wi-Fi

Відповідь: d) Завершу всі сеанси та вимкну Wi-Fi.

3. Кібергігієна електронної пошти

До цього модулю увійшли запитання та ситуаціїї на тему правильного та безпечного використання поштових сервісів, адже майже кожна посада на підприємствах включає в себе спілкування у форматі електроних поштових листів.

Питання: Як можна забезпечити безпеку паролів для доступу до електронної пошти?

a) Використання простих та загальних паролів

b) Регулярна зміна паролів

c) Відправка паролів по електронній пошті

d) Зберігання паролів у відкритому тексті

Відповідь: b) Регулярна зміна паролів

Ситуація: Співробітник отримав лист від невідомого відправника з проханням надати конфіденційну інформацію. Яким чином слід вчинити?

a) Негайно відправити запитання на визначення особистості відправника

b) Надати запитувану інформацію без будь-якої перевірки

c) Залишити лист без відповіді

d) Повідомити відділ безпеки про подію для подальшого аналізу

Відповідь: d) Повідомити відділ безпеки про подію для подальшого аналізу

Ситуація: Керівник підприємства отримав лист з вимогою великої суми грошей в обмін на відновлення доступу до важливих даних. Як вчинити?

a) Негайно відправити велику суму грошей для відновлення доступу

b) Вимагати докази автентичності вимог та повідомити відділ безпеки

c) Проігнорувати вимоги та спробувати вирішити проблему самостійно

d) Передати всі дані, які вимагаються, для відновлення доступу

Відповідь: b) Вимагати докази автентичності вимог та повідомити відділ безпеки

4. Кібергігієна соцмереж та месенджерів

Даний модуль підіймає питання безпеки соцмереж, так як на кожному підприємстві є корпоративні та особисті чати в різних месенджерах та соцмережах, що підвищує ризик втрати важливої конфідеційної інформації.

Питання: Як захистити особистий обліковий запис в соціальній мережі від несанкціонованого доступу?

a) Використовувати один пароль для всіх соціальних мереж

b) Застосувати двоетапну аутентифікацію

c) Зберігати паролі на папері поблизу робочого місця

d) Публікувати пароль у власному профілі для власного запам'ятовування

Відповідь: b) Застосувати двоетапну аутентифікацію

Питання: Як забезпечити конфіденційність обговорень у корпоративних чатах?

a) Відправляти конфіденційну інформацію у відкритому тексті

b) Застосування шифрування чатів та повідомлень

c) Надсилання паролів для доступу до файлів через чат

d) Відкрита публікація обговорень в корпоративних чатах

Відповідь: b) Застосування шифрування чатів та повідомлень

Ситуація: Співробітник отримав від невідомого контакту в месенджері посилання на файлообмінник із проханням завантажити важливий файл. Як вчинити?

a) Відразу завантажити файл без будь-яких перевірок

b) Звернутися до відділу безпеки для перевірки посилання

c) Ігнорувати повідомлення та видалити контакт

d) Надіслати запитання невідомому контакту про його ідентифікацію

Відповідь: b) Звернутися до відділу безпеки для перевірки посилання

Ситуація: Керівник отримав від колеги запитання в месенджері про конфіденційну стратегічну інформацію компанії. Як вчинити?

a) Відразу відправити всю необхідну інформацію

b) Вимагати офіційного запиту через корпоративну пошту або інші безпечні канали

c) Направити запитання керівництву для визначення дій

d) Попросити колегу відправити запитання через електронну пошту для більшої безпеки

Відповідь: b) Вимагати офіційного запиту через корпоративну пошту або інші безпечні канали

5. Кібергігієна електроних платежів

Питання: Як можна захистити особисті фінансові дані під час електронних платежів?

a) Використання одного пароля для всіх електронних платформ

b) Використання безпечних і складних паролів для кожного облікового запису

c) Надсилання фінансових даних через звичайні текстові повідомлення

d) Зберігання всіх фінансових паролів на пристрої без паролю

Відповідь: b) Використання безпечних і складних паролів для кожного облікового запису

Питання: Як використовувати публічні Wi-Fi мережі безпечно під час здійснення електронних платежів?

a) Використовувати тільки особистий мобільний інтернет

b) Заборона використання будь-яких публічних Wi-Fi для платежів

c) Використання віртуальної приватної мережі (VPN)

d) Надсилання фінансових даних без шифрування

Відповідь: c) Використання віртуальної приватної мережі (VPN)

Ситуація: Користувач отримав електронне повідомлення про підозрілу транзакцію на своєму банківському рахунку. Як слід вчинити?

a) Проігнорувати повідомлення, оскільки це, ймовірно, шахрайська атака

b) Негайно звернутися до банку для перевірки та блокування неправомірних транзакцій

c) Видалити всі фінансові деталі з облікового запису

d) Надіслати всі фінансові дані у відповідь на це повідомлення

Відповідь: b) Негайно звернутися до банку для перевірки та блокування неправомірних транзакцій

Ситуація: Користувач випадково надіслав гроші невідомому одержувачеві через електронну платіжну платформу. Як вирішити цю ситуацію?

a) Намагатися скасувати транзакцію самостійно

b) Негайно повідомити платіжну платформу та звернутися до служби підтримки

c) Ігнорувати ситуацію, оскільки нічого не можна змінити

d) Вимагати повернення грошей у невідомого одержувача

Відповідь: b) Негайно повідомити платіжну платформу та звернутися до служби підтримки

6. Кібергігієна технології WI-FI

Дана технологія наразі використовується всюди, на підприємствах та в домашніх умовах, тому важливо правильно користуватись мережею Інтернет та вміти уникнути найбільш популярних атак.

Питання: Як можна забезпечити безпеку власної домашньої Wi-Fi мережі?

a) Використання стандартного пароля, наданого провайдером

b) Зміна пароля за замовчуванням та використання складного пароля WPA2 або WPA3

c) Вимкнення всіх методів шифрування для забезпечення високої швидкості

d) Надсилання паролю всім сусідам для спільного використання мережі

Відповідь: b) Зміна пароля за замовчуванням та використання складного пароля WPA2 або WPA3

Питання: Як виявити, чи використовуються моєю Wi-Fi мережею несанкціоновані пристрої?

a) Періодично змінювати пароль для виключення доступу несанкціонованих пристроїв

b) Використовувати функцію моніторингу підключених пристроїв у налаштуваннях маршрутизатора

c) Включити режим гостьової мережі для ізоляції несанкціонованих пристроїв

d) Вимагати від кожного пристрою сканувати QR-код для підключення до мережі

Відповідь: b) Використовувати функцію моніторингу підключених пристроїв у налаштуваннях маршрутизатора

Ситуація: Користувач помітив підозрілу активність у своєму списку підключених пристроїв до мережі. Як вчинити?

a) Ігнорувати ситуацію, оскільки це може бути звичайний збій мережі

b) Змінити пароль мережі і відключити всі пристрої, крім дозволених

c) Надсилати підозрілому пристрою запитання про його призначення

d) Припинити використання Wi-Fi та виключити маршрутизатор для додаткової безпеки

Відповідь: b) Змінити пароль мережі і відключити всі пристрої, крім дозволених

7. Кібербезпека споживання інформації

Питання: Як розпізнати фейкові новини та перевірити достовірність інформації в Інтернеті?

a) Вірити кожній новині, яка виглядає цікаво

b) Перевіряти джерело інформації та шукати підтвердження від інших надійних джерел

c) Ділитися будь-якою інформацією без перевірки

d) Визначати достовірність інформації за кількістю лайків та репостів

Відповідь: b) Перевіряти джерело інформації та шукати підтвердження від інших надійних джерел

Питання: Як забезпечити приватність в Інтернеті під час споживання новин та контенту?

a) Використовувати тільки відкриті профілі в соціальних мережах

b) Забороняти доступ до персональних даних на всіх веб-сайтах

c) Використання VPN та інших інструментів для шифрування інтернет-з'єднання

d) Публікувати всю особисту інформацію в мережі для більшої доступності

Відповідь: c) Використання VPN та інших інструментів для шифрування інтернет-з'єднання

Ситуація: Користувач отримав посилання на електронну пошту, яке здається підозрілим. Як вчинити?

a) Негайно клікнути на посилання для отримання додаткової інформації

b) Відправити електронного листа в спам та видалити його

c) Перевірити відправника та адресу посилання перед відкриттям

d) Відправити всі свої особисті дані у відповідь на це електронне повідомлення

Відповідь: c) Перевірити відправника та адресу посилання перед відкриттям

8. Кібергігієна персонального комп’ютера

Питання: Як забезпечити безпеку віддаленого доступу до персонального комп'ютера?

a) Включення безпечного режиму віддаленого доступу та використання слабкого пароля

b) Відмова від віддаленого доступу для заощадження енергії

c) Використання найпростіших паролів для віддаленого доступу

d) Встановлення двофакторної аутентифікації та регулярне оновлення паролів

Відповідь: d) Встановлення двофакторної аутентифікації та регулярне оновлення паролів

Ситуація: Користувач помітив підозрілі активності на своєму комп'ютері, що може вказувати на вторгнення. Як вчинити?

a) Продовжити роботу та ігнорувати підозрілу активність

b) Вимкнути комп'ютер та звернутися до інформаційно-технічного відділу

c) Змінити паролі та видалити всі важливі дані

d) Відправити повідомлення хакерам з проханням припинити вторгнення

Відповідь: b) Вимкнути комп'ютер та звернутися до інформаційно-технічного відділу

Ситуація: Користувач помітив, що його веб-камера активується без його дозволу. Як вчинити для захисту приватності?

a) Продовжувати використовувати комп'ютер, оскільки це може бути звичайний збій

b) Пошукати та вимкнути всі процеси, які активують веб-камеру без дозволу

c) Заклеїти веб-камеру стрічкою чи спеціальними наклейками

d) Відправити запит до виробника комп'ютера для вирішення проблеми

Відповідь: b) Пошукати та вимкнути всі процеси, які активують веб-камеру без дозволу

2.4 Розробка рекомендацій за напрямками кібергігієни

Нижче наведено рекомендації для забезпечення безпеки підприємств за кожним напрямком кібергігієни.

1) Кібергігієна паролів

Базові рекомендації для забезпечення високого рівня кібергігієни паролів на підприємствах:

- вимагайте від працівників використовувати паролі з достатньою довжиною (рекомендації зазвичай становлять принаймні 12 символів).

Заохочуйте використання різноманітних символів, таких як великі та маленькі літери, цифри та спецсимволи.

- вимагайте від працівників використовувати унікальні паролі для кожного облікового запису. Заохочуйте використання менеджерів паролів, які дозволяють безпечно зберігати та генерувати складні паролі.

- уникайте використання очевидних інформаційних елементів у паролях, таких як ім'я користувача, дата народження, інформація з соціальних мереж тощо.

- встановлюйте політику періодичної зміни паролів (наприклад, кожні 90 днів). Уникайте повторного використання старих паролів.

- встановлюйте двоетапну або багатоетапну автентифікацію для додаткового рівня безпеки.

- надавайте регулярне навчання щодо кібербезпеки та безпечного створення та зберігання паролів. Поясніюйте небезпеку використання одного паролю для всіх служб та ресурсів.

- використовуйте системи виявлення аномальної поведінки для виявлення непередбачуваних або небезпечних змін у користувацьких аккаунтах.

- забезпечте шифрування паролів у базі даних, щоб ускладнити їх злам.

- встановіть механізми блокування облікових записів після кількох невдалих спроб введення пароля для запобігання брутфорс-атакам.

- ведіть аудит активності користувачів та моніторте події, щоб вчасно виявляти надзвичайні ситуації.

Розроблення та виконання чіткої політики безпеки паролів може суттєво знизити ризик неправомірного доступу та забезпечити безпеку підприємства [14].

2) Кібергігієна мобільних пристроїв

Забезпечення кібергігієни мобільних пристроїв на підприємстві є критичним для захисту від кіберзагроз та забезпечення конфіденційності та

цілісності інформації [14]. Базові рекомендації для підприємств у цьому контексті:

- захищайте доступ до мобільних пристроїв паролями або біометричними даними (відбитками пальців, розпізнаванням обличчя). Вимагайте від працівників використовувати складні паролі та періодично їх змінювати.

- використовуйте шифрування для захисту даних на мобільних пристроях, особливо якщо вони містять конфіденційну чи корпоративну інформацію.

- встановлюйте тільки довірені додатки з офіційних магазинів (Google Play, App Store). Використовуйте системи управління мобільними пристроями (Mobile Device Management, MDM) для контролю додатків та віддаленого видалення у випадку втрати чи крадіжки пристрою.

- активуйте автоматичне оновлення для операційних систем та додатків для забезпечення останніх заходів безпеки.

- захищайте корпоративні дані за допомогою віртуальної приватної мережі (VPN) для шифрування з'єднань на мобільних пристроях.

- уникайте підключення до ненадійних та невідомих мереж Wi-Fi. Використовуйте тільки захищені мережі із застосуванням WPA3 або WPA2 шифрування.

- встановлюйте функції віддаленого видалення та блокування для втрачених або викрадених пристроїв. Заохочуйте негайне повідомлення про втрату або крадіжку мобільних пристроїв.

- проводьте регулярні навчання щодо безпеки мобільних пристроїв та усвідомлення загроз. Пояснюйте правила використання мобільних пристроїв та обов'язкові заходи безпеки.

- вимагайте від працівників вимикати непотрібні функції (Bluetooth, NFC, GPS) під час роботи.

- використовуйте системи виявлення загроз для моніторингу діяльності на мобільних пристроях та виявлення надзвичайних ситуацій.

Ці заходи допоможуть підприємствам створити безпечне середовище для використання мобільних пристроїв та зменшити ризики витоку чи втрати конфіденційної інформації.

3) Кібергігієна електронної пошти

Забезпечення кібергігієни електронної пошти є важливим аспектом кібербезпеки підприємств оскільки електронна пошта залишається однією з основних напрямків атак [15]. Базові рекомендації для підприємств:

- використовуйте потужні антивірусні та антиспамові фільтри для виявлення та блокування шкідливих листів та спаму.

- встановлюйте шифрування для електронних листів, особливо якщо вони містять конфіденційну інформацію.

- активуйте двоетапну або багатоетапну аутентифікацію для підвищення рівня безпеки облікових записів електронної пошти.

- проводьте навчання та свідомість щодо фішингових атак, особливо тих, що стосуються електронної пошти.

- заохочуйте працівників перевіряти джерела та вміст електронних листів перед тим, як взяти в них участь.

- встановлюйте політику щодо строку дії паролів для забезпечення регулярної їх зміни.

- захищайте мережу, щоб уникнути несанкціонованого доступу до електронної пошти.

- використовуйте мережеві фільтри для блокування небезпечних вкладень та веб-посилань у листах.

- використовуйте інструменти для моніторингу та виявлення можливих витоків конфіденційної інформації через електронну пошту.

- ведіть аудит активності електронної пошти та моніторте небезпечні події, щоб вчасно виявляти атаки.

- регулярно резервуйте електронну пошту для відновлення в разі втрати даних внаслідок атак або інших непередбачених ситуацій.

- захищайте електронну пошту на мобільних пристроях за допомогою антивірусів, шифрування та інших заходів безпеки.

- встановлюйте правила щодо використання особистої електронної пошти на корпоративних пристроях та в мережі підприємства.

Ці рекомендації допоможуть підприємствам захистити свою електронну пошту від різних кіберзагроз та зберегти конфіденційність корпоративної інформації.

4) Кібергігієна соцмереж та месенджерів

Забезпечення кібергігієни у використанні соціальних мереж та месенджерів на підприємстві є важливим елементом кібербезпеки. Базові рекомендації для підприємств:

- встановіть чітку політику використання соціальних мереж на робочих пристроях та в мережі підприємства.

- реагуйте швидко на інциденти у соціальних мережах та моніторте їх для виявлення потенційних загроз.

- регулюйте рівні доступу до соціальних мереж залежно від ролі та обов'язків працівників.

- надавайте навчання з безпеки використання соціальних мереж, включаючи розпізнавання фішингу та соціально-інженерних атак.

- моніторте зовнішню активність працівників у соцмережах та реагуйте на недоречні публікації або витоки інформації.

- використовуйте месенджери, які підтримують шифрування повідомлень для захисту конфіденційної інформації.

- керуйте доступом до корпоративних месенджерів, встановлюючи чіткі політики та періодично переглядаючи облікові записи.

- вимагайте від працівників активувати двоетапну або багатоетапну аутентифікацію для месенджерів.

- використовуйте фільтри для обмеження небажаної комунікації та виявлення можливих загроз.

- заохочуйте працівників не використовувати особисті облікові записи для робочих цілей у корпоративних месенджерах.

- проводьте навчання щодо безпеки користування месенджерами та відсилання файлів.

- моніторте та аналізуйте файли та посилання, що відправляються через месенджери, для виявлення можливих загроз.

- забезпечуйте безпеку мобільних пристроїв, на яких встановлені корпоративні месенджери, за допомогою антивірусів та шифрування.

Впровадження цих заходів допоможе підприємствам зменшити ризики витоку конфіденційної інформації та інших кіберзагроз, пов'язаних із використанням соціальних мереж та месенджерів [15].

5) Кібергігієна електронних платежів

Забезпечення кібергігієни електронних платежів важливо для підприємств, щоб уникнути фінансових втрат та зберегти конфіденційність та цілісність фінансових даних. Базові рекомендації для підприємств у цьому контексті:

- вибирайте відомі та визнані платіжні системи та платформи, які відповідають вимогам стандартів безпеки, таких як PCI DSS.

- захищайте фінансові дані за допомогою шифрування під час передачі і зберігання. Використовуйте безпечні протоколи (наприклад, HTTPS) для забезпечення шифрування.

- застосовуйте двоетапну або багатоетапну аутентифікацію для підтвердження особи, яка здійснює фінансову транзакцію.

- проводьте регулярні аудити безпеки платіжних систем та моніторте фінансові транзакції для виявлення надзвичайних або підозрілих дій.

- навчайте персонал правилам безпеки використання електронних платежів, виявлення фішингу та інших атак.

- захищайте корпоративні облікові записи та паролі, які мають доступ до фінансових систем.

- заохочуйте використання різних облікових записів для різних фінансових транзакцій та доступів.

- використовуйте системи відстеження та механізми підтвердження транзакцій для запобігання шахрайству та недозволеним операціям.

-встановлюйте чіткі політики визначення прав доступу до фінансових систем і обмежуйте доступ тільки необхідним працівникам.

- якщо використовується мобільний платіж, застосовуйте безпекові функції, такі як відбиток пальця чи обличчя для аутентифікації.

- налаштуйте систему на висилання сповіщень про будь-яку підозрілу або невизначену активність в облікових записах.

- регулярно створюйте резервні копії фінансових даних та перевіряйте їх можливість відновлення.

Впровадження цих заходів допоможе підприємствам зменшити ризики фінансових втрат і забезпечити безпеку електронних платежів.

6) Кібергігієна технології WI-FI

Забезпечення кібергігієни технологій Wi-Fi важливо для запобігання неправомірному доступу до мережі та збереження конфіденційності та цілісності даних [15]. Базові рекомендації для підприємств щодо безпеки технологій Wi-Fi:

- встановлюйте сильний пароль для доступу до бездротової мережі. Використовуйте комбінацію великих і малих літер, цифр і спецсимволів.

- забезпечте шифрування трафіку між пристроями та точкою доступу, наприклад, за допомогою WPA3 (Wi-Fi Protected Access 3).

- відключіть функцію Wi-Fi Protected Setup (WPS), оскільки це може бути вразливим до атак.

- регулярно оновлюйте програмне забезпечення на точках доступу, щоб захистити систему від відомих вразливостей.

- вимкніть трансляцію імені мережі (SSID) для ускладнення виявлення вашої мережі.

- де можливо, встановлюйте стандарт WPA3, який надає більш високий рівень безпеки порівняно з попередніми версіями.

- розділіть мережу на гостьову та корпоративну для підвищення безпеки.

- використовуйте віртуальні локальні мережі (VLAN) для ізоляції різних частин мережі.

- моніторте підключення до мережі і виявляйте неповноважні пристрої.

- встановіть брандмауер на точках доступу для обмеження неповноважного доступу.

- регулярно переглядайте налаштування безпеки на точках доступу та внутрішній мережі.

- для корпоративних мереж використовуйте сервер аутентифікації RADIUS для керування доступом.

- якщо є потреба віддаленого доступу, використовуйте віртуальні приватні мережі (VPN) для забезпечення безпеки трафіку.

- встановіть системи виявлення вторгнень (IDS) та системи виявлення аномальної поведінки (AIDP) для моніторингу атак.

- забезпечте безпеку мобільних пристроїв, які підключаються до Wi-Fi, за допомогою антивірусів та оновлень.

Ці рекомендації спрямовані на покращення безпеки Wi-Fi на підприємствах та зменшення ризиків, пов'язаних із зловживанням мережевих технологій.

7) Кібергігієна споживання інформації

Забезпечення кібергігієни споживання інформації є важливим аспектом кібербезпеки на підприємствах. Базові рекомендації для підприємств з цього питання:

- проводьте регулярні тренінги з безпеки для працівників, навчаючи їх розпізнавати фішингові атаки, соціальні інженерні втручання та інші загрози.

- визначайте джерела інформації, перевіряйте їх автентичність та надійність перед розповсюдженням чи використанням інформації.

- сприяйте використанню надійних та авторитетних джерел інформації для прийняття рішень.

- застосовуйте строгі правила та політики збереження та обробки корпоративної інформації.

- використовуйте шифрування для захисту конфіденційних даних та комунікацій.

- навчайте персонал впізнавати фішингові листи та інші атаки через електронну пошту.

- застосовуйте технології та заходи для захисту від витоків даних та забезпечення конфіденційності інформації.

- активуйте автоматичне оновлення програмного забезпечення на всіх комп'ютерах та пристроях для виправлення вразливостей.

- усім користувачам надавайте інструкції щодо безпечного перегляду веб-сайтів та виявлення потенційно небезпечних ресурсів.

- використовуйте антивірусне програмне забезпечення та антималware для захисту від вірусів та зловмисного програмного забезпечення.

- встановлюйте строгі політики щодо сильних паролів та ефективного управління доступом.

- проводьте регулярний аудит та моніторинг дій користувачів для виявлення неповноважного доступу чи надто активної активності.

- забезпечте безпеку мобільних пристроїв, що використовуються працівниками, через антивіруси та інші заходи безпеки.

Ці рекомендації допоможуть підприємствам покращити безпеку споживання інформації та зменшити ризики кіберзагроз.

8) Кібергігієна персонального комп'ютера

Забезпечення кібергігієни персональних комп'ютерів на підприємстві є важливою частиною загальної стратегії кібербезпеки. Основні рекомендації для забезпечення безпеки комп'ютерів на робочому місці:

- встановіть і оновлюйте регулярно антивірусне програмне забезпечення для захисту від шкідливих програм.

- активуйте автоматичне оновлення операційної системи, браузера та інших програм для закриття вразливостей.

- використовуйте фаєрвол для контролю мережевого трафіку та блокування небажаних з'єднань.

- встановіть політику використання сильних паролів та регулярно змінюйте їх.

- де можливо, використовуйте двоетапну аутентифікацію для збільшення рівня безпеки облікового запису.

- шифруйте чутливі дані на жорсткому диску або використовуйте шифрування файлів для захисту інформації.

- регулярно створюйте резервні копії важливої інформації та перевіряйте їх можливість відновлення.

- встановіть політику, щоб користувачі не встановлювали небезпечне чи невідоме програмне забезпечення.

- застосовуйте принцип найменших прав доступу (Least Privilege Principle) для обмеження доступу користувачів.

- захищайте мережу за допомогою заходів безпеки, таких як захист від атак на рівні мережі.

- вимикайте непотрібні мережеві сервіси та служби для зменшення поверхні атак.

- встановіть системи моніторингу для виявлення надзвичайної активності чи підозрілих подій.

- забезпечте фізичну безпеку комп'ютерів, щоб уникнути несанкціонованого доступу.

Ці заходи допоможуть забезпечити ефективну кібергігієну персональних комп'ютерів на підприємстві та запобігти багатьом загрозам кібербезпеки.

9) Соціальна інженерія

Соціальна інженерія є методом атак, при якому зловмисники використовують маніпулювання людьми для отримання конфіденційної інформації або навіть викликання неправомірних дій. Забезпечення захисту від соціальної інженерії на підприємстві вимагає комплексного підходу [16]. Базові рекомендації для підприємств:

- проводьте регулярні навчання та тренінги для працівників щодо соціальної інженерії та методів виявлення шахрайства.

- встановіть чітку політику конфіденційності та покажіть працівникам, яка інформація є конфіденційною та як нею користуватися.

- встановіть процедури перевірки ідентифікації для всіх працівників та персоналу з високим рівнем доступу.

- введіть строгу політику щодо обробки та витоку конфіденційної інформації та вимагайте її дотримання.

- визначайте доступ до конфіденційної інформації згідно з ролями та відповідальністю працівників.

- застосовуйте принцип найменших прав доступу (Least Privilege Principle) — дайте працівникам тільки ту інформацію, яку вони дійсно потребують для своєї роботи.

- моніторте та аналізуйте поведінку працівників у системі для виявлення аномальних або підозрілих активностей.

- застосовуйте міцні та надійні методи аутентифікації, такі як двоетапна або багатоетапна аутентифікація.

- використовуйте технології антиспаму та антивірусу, і навчайте працівників виявляти підозрілі дії.

- використовуйте захищені канали для обміну конфіденційною інформацією.

- розгляньте можливість обмеження використання зовнішніх USB-пристроїв на робочих комп'ютерах.

- розробіть план реагування на інциденти та навчайте персонал діяти в разі підозрілої або атаки соціальної інженерії.

- забезпечте фізичну безпеку приміщень та обладнання, щоб уникнути фізичних атак.

- контролюйте доступ зовнішніх підрядників та забезпечте їхню освіту щодо кібербезпеки.

- проводьте регулярні аудити безпеки для оцінки ефективності вжитих заходів та виявлення нових вразливостей.

3 ПРОГРАМНА РЕАЛІЗАЦІЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ

3.1 Обґрунтування вибору інструментальних засобів розробки

Наступним етапом програмної реалізації інформаційної технології є вибір інструментальних засобів (бібліотеки мови програмування, модулі, програмні засоби), використовуючи які, будуть реалізовані основні модулі та спроектована система в цілому.

Для розробки програмного засобу буде використано мову програмування високого рівня Python. Перевагами вказаної мови є наявність великої кількості бібліотек та простий синтаксис [17].

Наступним кроком є обрання середовища розробки. Запуск програмного засобу буде відбуватися на персональному комп'ютері користувача.

Серед найбільш популярних середовищ варто відокремити наступні, оскільки вони передбачають комплексну та швидку розробку програмного забезпечення [18]:

1) Sublime Text 3 – умовно безкоштовне середовище розробки, яке підтримує велику кількість мов програмування, включаючи Python. За замовчуванням має базову підтримку Python, проте для полегшення та пришвидшення розробки необхідно встановлювати пакети доповнень.

2) PyCharm – найпопулярніша середа розробки. Має набір додатків та функцій, які прискорюють розробку програмного забезпечення, які встановлюються із середовищем за замовчуванням. Має безкоштовну та платну версії.

3) Visual Studio Code – загальне середовище розробки, яке підтримує різні мови програмування. Постачається з системою автодоповнення. Для розробки програмних засобів мовою Python, необхідно завантажити розширення та виконати налаштування середовища розробки.

База даних релізована з допомогою SQLite - це компактна вбудована реляційна база даних з відкритим кодом. Вона одна з найпопулярніших у світі, має нагороду Google-O'Reilly Open Source Awards і широко використовується в додатках та системах, де потрібно організувати зберігання даних [16].

Однією з основних особливостей SQLite є те, що вона є сервером баз даних "без сервера", що означає відсутність окремого серверного процесу, який обробляє запити. SQLite проста у використанні, легка та ефективна, і часто використовується для вбудованих додатків, мобільних додатків та інших проектів з невеликими обсягами даних [19].

Основні характеристики SQLite:

- Вбудована СУБД: SQLite не вимагає окремого серверного процесу та використовує невеликий обсяг пам'яті, що робить його ідеальним для вбудованих систем та пристроїв з обмеженими ресурсами.

- Проста у використанні: SQLite не потребує конфігурації та налаштувань перед початком використання. Все необхідне вбудовано в бібліотеку, і вона легко інтегрується в проекти.

- Синтаксис SQL: SQLite підтримує стандартний SQL-синтаксис для виконання запитів та маніпулювання даними в базі даних.

- Підтримка ACID: SQLite гарантує виконання принципів ACID (атомарність, консистентність, ізоляція, довговічність), що забезпечує стабільність та надійність операцій з даними.

- Система типів даних: SQLite має підтримку різних типів даних, таких як INTEGER, TEXT, REAL, BLOB і NULL.

- Багато мов програмування: SQLite доступний для використання в різних мовах програмування, таких як C, C++, Java, Python, PHP та інші [19].

Переваги:

- це дуже легка база даних, яка не потребує окремого сервера. Вона працює швидко та ефективно, особливо на системах з обмеженими ресурсами;

- SQLite відносно проста у використанні та не вимагає складних налаштувань. Взаємодіяти з базою даних можна, використовуючи стандартні мови програмування і мову запитів SQL;
- СУБД можна вбудовувати безпосередньо в програмне забезпечення, що полегшує розповсюдження та розгортання додатків;
- всі дані зберігаються в одному файлі бази даних, що робить резервне копіювання і перенесення простою справою;
- SQLite підтримує транзакції, і це дозволяє забезпечити цілісність та безпеку даних;
- СУБД має багато різних оболонок і бібліотек, які роблять SQLite доступним для багатьох мов програмування: Python, Java, C#, і багато інших.

Недоліки:

- SQLite не підтримує велику кількість одночасних записів. В таких ситуаціях можуть виникати блокування і конфлікти;
- база даних не підходить для великих обсягів даних або високонавантажених систем, оскільки має обмежену підтримку;
- SQLite не підтримує віддалений доступ через мережу;
- відсутня безкоштовна технічна підтримка: проблемні ситуації доведеться розв’язувати через спільноту;
- СУБД призначена в основному для операцій CRUD (створення, читання, оновлення, видалення) і не підходить для складних аналітичних дій з даними.

Для розробки програмного засобу було використано фреймворк Flask. Flask - це легкий мікрофреймворк для розробки веб-додатків на мові програмування Python. Він відомий своєю простотою і гнучкістю. Нижче наведені деякі переваги та недоліки Flask [20].

Переваги:

- Flask має простий синтаксис і лаконічну структуру, що дозволяє швидко створювати веб-додатки.

- Flask не нав'язує жорстких правил або структур проекту, що дає розробникам велику свободу у виборі технологій і архітектур.

- Фреймворк є легковаговим, і його основна функціональність обмежена. Він не має багатофункціональних елементів, які не завжди потрібні, що робить його швидким і ефективним.

- Flask має велику та активну спільноту, а також чудову офіційну документацію. Це полегшує вирішення проблем і знаходження рішень.

- Flask має багату екосистему розширень, які дозволяють додавати функціональність за необхідності [20].

Недоліки Flask:

- Порівняно з іншими фреймворками, такими як Django, Flask не має вбудованих компонентів, таких як ORM або адміністративний інтерфейс. Ви повинні обирати і встановлювати їх окремо, якщо вони потрібні.

- Велика свобода може призвести до різних підходів до розробки, що робить проекти менш однорідними і може ускладнити роботу великих команд.

- Оскільки Flask надає мінімальний набір інструментів, він може бути менш зручним для розробки великих та складних веб-додатків, порівняно з фреймворками, які вже включають багато стандартних рішень.

- Відсутність вбудованих елементів може змушувати розробників використовувати сторонні бібліотеки і розширення, що може впливати на спрощення та єдність коду [20].

3.2 Розробка програмного засобу

Відповідно до алгоритму роботи програмного засобу було створено ряд функцій, які забезбечують роботу додатка:

1. is_admin – функція для перевірки, чи користувач має права адміністратора;
2. create_survey – функція для створення тем та питань;
3. take_survey – функція для вибору опитування та відображення питань;
4. get_correct_answer – функція для отримання правильної відповіді на питання з бази даних;
5. start_survey – функція для старту опитування;
6. survey_results – функція для отримання результатів опитування;
7. del_survey_menu – функція для видалення опитування;
8. login – функція для входу в систему;
9. logout – функція для виходу з системи;
10. register – функція для реєстрації.

Відповідно до поставлених задач було розроблено структуру бази даних, яка складається з 4 таблиць.

Таблиця "Users" (Користувачі):

UserID (PK): Ідентифікатор користувача.

Username: Логін користувача для автентифікації.

Password: Хеш пароля користувача.

FirstName: Ім'я користувача.

LastName: Прізвище користувача.

Email: Електронна пошта користувача.

Role: Роль користувача ("employee" чи "instructor").

Всі поля таблиці "Users" є атомарними, а ключ (UserID) ідентифікує всі інші атрибути.

Таблиця "TestCategories" (Категорії тестів):

CategoryID (PK): Ідентифікатор категорії тестів.

CategoryName: Назва категорії тестів.

Всі поля "TestCategories" є атомарними, а ключ (CategoryID) ідентифікує всі інші атрибути.

Таблиця "Tests" (Тести):

TestID (PK): Ідентифікатор тесту.

TestCategoryID (FK): Зовнішній ключ, посилається на "CategoryID" в таблиці "TestCategories".

Question: Питання тесту.

CorrectAnswer: Правильна відповідь на тест.

Weight: Вага тесту в загальному рейтингу.

Всі поля таблиці "Tests" є атомарними , а ключ (TestID) ідентифікує всі інші атрибути. Поле TestCategoryID є зовнішнім ключем, вказуючи на "CategoryID" в таблиці "TestCategories".

Таблиця "UserTestResults" (Результати тестування користувача):

ResultID (PK): Ідентифікатор результату тестування.

UserID (FK): Зовнішній ключ, посилається на "UserID" в таблиці "Users".

TestID (FK): Зовнішній ключ, посилається на "TestID" в таблиці "Tests".

UserAnswer: Відповідь користувача на тест.

IsCorrect: Ознака правильної відповіді.

Всі поля є атомарними, а ключ (ResultID) ідентифікує всі інші атрибути.

Поля таблиці "UserTestResults"UserID та TestID є зовнішніми ключами, вказуючи на відповідні ключі в таблицях "Users" та "Tests".

Таблиця "LearningResources" (Навчальні ресурси):

ResourceID (PK): Ідентифікатор навчального ресурсу.

ResourceName: Назва навчального ресурсу.

ResourceType: Тип ресурсу ("відео", "текст", "аудіо").

Content: Зміст навчального ресурсу.

TestCategoryID (FK): Зовнішній ключ, посилається на "CategoryID" в таблиці "TestCategories".

Всі поля є атомарними, а ключ (ResourceID) ідентифікує всі інші атрибути.

Поле TestCategoryID є зовнішнім ключем, вказуючи на "CategoryID" в таблиці "TestCategories".

Кожна таблиця має унікальний первинний ключ.

Немає транзитивних залежностей, кожен атрибут визначений через первинний ключ.

Всі дані розподілені між таблицями, і вони знаходяться у третій нормальній формі.

Нижче наведені елементи додатку, такі як вікно реєстрації (рис.3.1):

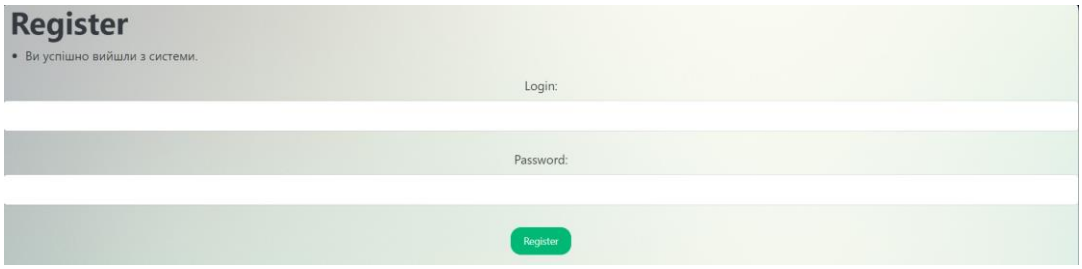

Рисунок 3.1 – Вікно реєстрації

Також реалізовано вікно входу для зареєстрованих раніше користувачів (рис 3.2):

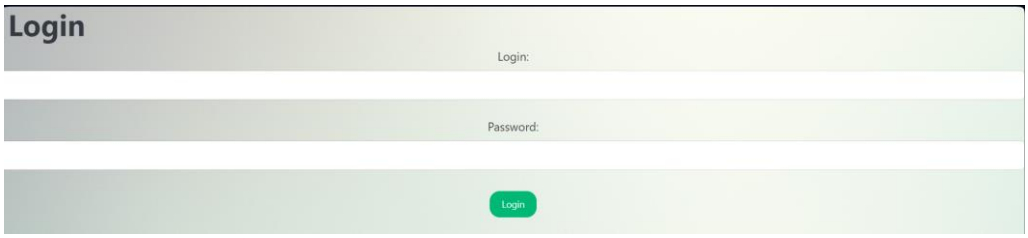

Рисунок 3.2 – Вікно входу в систему

Користувач з правами адміністратора може додавати нові теми та питання до системи (рис 3.3):

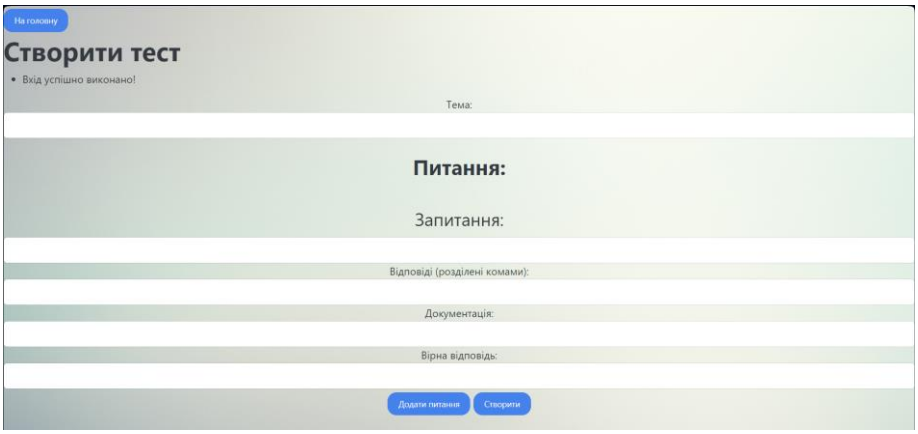

Рисунок 3.3 – Форма для додавання нових тем та питань

В результаті додавання тем з'являється можливість для інших користувачів обирати модулі для тестування (рис 3.4):

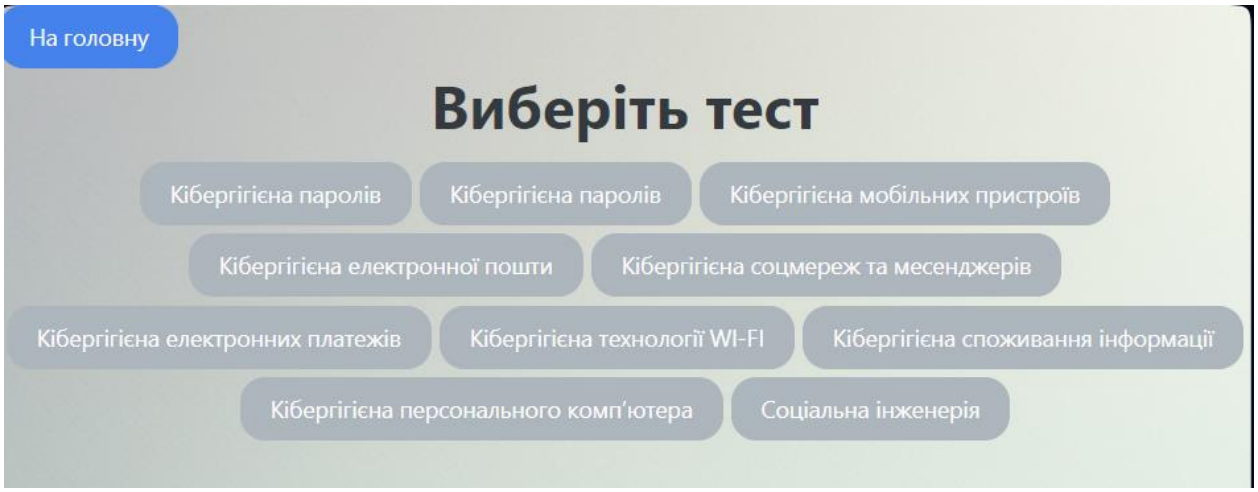

Рисунок 3.4 – Меню вибору напрямків тестування

Після вибору напрямків тестування переходимо безпосередньо до проходження тесту (рис 3.5):

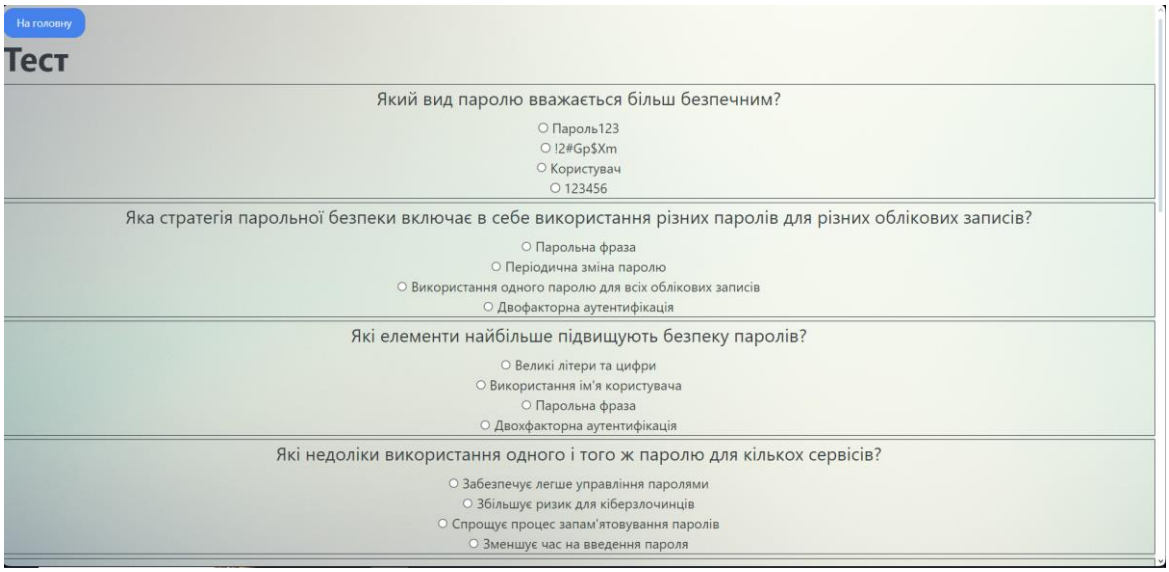

Рисунок 3.5 – Вигляд сторінки з питаннями

Після проходження тесту користувачу на екран виводиться результат та рекомендовані навчальні матеріали (рис. 3.6):

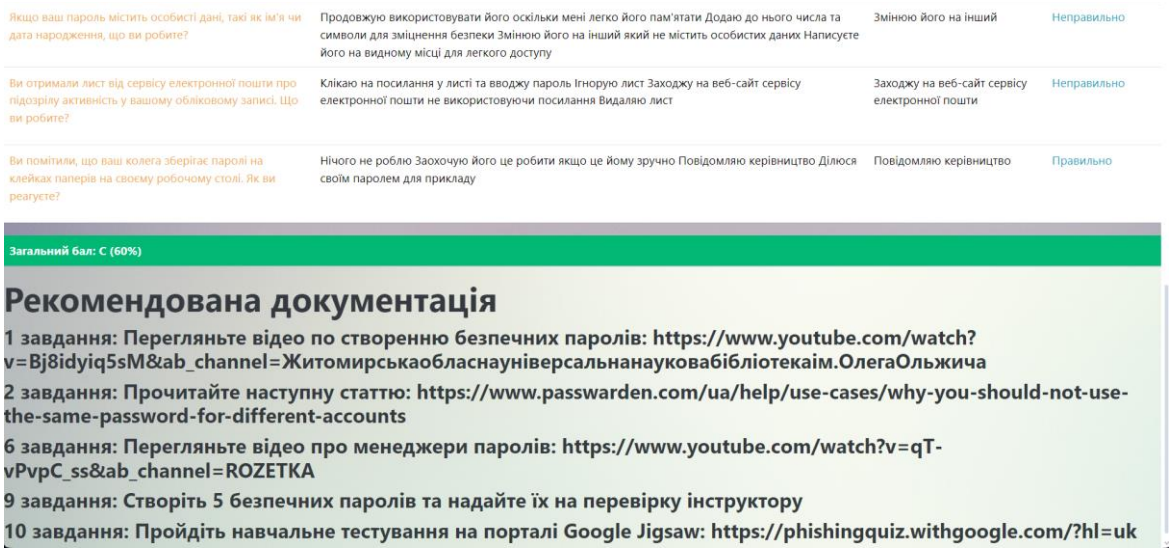

Рисунок 3.6 – Вигляд фінальної сторінки з оцінкою та результатами

Текст програмного засобу наведено у додатку В. Для перевірки розробленого програмного засобу необхідно провести тестування.

3.3 Тестування програмного засобу

Тестування буде проведено з використанням двох сценаріїв:

- перевірка правильної роботи програмного засобу;

- перевірка роботи програмного засобу при використанні неправильних даних.

Перевіримо сторінку входу до системи. Спробуємо ввести у поля логіну та пароля вірні дані (рис 3.1).

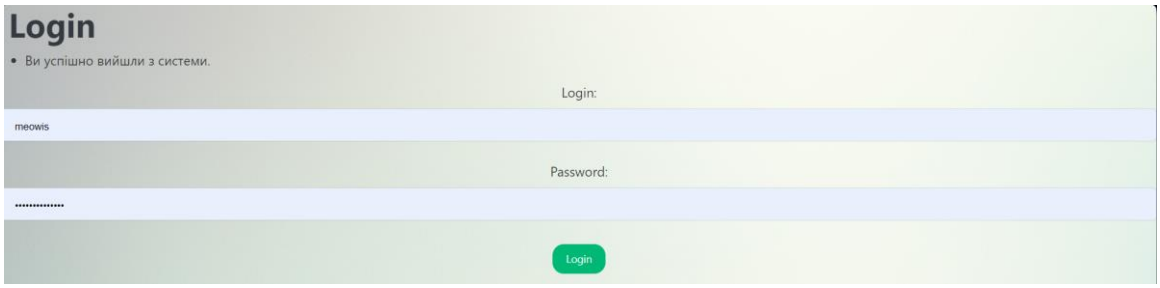

Рисунок 3.1 – Введення коректних даних для входу

В результаті введення вірного логіну та пароля потрапляємо на головну сторінку, в даному випадку на сторінку адміністратора (рис. 3.2).

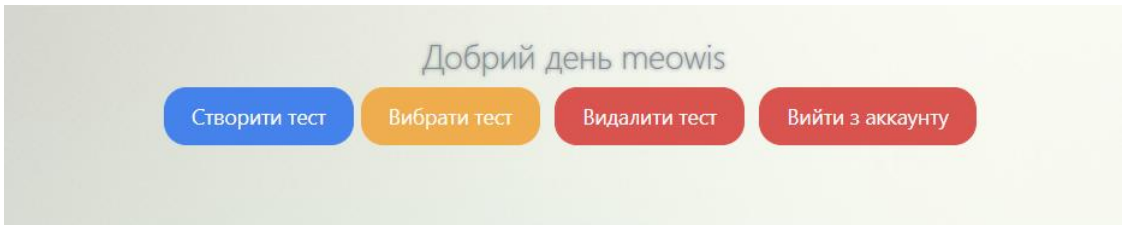

Рисунок 3.2 – Головна сторінка з правами адміністратора

Спробуємо ввести неправильні данні (рис. 3.3).

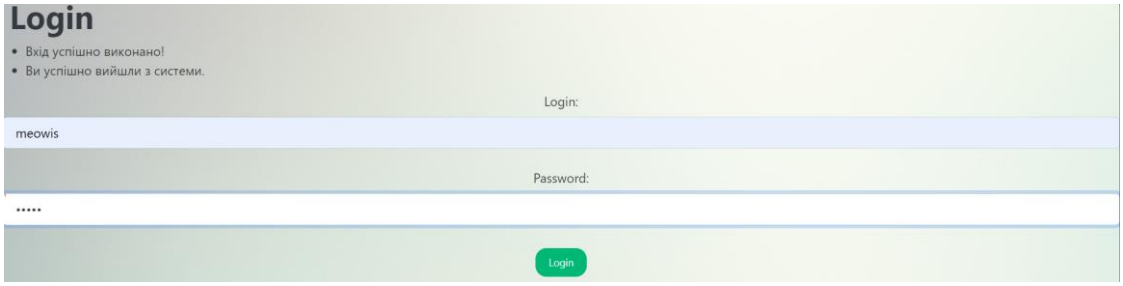

Рисунок 3.3 – Введення некоректних даних для входу

Система виводить на екран, що данні було введено невірно (рис. 3.4).

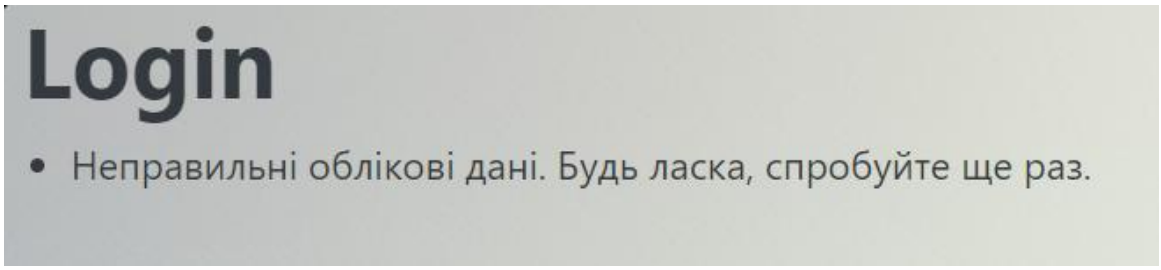

Рисунок 3.4 – Повідомлення про неправильні облікові данні

Було виконано тестування програмного засобу, використовуючи два сценарії (введення правильних і неправильних даних). За результатами тестування можна стверджувати, що програмний засіб працює правильно і виконується обробка помилок в разі їх появи.

4 ЕКОНОМІЧНА ЧАСТИНА

Для успішного впровадження науково-технічної розробки вельми важливо, щоб вона відповідала сучасним вимогам науково-технічного прогресу та враховувала економічні аспекти. Надання оцінки економічної ефективності результатів науково-дослідної роботи є важливою складовою цього процесу. Дослідження, яке представлене у магістерській роботі і присвячене розробці та вивченню "Інформаційна технологія оцінювання рівня кібергігієни особи", віднесено до науково-технічних проектів, спрямованих на введення на ринок. Рішення про комерціалізацію розробки може бути прийняте протягом виконання самої роботи, розкриваючи можливості для подальшого виведення на ринок. Цей напрямок визначається як пріоритетний, оскільки розроблені результати можуть бути корисними для різних зацікавлених сторін і приносити економічні вигоди. Проте для успішної реалізації цього процесу вирішальним є залучення зацікавленого інвестора, який виявить інтерес до втілення даного проекту, і переконання його у доцільності інвестування у цю розробку. З метою досягнення цього завдання були визначені такі етапи виконання робіт:

1. Проведення комерційного аудиту науково-технічної розробки, включаючи визначення науково-технічного рівня та комерційного потенціалу.
2. Розрахунок витрат на реалізацію науково-технічної розробки.
3. Проведення розрахунку економічної ефективності впровадження та комерціалізації науково-технічної розробки для потенційного інвестора, а також обґрунтування економічної доцільності комерціалізації з точки зору інвестора.

4.1 Проведення комерційного та технологічного аудиту науково-технічної розробки

Метою проведення комерційного і технологічного аудиту дослідження

за темою "Інформаційна технологія оцінювання рівня кібергігієни особи" є підвищення рівня інформаційної безпеки шляхом тестування осіб на їх рівень кібергігієни.

Оцінювання науково-технічного рівня розробки та її комерційного потенціалу рекомендується здійснювати із застосуванням 5-ти бальної системи оцінювання за 12-ма критеріями, наведеними в табл. 4.1 [21].

Таблиця 4.1 – Рекомендовані критерії оцінювання науково-технічного рівня і комерційного потенціалу розробки та бальна оцінка

Бали (за 5-ти бальною шкалою)					
	0	1	2	3	4
Технічна здійсненність концепції					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено працездатність продукту в реальних
Ринкові переваги (недоліки)					
2	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів
4	Технічні та споживчі властивості продукту	Технічні та споживчі влас-тивості продукту	Технічні та споживчі властивості продукту на	Технічні та споживчі властивості продукту	Технічні та споживчі властивості продукту
5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів
Ринкові перспективи					

Продовження табл. 4.1

6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає
Практична здійсненність					
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні. Джерела	Потрібні незначні фінансові ресурси. Джерела фінансування	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування
10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуют
11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій	Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій

Продовження табл. 4.1

12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь-які регламентні обмеження на виробництво та реалізацію продукту

Результати оцінювання науково-технічного рівня та комерційного потенціалу науково-технічної розробки потрібно звести до таблиці. Для оцінки науково-технічного рівня і комерційного потенціалу розробки експертами було запрошено трьох незалежних експертів Вінницького національного технічного університету кафедри «Захисту інформації»: Кондратенко Наталія Романівна, к. т. н., професор, Дудатьєв Андрій Веніамінович, к. т. н., доцент, Войтович Олеся Петрівна, к. т. н., доцент.

Таблиця 4.2 – Результати оцінювання науково-технічного рівня і комерційного потенціалу розробки експертами

Критерії	Експерт (ПІБ, посада)		
	Кондратенко Н. Р.	Дудатьєв А. В.	Войтович О. П.
	Бали, виставлені експертами:		
1. Технічна здійсненність концепції	3	3	3
2. Ринкові переваги (наявність аналогів)	3	3	3
3. Ринкові переваги (ціна продукту)	5	5	5
4. Ринкові переваги (технічні властивості)	2	3	2
5. Ринкові переваги (експлуатаційні витрати)	4	5	5

Продовження табл. 4.2

6. Ринкові перспективи (розмір ринку)	3	4	5
7. Ринкові перспективи (конкуренція)	4	5	4
8. Практична здійсненність (наявність фахівців)	4	4	5
9. Практична здійсненність (наявність фінансів)	2	3	3
10. Практична здійсненність (необхідність нових матеріалів)	4	4	3
11. Практична здійсненність (термін реалізації)	3	3	4
12. Практична здійсненність (розробка документів)	2	2	3
Сума балів	$СБ_1$=39	$СБ_2$=44	$СБ_3$=45
Середньоарифметична сума балів $СБ_c$	43		

За результатами розрахунків, наведених в таблиці 4.2, зробимо висновок щодо науково-технічного рівня і рівня комерційного потенціалу розробки. При цьому використаємо рекомендації, наведені в табл. 4.3 [21].

Таблиця 4.3 – Науково-технічні рівні та комерційні потенціали розробки

Середньоарифметична сума балів СБ , розрахована на основі висновків експертів	Науково-технічний рівень та комерційний потенціал розробки
41…48	Високий
31…40	Вище середнього
21…30	Середній
11…20	Нижче середнього
0…10	Низький

Згідно проведених досліджень рівень комерційного потенціалу розробки за темою "Інформаційна технологія оцінювання рівня кібергігієни особи" становить 43 бали, що, відповідно до таблиці 4.3 рівень комерційного потенціалу розробки високий, що свідчить про комерційну важливість проведення даних досліджень.

Магістерська кваліфікаційна робота "Інформаційна технологія

оцінювання рівня кібергігієни особи" відноситься до науково-технічних робіт, які орієнтовані на виведення на ринок, тобто при цьому відбувається комерціалізація науково-технічної розробки. Цей напрямок є для нас пріоритетним, оскільки результатами розробки можуть користуватися не тільки самі розробники, а й інші споживачі, отримуючи при цьому суттєвий економічний ефект.

4.2 Розрахунок витрат на проведення науково-дослідної роботи

Витрати, пов’язані з проведенням науково-дослідної роботи на тему "Інформаційна технологія оцінювання рівня кібергігієни особи", під час планування, обліку і калькулювання собівартості науково-дослідної роботи групуємо за відповідними статтями.

4.2.1 Витрати на оплату праці

До статті «Витрати на оплату праці» належать витрати на виплату основної та додаткової заробітної плати керівникам відділів, лабораторій, секторів і груп, науковим, інженерно-технічним працівникам, конструкторам, технологам, креслярам, копіювальникам, лаборантам, робітникам, студентам, аспірантам та іншим працівникам, безпосередньо зайнятим виконанням конкретної теми, обчисленої за посадовими окладами, відрядними розцінками, тарифними ставками згідно з чинними в організаціях системами оплати праці.

Основна заробітна плата дослідників

Витрати на основну заробітну плату дослідників ($З_о$) розраховуємо у відповідності до посадових окладів працівників, за формулою [21]:

$$З_о = \sum_{i=1}^{k} \frac{M_{ni} \cdot t_i}{T_p}, \qquad (4.1)$$

де k – кількість посад дослідників залучених до процесу досліджень;

M_{ni} – місячний посадовий оклад конкретного дослідника, грн;

t_i – число днів роботи конкретного дослідника, дн.;

T_p – середнє число робочих днів в місяці, T_p=21 дні.

$$З_о = 16000 \cdot 5 / 21 = 3636 \text{грн.}$$

Проведені розрахунки зведемо до таблиці.

Таблиця 4.4 – Витрати на заробітну плату дослідників

Найменування посади	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Число днів роботи	Витрати на заробітну плату, грн
Керівник проекту	16000	727,3	5	3636
Інженер-програміст 1-ї категорії	12000	545,5	21	11455
Всього				15091

Основна заробітна плата робітників

Витрати на основну заробітну плату робітників ($З_р$) за відповідними найменуваннями робіт НДР на тему "Інформаційна технологія оцінювання рівня кібергігієни особи" розраховуємо за формулою:

$$З_р = \sum_{i=1}^{n} C_i \cdot t_i , \quad (4.2)$$

де C_i – погодинна тарифна ставка робітника відповідного розряду, за виконану відповідну роботу, грн/год;

t_i – час роботи робітника при виконанні визначеної роботи, год.

Погодинну тарифну ставку робітника відповідного розряду C_i можна визначити за формулою:

$$C_i = \frac{M_M \cdot K_i \cdot K_c}{T_p \cdot t_{зм}} , \quad (4.3)$$

де M_M – розмір прожиткового мінімуму працездатної особи, або мінімальної місячної заробітної плати (в залежності від діючого законодавства), приймемо $Мм$=6500 грн;

K_i – коефіцієнт міжкваліфікаційного співвідношення для встановлення тарифної ставки робітнику відповідного розряду (табл. Б.2, додаток Б) [21];

K_c – мінімальний коефіцієнт співвідношень місячних тарифних ставок робітників першого розряду з нормальними умовами праці виробничих об'єднань і підприємств до законодавчо встановленого розміру мінімальної заробітної плати.

T_p – середнє число робочих днів в місяці, приблизно T_p = 21 дн;

$t_{зм}$ – тривалість зміни, год.

$C_1 = 6700{,}00 \cdot 1 \cdot 1{,}65 / (21 \cdot 8) = 65{,}8$ грн.
$З_{р1} = 65{,}8 \cdot 6 = 394{,}8$ грн.

Таблиця 4.5 – Величина витрат на основну заробітну плату робітників

Найменування робіт	Тривалість роботи, год	Розряд роботи	Погодинна тарифна ставка, грн	Величина оплати на робітника грн
1.Підготовка робочого місця інструктора	6	1	65,8	394,8
2. Інсталяція програмного засобу на машину інструктора	1	3	88,8	88,8
3.Формування кодів програмних блоків	13	5	111,9	1454,3
4.Формування бази даних для системи тестування	9	2	72,4	651,5
5.Контроль проходження тестування	8	4	59,8	478,6
Всього				3067,9

Додаткова заробітна плата дослідників та робітників

Додаткову заробітну плату розраховуємо як 10 … 12% від суми основної заробітної плати дослідників та робітників за формулою:

$$З_{дод} = (З_о + З_р) \cdot \frac{Н_{дод}}{100\%}, \qquad (4.4)$$

де $Н_{дод}$ – норма нарахування додаткової заробітної плати. Приймемо 11%.

$З_{дод}$ = (15091+3067,9) · 11 / 100% = 1997,47 грн.

4.2.2 Відрахування на соціальні заходи

Нарахування на заробітну плату дослідників та робітників розраховуємо як 22% від суми основної та додаткової заробітної плати дослідників і робітників за формулою:

$$З_н = (З_о + З_р + З_{дод}) \cdot \frac{Н_{зп}}{100\%} \quad (4.5)$$

де $Н_{зп}$ – норма нарахування на заробітну плату. Приймаємо 22%.

$Зн$ = (15091+3067,9+1997,47) · 22 / 100% = 4434,39 грн.

4.2.3 Сировина та матеріали

До статті «Сировина та матеріали» належать витрати на сировину, основні та допоміжні матеріали, інструменти, пристрої та інші засоби і предмети праці, які придбані у сторонніх підприємств, установ і організацій та витрачені на проведення досліджень за темою "Інформаційна технологія оцінювання рівня кібергігієни особи".

Витрати на матеріали ($М$), у вартісному вираженні розраховуються окремо по кожному виду матеріалів за формулою:

$$М = \sum_{j=1}^{n} Н_j \cdot Ц_j \cdot К_j - \sum_{j=1}^{n} В_j \cdot Ц_{вj}, \quad (4.6)$$

де $Н_j$ – норма витрат матеріалу j-го найменування, кг;

n – кількість видів матеріалів;

$Ц_j$ – вартість матеріалу j-го найменування, грн/кг;

$К_j$ – коефіцієнт транспортних витрат, ($К_j$ = *1,1 … 1,15*);

$В_j$ – маса відходів j-го найменування, кг;

$Ц_{вj}$ – вартість відходів j-го найменування, грн/кг.

Проведені розрахунки зведемо до таблиці.

Таблиця 4.7 – Витрати на матеріали

Найменування матеріалу, марка, тип, сорт	Ціна за 1 кг, грн	Норма витрат, кг	Вартість витраченого матеріалу, грн
Папір офісний CRYSTAL PRO A4 80г/м	210	0,2	42
Картридж для принтера	560	0,5	280
USB Kingston DataTraveler Exodia Onyx 64GB USB 3.2 Gen 1 Black (DTXON/64GB)	199	1	199
Всього			521
З врахуванням коефіцієнта транспортування			573,1

4.3.4 Спецустаткування для наукових (експериментальних) робіт

До статті «Спецустаткування для наукових (експериментальних) робіт» належать витрати на виготовлення та придбання спецустаткування необхідного для проведення досліджень, також витрати на їх проектування, виготовлення, транспортування, монтаж та встановлення.

Балансову вартість спецустаткування розраховуємо за формулою:

$$B_{спец} = \sum_{i=1}^{k} Ц_i \cdot C_{пр.i} \cdot K_i \ , \qquad (4.7)$$

де $Ц_i$ – ціна придбання одиниці спецустаткування даного виду, марки, грн;

$C_{пр.i}$ –кількість одиниць устаткування відповідного найменування, які придбані для проведення досліджень, шт.;

K_i – коефіцієнт, що враховує доставку, монтаж, налагодження устаткування тощо, (K_i *= 1,10…1,12);*

k – кількість найменувань устаткування.

$B_{спец} = 1099{,}00 \cdot 1 \cdot 1{,}11 = 1208{,}90$ *грн.*

Отримані результати зведемо до таблиці:

Таблиця 4.8 – Витрати на придбання спецустаткування по кожному виду

Найменування устаткування	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
Оперативна пам’ять Kinston	1	1099	1208,9

8GB			
Диск Kingston SSD V300 120 GB	1	1899	2088,9
Процесор Intel Core i3-13100	1	5499	6048,9
Всього			9346,7

4.3.5 Програмне забезпечення для наукових (експериментальних) робіт

До статті «Програмне забезпечення для наукових (експериментальних) робіт» належать витрати на розробку та придбання спеціальних програмних засобів і програмного забезпечення, (програм, алгоритмів, баз даних) необхідних для проведення досліджень, також витрати на їх проектування, формування та встановлення.

Балансову вартість програмного забезпечення розраховуємо за формулою:

$$B_{прг} = \sum_{i=1}^{k} Ц_{iпрг} \cdot C_{прг.i} \cdot K_i \ , \qquad (4.8)$$

де $Ц_{iпрг}$ – ціна придбання одиниці програмного засобу даного виду, грн;

$C_{прг.i}$ – кількість одиниць програмного забезпечення відповідного найменування, які придбані для проведення досліджень, шт.;

K_i – коефіцієнт, що враховує інсталяцію, налагодження програмного засобу тощо, ($K_i = 1,10…1,12$);

k – кількість найменувань програмних засобів.

$B_{прг} = 935 \cdot 1 \cdot 1,11 = 6215$ *грн.*

Отримані результати зведемо до таблиці:

Таблиця 4.9 – Витрати на придбання програмних засобів по кожному виду

Найменування програмного засобу	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
Середовище програмування VSCode	1	850	935
Операційна система Windows	1	4500	4950
Доступ до мережі інтернет ВОЛЯ	1	300	330
Всього			6215

4.2.6 Амортизація обладнання, програмних засобів та приміщень

В спрощеному вигляді амортизаційні відрахування по кожному виду обладнання, приміщень та програмному забезпеченню тощо, розраховуємо з використанням прямолінійного методу амортизації за формулою:

$$A_{обл} = \frac{Ц_б}{T_в} \cdot \frac{t_{вик}}{12}, \quad (4.9)$$

де $Ц_б$ – балансова вартість обладнання, програмних засобів, приміщень тощо, які використовувались для проведення досліджень, грн;

$t_{вик}$ – термін використання обладнання, програмних засобів, приміщень під час досліджень, місяців;

$T_в$ – строк корисного використання обладнання, програмних засобів, приміщень тощо, років.

$A_{обл} = (20000 \cdot 1) / (2 \cdot 12) = 833{,}33$ грн.

Проведені розрахунки зведемо до таблиці.

Таблиця 4.10 – Амортизаційні відрахування по кожному виду обладнання

Найменування обладнання	Балансова вартість, грн	Строк корисного використання, років	Термін використання обладнання, місяців	Амортизаційні відрахування, грн
Персональний комп'ютер	20000	2	1	833,33
Робоче місце розробника ПЗ	195000	20	2	1625,00
Всього				2458,33

4.2.7 Паливо та енергія для науково-виробничих цілей

Витрати на силову електроенергію ($B_е$) розраховуємо за формулою:

$$B_е = \sum_{i=1}^{n} \frac{W_{уі} \cdot t_i \cdot Ц_е \cdot K_{впі}}{\eta_i}, \quad (4.10)$$

де $W_{уі}$ – встановлена потужність обладнання на визначеному етапі розробки, кВт;

t_i – тривалість роботи обладнання на етапі дослідження, год;

$Ц_е$ – вартість 1 кВт-години електроенергії, грн; (вартість електроенергії визначається за даними енергопостачальної компанії), приймемо $Ц_е$ = 7,5 грн;

$К_{вп і}$ – коефіцієнт, що враховує використання потужності, $К_{вп і} < 1$;

η_i – коефіцієнт корисної дії обладнання, $\eta_i < 1$.

$В_е = 0,25 \cdot 260,0 \cdot 7,5 \cdot 0,5 / 0,8 = 304,69$ грн.

4.2.8 Службові відрядження

До статті «Службові відрядження» дослідної роботи на тему "Інформаційна технологія оцінювання рівня кібергігієни особи" належать витрати на відрядження штатних працівників, працівників організацій, які працюють за договорами цивільно-правового характеру, аспірантів, зайнятих розробленням досліджень, відрядження, пов'язані з проведенням випробувань машин та приладів, а також витрати на відрядження на наукові з'їзди, конференції, наради, пов'язані з виконанням конкретних досліджень.

Витрати за статтею «Службові відрядження» розраховуємо як 20…25% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{св} = (З_о + З_р) \cdot \frac{Н_{св}}{100\%}, \qquad (4.11)$$

де $Н_{св}$ – норма нарахування за статтею «Службові відрядження», приймемо $Н_{св}$ = 20%.

$В_{св} = (15091+3067,9) \cdot 20 / 100\% = 3631,77$ грн.

4.2.9 Інші витрати

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками.

Витрати за статтею «Інші витрати» розраховуємо як 50…100% від суми основної заробітної плати дослідників та робітників за формулою:

$$I_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (4.12)$$

де $Н_{ів}$ – норма нарахування за статтею «Інші витрати», приймемо $Н_{ів}$ = 50%.

$І_в$ = (15091+3067,9) · 50 / 100% = 9079,43 грн.

4.2.10 Накладні (загальновиробничі) витрати

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов'язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов'язані з набором робочої сили; витрати на оплату послуг банків; витрати, пов'язані з освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін.

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуємо як 100…150% від суми основної заробітної плати дослідників та робітників за формулою:

$$В_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \quad (4.13)$$

де $Н_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати», приймемо $Н_{нзв}$ = 100%.

$В_{нзв}$ = (15091+3067,9) · 100 / 100% = 18158,85 грн.

Витрати на проведення науково-дослідної роботи на тему "Інформаційна технологія оцінювання рівня кібергігієни особи" розраховуємо як суму всіх попередніх статей витрат за формулою:

$$В_{заг} = З_о + З_р + З_{дод} + З_н + М + К_в + В_{спец} + В_{прг} + А_{обл} + В_е + В_{св} + В_{сп} + І_в + В_{нзв}. \quad (4.14)$$

$В_{заг}$=15091+3067,9+1997,47+4434,39+573,1+9346,7+6215+2458,33+304,69+3631,77+9079,43+18158,85 = 74358,58 грн.

Загальні витрати *ЗВ* на завершення науково-дослідної (науково-

технічної) роботи та оформлення її результатів розраховується за формулою:

$$ЗВ = \frac{В_{заг}}{\eta}, \quad (4.15)$$

де η - коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи, приймемо η=0,5.

ЗВ = 74358,58 / 0,5 = 148717,17 грн.

4.3 Розрахунок економічної ефективності науково-технічної розробки при її можливій комерціалізації потенційним інвестором

В ринкових умовах узагальнюючим позитивним результатом, що його може отримати потенційний інвестор від можливого впровадження результатів тієї чи іншої науково-технічної розробки, є збільшення у потенційного інвестора величини чистого прибутку.

Результати дослідження проведені за темою "Інформаційна технологія оцінювання рівня кібергігієни особи" передбачають комерціалізацію протягом 3-х років реалізації на ринку.

В цьому випадку основу майбутнього економічного ефекту будуть формувати:

ΔN – збільшення кількості споживачів яким надається відповідна інформаційна послуга у періоди часу, що аналізуються;

N – кількість споживачів яким надавалась відповідна інформаційна послуга у році до впровадження результатів нової науково-технічної розробки, приймемо 1 особа

$Ц_б$ – вартість послуги у році до впровадження інформаційної системи, приймемо 3500,00 грн;

$\pm\Delta Ц_о$ – зміна вартості послуги від впровадження результатів, приймемо зростання на 300,00 грн.

Можливе збільшення чистого прибутку у потенційного інвестора $\Delta П_i$

для кожного із 3-х років, протягом яких очікується отримання позитивних результатів від можливого впровадження та комерціалізації науково-технічної розробки, розраховуємо за формулою [21]:

$$\Delta П_i = (\pm \Delta Ц_o \cdot N + Ц_o \cdot \Delta N)_i \cdot \lambda \cdot \rho \cdot (1 - \frac{\vartheta}{100}), \quad (4.16)$$

де λ – коефіцієнт, який враховує сплату потенційним інвестором податку на додану вартість. У 2023 році ставка податку на додану вартість складає 20%, а коефіцієнт $\lambda = 0,8333$;

ρ – коефіцієнт, який враховує рентабельність інноваційного продукту). Приймемо $\rho = 40\%$;

ϑ – ставка податку на прибуток, який має сплачувати потенційний інвестор, у 2023 році $\vartheta = 18\%$;

Збільшення чистого прибутку 1-го року:

$\Delta П_1 = (1 \cdot 300 + 3500 \cdot 450) \cdot 0,83 \cdot 0,4 \cdot (1\text{-}0,18/100\%) = 292164,56$ грн.

Збільшення чистого прибутку 2-го року:

$\Delta П_2 = (1 \cdot 300 + 3500 \cdot (450 + 350)) \cdot 0,83 \cdot 0,4 \cdot (1\text{-}0,18/100\%) = 519612,56$ грн.

Збільшення чистого прибутку 3-го року:

$\Delta П_3 = (1 \cdot 300 + 3500 \cdot (450 + 350 + 200)) \cdot 0,83 \cdot 0,4 \cdot (1\text{-}0,18/100\%) = 649440,7$ грн.

Приведена вартість збільшення всіх чистих прибутків *ПП*, що їх може отримати потенційний інвестор від можливого впровадження та комерціалізації науково-технічної розробки:

$$ПП = \sum_{i=1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, \quad (4.17)$$

де $\Delta П_i$ – збільшення чистого прибутку у кожному з років, протягом яких виявляються результати впровадження науково-технічної розробки, грн;

T – період часу, протягом якого очікується отримання позитивних результатів від впровадження та комерціалізації науково-технічної розробки, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, τ=18%;

t – період часу (в роках) від моменту початку впровадження науково-технічної розробки до моменту отримання потенційним інвестором додаткових чистих прибутків у цьому році.

$$ПП = 292164{,}56 /(1+0{,}18)^1 + 519612{,}56 /(1+0{,}18)^2 + 649440{,}7 /(1+0{,}18)^3 =$$

$$= 981894{,}33 \text{ грн.}$$

Величина початкових інвестицій PV, які потенційний інвестор має вкласти для впровадження і комерціалізації науково-технічної розробки:

$$PV = k_{інв} \cdot ЗВ, \tag{4.18}$$

де $k_{інв}$ – коефіцієнт, що враховує витрати інвестора на впровадження науково-технічної розробки та її комерціалізацію, приймаємо $k_{інв}$=2;

$ЗВ$ – загальні витрати на проведення науково-технічної розробки та оформлення її результатів, приймаємо 148717,17 грн.

$PV = k_{інв} \cdot ЗВ$ = 2* 148717,17 = 297434,33 грн.

Абсолютний економічний ефект $E_{абс}$ для потенційного інвестора від можливого впровадження та комерціалізації науково-технічної розробки становитиме:

$$E_{абс} = ПП - PV \tag{4.19}$$

де $ПП$ – приведена вартість зростання всіх чистих прибутків від можливого впровадження та комерціалізації науково-технічної розробки,

981894,33 грн;

PV – теперішня вартість початкових інвестицій, 297434,33 грн.

$E_{абс} = ПП - PV$ = 981894,33 - 297434,33 = 684459,99 грн.

Внутрішня економічна дохідність інвестицій $E_в$, які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки:

$$E_в = \sqrt[Tж]{1 + \frac{E_{абс}}{PV}} - 1, \quad (4.20)$$

де $E_{абс}$ – абсолютний економічний ефект вкладених інвестицій, грн;

PV – теперішня вартість початкових інвестицій, грн;

$T_ж$ – життєвий цикл науково-технічної розробки, тобто час від початку її розробки до закінчення отримування позитивних результатів від її впровадження, 3 роки.

$E_в = \sqrt[Tж]{1 + \frac{E_{абс}}{PV}} - 1$ = (1+684459,99 /297434,33)$^{1/3}$ – 1 = 0,78.

Мінімальна внутрішня економічна дохідність вкладених інвестицій $\tau_{мін}$:

$$\tau_{мін} = d + f, \quad (4.21)$$

де d – середньозважена ставка за депозитними операціями в комерційних банках; в 2023 році в Україні d =0,1;

f – показник, що характеризує ризикованість вкладення інвестицій, приймемо 0,25.

$\tau_{мін}$ = 0,1+0,25 = 0,35 < 0,78 свідчить про те, що внутрішня економічна дохідність інвестицій $E_в$, які можуть бути вкладені потенційним інвестором у

впровадження та комерціалізацію науково-технічної розробки вища мінімальної внутрішньої дохідності. Тобто інвестувати в науково-дослідну роботу за темою «Інформаційна технологія онтологічного моделювання бази знань з організації бібліотеки» доцільно.

Період окупності інвестицій $T_{ок}$ які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки:

$$T_{ок} = \frac{1}{E_в}, \tag{4.22}$$

де $E_в$ – внутрішня економічна дохідність вкладених інвестицій.

$T_{ок}$ = 1 / 0,78 = 1,3 р.

$T_{ок}$ < 3-х років, що свідчить про комерційну привабливість науково-технічної розробки і може спонукати потенційного інвестора профінансувати впровадження даної розробки та виведення її на ринок.

ВИСНОВКИ

У ході виконання магістерської кваліфікаційної роботи було виконано усі поставлені задачі. Було проведено аналіз напрямків кібергігієни. Було проаналізовано актуальність проведення оцінювання рівня кібергігієни особи на підприємствах. Проведено аналіз існуючих засобів оцінювання рівня кібергігієни.

Визначено, що проблема є доволі актуальною. Прийнято рішення підвищити рівень інформаційної безпеки шляхом розробки інформаційної технології для тестування працівників підприємств. Для виконання даної задачі було спроектовано архітектуру програмного засобу та бази даних питань і навчальних матеріалів. Також було обрано технології програмування для вирішення задачі.

Виконано розробку структури інформаційної технології оцінювання рівня кібергігієни особи, що включає у себе процес підготовки опитування, процес вибору модулів опитування, процес проходження тесту та запису результатів до бази даних, процес оцінки результатів згідно зі шкалою оцінювання.

Виконано обґрунтування вибору інструментальних засобів розробки. Результати: мова програмування - Python, середовище розробки – Visual Studio Code. На основі створених вимог до програмного засобу, створених алгоритмів та архітектури системи, створено програмний засіб, що реалізує інформаційну технологію оцінювання рівня кібергігієни особи. Створений програмний засіб має простий та зрозумілий інтерфейс. Для використання потрібно лише запустити виконуваний файл, який знаходиться у папці разом із необхідними файлами.

Проведено тестування розробленого програмного засобу. Тестування проводилось для двох сценаріїв роботи: при використанні правильних даних та при використанні неправильних даних. Помилки при введенні початкових

даних обробляються, а відповідні повідомлення надаються користувачу для усунення проблем. Також розроблений програмний засіб надає користувачеві актуальну інформацію щодо його рівня знань за декількома напрямками кібергігієни, навчальні матеріали та рекомендації для вдосконалення знань.

Згідно проведених досліджень щодо рівня комерційного потенціалу розробки, результати вказують на комерційну важливість проведення даних досліджень (рівень комерційного потенціалу розробки є вищим за середній). Результати свідчать про доцільність проведення наукових досліджень.

Даний програмний засіб є корисним застосунком, який підвищує рівень інформаційної безпеки підприємств та держави в цілому шляхом оцінювання рівня кібергігієни працівників. Також власники підприємств можуть відстежувати динаміку знань працівників, порівнюючи результати проходження тестів в різні проміжки часу.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Making The World A Safer Place Through (Cyber) Hygiene. URL: https://www.forbes.com/sites/forbestechcouncil/2022/02/25/making-the-world-a-safer-place-through-cyber-hygiene/?sh=491b8a8e1d7f (дата звернення 05.11.2023)
2. What is cyber hygiene and why is it important? URL: https://www.techtarget.com/searchsecurity/definition/cyber-hygiene (дата звернення 08.11.2023)
3. How to Implement & Assess Your Cyber Hygiene. URL: https://www.cisecurity.org/insights/blog/how-to-implement-assess-your-cyber-hygiene (дата звернення 09.11.2023)
4. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення 10.11.2023).
5. Методичний посібник для тренерів з питань кібергігієни. URL: https://www.osce.org/files/f/documents/e/e/492655.pdf (дата звернення 10.11.2023)
6. Дія.Освіта. URL: https://osvita.diia.gov.ua (дата звернення 10.11.2023)
7. Здолати шахрая. URL: https://game.ema.com.ua (дата звернення 14.11.2023)
8. Cyberacademy. Кібергігієна для підприємців. URL: https://www.cyber.academy/kiberbezpeka (дата звернення 14.11.2023)
9. Як? Практичні поради. URL: https://yak.dslua.org (дата звернення 17.11.2023)
10. Цифрограм. Телеграм-бот для оцінки рівня кібергігієни. URL: https://t.me/digigram_ua_bot (дата звернення 18.11.2023)

11. Google Jigsaw. URL: https://phishingquiz.withgoogle.com/?hl=uk (дата звернення 20.11.2023)

12. Cybereducation.URL: https://cybereducation.org/mc/index.php/ us r/login/registration (дата звернення 24.11.2023)

13. Єшко. URL: https://eshko.ua/cybersecurity.html (дата звернення 24.11.2023)

14. Рекомендації з кібергігієни. URL: https://cybermonth.cip.gov.ua/ everyone/cyber-recommendations/index.html (дата звернення 27.11.2023)

15. Правила безпеки у кіберпросторі – рекомендації кіберполіції. URL: https://cyberpolice.gov.ua/article/pravyla-bezpeky-u-kiberprostori--rekomendacziyi-kiberpolicziyi-1747/ (дата звернення 28.11.2023)

16. What all businesses should know about cyber hygiene. URL: https://sopa.tulane.edu/blog/cyber-hygiene (дата звернення 28.11.2023)

17. Що таке Python? URL: https://acode.com.ua/intro-python/ (дата звернення 30.11.2023)

18. 7 редакторів коду та IDE для Python. URL: https://robotdreams.cc/uk/blog/160-7-redaktorov-koda-i-ide-dlya-python (дата звернення 01.12.2023)

19. What is SQLite? URL: https://www.sqlite.org/index.html (дата звернення 02.12.2023)

20. Flask documentation. URL: https://flask.palletsprojects.com/en/3.0.x/ (дата звернення 06.12.2023)

21. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт / Уклад. : В. О. Козловський, О. Й. Лесько, В. В. Кавецький. – Вінниця : ВНТУ, 2021. (дата звернення 06.12.2023)

ДОДАТКИ

ПРОТОКОЛ ПЕРЕВІРКИ МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Інформаційна технологія оцінювання рівня кібергігієни особи

Автор роботи: Федорова Анастасія Вячеславівна

Тип роботи: магістерська кваліфікаційна робота

Підрозділ кафедра захисту інформації ФІТКІ
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність – 91,33 %. Схожість – 8,67 %.

Аналіз звіту подібності (відмітити потрібне):

√ 1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

□ 2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

□ 3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Валентина КАПЛУН
(підпис)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Анастасія ФЕДОРОВА
(підпис)

Керівник роботи _____ Леонід КУПЕРШТЕЙН

Додаток Б

Додаток Б

Повний перелік питань тесту

1) Кібергігієна паролів

Питання: Який вид паролю вважається більш безпечним?
a) Пароль123
b) !2#Gp$Xm
c) Користувач
d) 123456
Відповідь: b) !2#Gp$Xm

Питання: Яка стратегія парольної безпеки включає в себе використання різних паролів для різних облікових записів?
a) Парольна фраза
b) Періодична зміна паролю
c) Використання одного паролю для всіх облікових записів
d) Двофакторна аутентифікація
Відповідь: a) Парольна фраза

Питання: Які елементи найбільше підвищують безпеку паролів?
a) Великі літери та цифри
b) Використання ім'я користувача
c) Парольна фраза
d) Публічно доступні дані
Відповідь: c) Парольна фраза

Питання: Які недоліки використання одного і того ж паролю для кількох сервісів?
a) Забезпечує легше управління паролями
b) Збільшує ризик для кіберзлочинців
c) Спрощує процес запам'ятовування паролів
d) Зменшує час на введення пароля
Відповідь: b) Збільшує ризик для кіберзлочинців

Питання: Як часто рекомендується змінювати паролі?
a) Раз на тиждень
b) Раз на місяць
c) Тільки у випадку компрометації
d) Раз на рік
Відповідь: c) Тільки у випадку компрометації

Питання: Де надійніше всього зберігати паролі, щоб до них не дістався жоден злочинець?
a) На клаптику паперу, схованому під клавіатурою
b) В спеціальній програмі для збереження паролів
c) У голові
d) У блокноті на робочому столі комп'ютера
Відповідь: В спеціальній програмі для збереження паролів

Питання: Як можна покращити запам'ятовування складних паролів?
a) Використання того самого паролю для різних облікових записів
b) Запис паролів на стікерах та клейках паперів
c) Використання парольних менеджерів
d) Зберігання паролів у недоступному для інших місці
Відповідь: c) Використання парольних менеджерів

Ситуація: Ваш колега залишив комп'ютер включеним і невимкненим на кілька годин. Як ви реагуєте щодо захисту паролю?
a) Нічого не роблю
b) Змінюю пароль
c) Повідомляю керівництво
d) Змінюю пароль і підказую колегові
Відповідь: b) Змінюю пароль

Ситуація: Якщо ваш пароль містить особисті дані, такі як ім'я чи дата народження, що ви робите?
a) Продовжую використовувати його, оскільки мені легко його пам'ятати
b) Додаю до нього числа та символи для зміцнення безпеки
c) Змінюю його на інший, який не містить особистих даних
d) Написуєте його на видному місці для легкого доступу
Відповідь: c) Змінюю його на інший, який не містить особистих даних

Ситуація: Ви отримали лист від сервісу електронної пошти про підозрілу активність у вашому обліковому записі. Що ви робите?
a) Клікаю на посилання у листі та вводжу пароль
b) Ігнорую лист
c) Заходжу на веб-сайт сервісу електронної пошти, не використовуючи посилання
d) Видаляю лист
Відповідь: c) Заходжу на веб-сайт сервісу електронної пошти, не використовуючи посилання

Ситуація: Ви отримали лист із запитанням про ваш пароль. Як ви реагуєте?
a) Надсилаю свій пароль
b) Видаляю лист
c) Звертаюся до служби підтримки
d) Міняю пароль
Відповідь: b) Видаляю лист

Ситуація: Ваш пароль включає ваше ім'я та дату народження. Що ви робите?
a) Залишаю пароль як є
b) Змінюю пароль на більш складний
c) Використовую цей пароль для всіх облікових записів
d) Змінюю пароль на ім'я домашнього улюбленця
Відповідь: b) Змінюю пароль на більш складний

Ситуація: Ви помітили, що ваш колега зберігає паролі на клейках паперів на своєму робочому столі. Як ви реагуєте?
a) Нічого не роблю
b) Заохочую його це робити, якщо це йому зручно
c) Повідомляю керівництво

d) Ділюся своїм паролем для прикладу
Відповідь: c) Повідомляю керівництво

2) Кібергігієна мобільних пристроїв

Питання: Яким чином двофакторна аутентифікація забезпечує додатковий рівень безпеки на мобільних пристроях?
a) Забезпечує шифрування файлів
b) Вимагає двох різних мобільних пристроїв
c) Використовує два різних методи аутентифікації
d) Змінює пароль двічі на місяць
Відповідь: c) Використовує два різних методи аутентифікації

Питання: Яка загроза може виникнути при використанні відкритого Wi-Fi на мобільному пристрої?
a) Затримка в роботі додатків
b) Зменшення рівня заряду батареї
c) Витік особистих даних через непрошений доступу до мережі
d) Втрата файлів з пристрою
Відповідь: c) Витік особистих даних через непрошений доступу до мережі
Питання: Які заходи можна прийняти для захисту мобільного пристрою від несанкціонованого доступу?
a) Завжди вимикати антивірус
b) Використовувати прості паролі
c) Активувати пароль або використовувати відбитки пальців/розпізнавання обличчя
d) Ділитися паролем з близькими друзями
Відповідь: c) Активувати пароль або використовувати відбитки пальців/розпізнавання обличчя

Питання: Чому важливо оновлювати операційну систему та додатки на мобільному пристрої?
a) Для зміни інтерфейсу
b) Збільшення швидкості пристрою
c) Покращення безпеки та виправлення вразливостей
d) Зменшення споживання інтернет-трафіку
Відповідь: c) Покращення безпеки та виправлення вразливостей

Питання: Який захід безпеки може допомогти у випадку втрати мобільного пристрою?
a) Зміна паролю на соціальних мережах
b) Блокування пристрою за допомогою паролю чи відбитка пальця
c) Використання гучного сигналу для знаходження пристрою
d) Закриття усіх облікових записів у віддаленому режимі
Відповідь: d) Закриття усіх облікових записів у віддаленому режимі.

Питання: Які загрози можуть виникнути внаслідок використання неофіційних додатків на мобільних пристроях?
a) Зниження ризику вірусів та шкідливих програм
b) Збільшення швидкості роботи пристрою
c) Можливість встановлення шкідливих програм та втрата особистої інформації
d) Забезпечення додаткового захисту від зловмисників

Відповідь: c) Можливість встановлення шкідливих програм та втрата особистої інформації

Ситуація: Якщо ваш мобільний пристрій втратив доступ до інтернету та автономно встановлює додаток, що ви робите?

a) Ігнорую це явище, оскільки це, ймовірно, нормальне оновлення

b) Вимикаю мобільний інтернет та видаляю автоматично встановлене додаток

c) Залишаю все як є, сподіваючись, що це не є загрозою

d) Звертаюся до служби підтримки виробника пристрою

Відповідь: b) Вимикаю мобільний інтернет та видаляю автоматично встановлене додаток

Ситуація: Під час користування відкритим Wi-Fi ви помітили незвичайну активність на своєму мобільному пристрої. Як ви реагуєте?

a) Продовжу користуватися мережею, ігноруючи незвичайну активність

b) Відключу Wi-Fi і перейду на мобільний інтернет

c) Запитаю персонал кафе щодо стану їхньої мережі

d) Завершу всі сеанси та вимкну Wi-Fi

Відповідь: d) Завершу всі сеанси та вимкну Wi-Fi.

Ситуація: Якщо ви отримали SMS-повідомлення з невідомого джерела з пропозицією отримати премію від керівництва з можливістю перейти за посиланням, що ви робите?

a) Переходжу за посиланням, оскільки можливість виграти приз виглядає привабливо

b) Видаляю повідомлення без перегляду

c) Питаю колег, чи вони отримали подібне повідомлення

d) Надсилаю відповідь із своїм номером телефону для отримання премії

Відповідь: b) Видаляю повідомлення без перегляду

3) Кібергігієна електронної пошти

Питання: Як можна забезпечити безпеку паролів для доступу до електронної пошти?

a) Використання простих та загальних паролів

b) Регулярна зміна паролів

c) Відправка паролів по електронній пошті

d) Зберігання паролів у відкритому тексті

Відповідь: b) Регулярна зміна паролів

Питання: Як зберегти конфіденційність електронної переписки?

a) Використовувати відкриті мережі для відправлення конфіденційної інформації

b) Використовувати шифрування для електронних листів

c) Надсилати паролі у тексті листа

d) Залишати електронні листи у непризначених для цього папках

Відповідь: b) Використовувати шифрування для електронних листів

Ситуація: Співробітник отримав лист від невідомого відправника з проханням надати конфіденційну інформацію. Яким чином слід вчинити?

a) Негайно відправити запитання на визначення особистості відправника

b) Надати запитувану інформацію без будь-якої перевірки

c) Залишити лист без відповіді

d) Повідомити відділ безпеки про подію для подальшого аналізу
Відповідь: d) Повідомити відділ безпеки про подію для подальшого аналізу

Ситуація: Керівник підприємства отримав лист з вимогою великої суми грошей в обмін на відновлення доступу до важливих даних. Як вчинити?
a) Негайно відправити велику суму грошей для відновлення доступу
b) Вимагати докази автентичності вимог та повідомити відділ безпеки
c) Проігнорувати вимоги та спробувати вирішити проблему самостійно
d) Передати всі дані, які вимагаються, для відновлення доступу
Відповідь: b) Вимагати докази автентичності вимог та повідомити відділ безпеки

4) Кібергігієна соцмереж та месенджерів

Питання: Як захистити особистий обліковий запис в соціальній мережі від несанкціонованого доступу?
a) Використовувати один пароль для всіх соціальних мереж
b) Застосувати двоетапну аутентифікацію
c) Зберігати паролі на папері поблизу робочого місця
d) Публікувати пароль у власному профілі для власного запам'ятовування
Відповідь: b) Застосувати двоетапну аутентифікацію

Питання: Де краще обмінюватись робочою інформацією?
a) Signal
b) Facebook Messenger
c) Viber
d) WhatsApp
e) Telegram
f) Електронна пошта, надана роботодавцем
Відповідь: f) Електронна пошта, надана роботодавцем

Питання: Який спосіб краще вибрати для додаткового захисту від крадіжки профілю соціальної мережі чи месенджера?
a) Записувати всі паролі в таємний блокнот і зберігати його в недоступному для інших місці
b) Користуватись одним сильним паролем для всіх соцмереж та месенджерів
c) Реєструватись із різними email в усіх соцмережах та месенджерах, використовуючи один і той самий сильний пароль
d) Активувати в налаштуваннях профілю вхід за додатковим простим одноразовим кодом
Відповідь: d) Активувати в налаштуваннях профілю вхід за додатковим простим одноразовим кодом

Питання: Яка інформація найменш корисна для використання злочинцями в соціальних мережах?
a) Інформація, де ви з друзями робите щось разом
b) Інформація про книги вашого улюбленого письменника
c) Інформація, яка стосується лише вашої сім'ї
d) Інформація з офіційного сайту компанії, де ви працюєте
Відповідь: b) Інформація про книги вашого улюбленого письменника

Питання: Ваш колега несподівано попросив вас у месенджері переказати йому на банківську картку 1000 грн. Ваші дії?

a) Відправлю кошти на вказану карту

b) Зателефоную йому особисто для підтвердження

c) Уточню, чи це картка того самого банку, що і в мене, щоб переказати кошти без комісії

d) Уточню, для яких саме цілей, а потім перекажу кошти

Відповідь: b) Зателефоную йому особисто для підтвердження

Питання: Як забезпечити конфіденційність обговорень у корпоративних чатах?

a) Відправляти конфіденційну інформацію у відкритому тексті

b) Застосування шифрування чатів та повідомлень

c) Надсилання паролів для доступу до файлів через чат

d) Відкрита публікація обговорень в корпоративних чатах

Відповідь: b) Застосування шифрування чатів та повідомлень

Ситуація: Співробітник отримав від невідомого контакту в месенджері посилання на файлообмінник із проханням завантажити важливий файл. Як вчинити?

a) Відразу завантажити файл без будь-яких перевірок

b) Звернутися до відділу безпеки для перевірки посилання

c) Ігнорувати повідомлення та видалити контакт

d) Надіслати запитання невідомому контакту про його ідентифікацію

Відповідь: b) Звернутися до відділу безпеки для перевірки посилання

Ситуація: Керівник отримав від колеги запитання в месенджері про конфіденційну стратегічну інформацію компанії. Як вчинити?

a) Відразу відправити всю необхідну інформацію

b) Вимагати офіційного запиту через корпоративну пошту або інші безпечні канали

c) Направити запитання керівництву для визначення дій

d) Попросити колегу відправити запитання через електронну пошту для більшої безпеки

Відповідь: b) Вимагати офіційного запиту через корпоративну пошту або інші безпечні канали

5) Кібергігієна електронних платежів

Питання: Як можна захистити особисті фінансові дані під час електронних платежів?

a) Використання одного пароля для всіх електронних платформ

b) Використання безпечних і складних паролів для кожного облікового запису

c) Надсилання фінансових даних через звичайні текстові повідомлення

d) Зберігання всіх фінансових паролів на пристрої без паролю

Відповідь: b) Використання безпечних і складних паролів для кожного облікового запису

Питання: Як використовувати мобільні платіжні додатки безпечно?

a) Зберігати паролі до додатків на записках поруч із телефоном

b) Використовувати невідомі та недовірені додатки для платежів

c) Використовувати двофакторну аутентифікацію та біометричні дані

d) Ділитися паролем до додатку з друзями

Відповідь: c) Використовувати двофакторну аутентифікацію та біометричні дані

Питання: Як використовувати публічні Wi-Fi мережі безпечно під час здійснення електронних платежів?

a) Використовувати тільки особистий мобільний інтернет

b) Заборона використання будь-яких публічних Wi-Fi для платежів

c) Використання віртуальної приватної мережі (VPN)

d) Надсилання фінансових даних без шифрування

Відповідь: c) Використання віртуальної приватної мережі (VPN)

Питання: Чому важливо перевіряти витрати в банківському висновку?

a) Для ведення статистики власних витрат

b) Для вчасного виявлення неправомірних транзакцій

c) Тільки, якщо у вас обмежений бюджет

d) Щоб публікувати в соцмережах свої фінансові витрати

Відповідь: b) Для вчасного виявлення неправомірних транзакцій

Питання: Які переваги має використання одноразових віртуальних карток для онлайн-платежів?

a) Збільшується ризик втрати грошей

b) Забезпечується постійна доступність кредиту

c) Зменшується ризик крадіжки інформації

d) Всі вищенаведені варіанти

Відповідь: c) Зменшується ризик крадіжки інформації

Ситуація: Користувач отримав електронне повідомлення про підозрілу транзакцію на своєму банківському рахунку. Як слід вчинити?

a) Проігнорувати повідомлення, оскільки це, ймовірно, шахрайська атака

b) Негайно звернутися до банку для перевірки та блокування неправомірних транзакцій

c) Видалити всі фінансові деталі з облікового запису

d) Надіслати всі фінансові дані у відповідь на це повідомлення

Відповідь: b) Негайно звернутися до банку для перевірки та блокування неправомірних транзакцій

Ситуація: Користувач випадково надіслав гроші невідомому одержувачеві через електронну платіжну платформу. Як вирішити цю ситуацію?

a) Намагатися скасувати транзакцію самостійно

b) Негайно повідомити платіжну платформу та звернутися до служби підтримки

c) Ігнорувати ситуацію, оскільки нічого не можна змінити

d) Вимагати повернення грошей у невідомого одержувача

Відповідь: b) Негайно повідомити платіжну платформу та звернутися до служби підтримки

Ситуація: Під час введення платіжних даних на публічному комп'ютері користувач помітив підозрілі програми. Як вчинити в цьому випадку?

a) Терміново завершити проведення транзакції та вийти з системи

b) Продовжити введення даних, оскільки це, ймовірно, нормальне явище

c) Зберегти платіжні дані на комп'ютері для зручності

d) Повідомити адміністратора комп'ютера та службу підтримки платіжної платформи

Відповідь: a) Терміново завершити проведення транзакції та вийти з системи

Ситуація: Якщо ви випадково надали невірні банківські реквізити при онлайн-платежі, що ви робите?

a) Ігнорую помилку, оскільки це не є серйозним

b) Негайно повідомляю банк і змінюю паролі

c) Змінюю інформацію на іншу вірну

d) Публікую цю помилку на соцмережах для поради

Відповідь: b) Негайно повідомляю банк і змінюю паролі

6) Кібергігієна технології WI-FI

Питання: Як можна забезпечити безпеку Wi-Fi мережі?

a) Використання стандартного пароля, наданого провайдером

b) Зміна пароля за замовчуванням та використання складного пароля WPA2 або WPA3

c) Вимкнення всіх методів шифрування для забезпечення високої швидкості

d) Надсилання паролю для спільного використання мережі

Відповідь: b) Зміна пароля за замовчуванням та використання складного пароля WPA2 або WPA3

Питання: Як виявити, чи використовуються моєю Wi-Fi мережею несанкціоновані пристрої?

a) Періодично змінювати пароль для виключення доступу несанкціонованих пристроїв

b) Використовувати функцію моніторингу підключених пристроїв у налаштуваннях маршрутизатора

c) Включити режим гостьової мережі для ізоляції несанкціонованих пристроїв

d) Вимагати від кожного пристрою сканувати QR-код для підключення до мережі

Відповідь: b) Використовувати функцію моніторингу підключених пристроїв у налаштуваннях маршрутизатора

Питання: Як використовувати Wi-Fi безпечно в громадських місцях?

a) Використовувати тільки мережі з відкритим доступом без шифрування

b) Включити VPN для захисту передачі даних через відкриті мережі

c) Вимагати від всіх користувачів введення особистих даних для безпеки

d) Використовувати один і той самий пароль для всіх громадських мереж

Відповідь: b) Включити VPN для захисту передачі даних через відкриті мережі

Питання: Як вберегти свою Wi-Fi мережу від атаки "Man-in-the-Middle"?

a) Використовувати відкриті мережі для уникнення атак

b) Заблокувати всі підключення, крім свого пристрою

c) Використовувати безпечні протоколи шифрування та VPN

d) Регулярно змінювати пароль мережі

Відповідь: c) Використовувати безпечні протоколи шифрування та VPN

Питання: Які переваги має використання хмарових Wi-Fi мереж?

a) Зменшення швидкості з'єднання

b) Забезпечення додаткових точок доступу

c) Покращення безпеки та управління мережею віддалено

d) Збільшення кількості підключених пристроїв

Відповідь: c) Покращення безпеки та управління мережею віддалено

Питання: Чому важливо вимикати Wi-Fi на пристроях, коли вони не використовуються?

a) Для економії електроенергії
b) Зменшення шансів несанкціонованого доступу до мережі
c) Тільки, якщо ви використовуєте обмежений трафік
d) Зменшення швидкості Інтернет-з'єднання
Відповідь: b) Зменшення шансів несанкціонованого доступу до мережі

Ситуація: Якщо ваша Wi-Fi мережа виявляється в результаті пошуку, що ви робите, щоб збільшити безпеку?
a) Публікую назву мережі на форумах для зручності
b) Вимикаю трансляцію SSID для уникнення виявлення
c) Міняю пароль для забезпечення безпеки
d) Додаю всіх сусідів до своєї мережі для обміну трафіком
Відповідь: b) Вимикаю трансляцію SSID для уникнення виявлення

Ситуація: Користувач помітив підозрілу активність у своєму списку підключених пристроїв до мережі. Як вчинити?
a) Ігнорувати ситуацію, оскільки це може бути звичайний збій мережі
b) Змінити пароль мережі і відключити всі пристрої, крім дозволених
c) Надсилати підозрілому пристрою запитання про його призначення
d) Припинити використання Wi-Fi та виключити маршрутизатор для додаткової безпеки
Відповідь: b) Змінити пароль мережі і відключити всі пристрої, крім дозволених

7) Кібергігієна споживання інформації

Питання: Як розпізнати фейкові новини та перевірити достовірність інформації в Інтернеті?
a) Вірити кожній новині, яка виглядає цікаво
b) Перевіряти джерело інформації та шукати підтвердження від інших надійних джерел
c) Ділитися будь-якою інформацією без перевірки
d) Визначати достовірність інформації за кількістю лайків та репостів
Відповідь: b) Перевіряти джерело інформації та шукати підтвердження від інших надійних джерел

Питання: Як забезпечити приватність в Інтернеті під час споживання новин та контенту?
a) Використовувати тільки відкриті профілі в соціальних мережах
b) Забороняти доступ до персональних даних на всіх веб-сайтах
c) Використання VPN та інших інструментів для шифрування інтернет-з'єднання
d) Публікувати всю особисту інформацію в мережі для більшої доступності
Відповідь: c) Використання VPN та інших інструментів для шифрування інтернет-з'єднання

Питання: Як визначити, чи є веб-сайт безпечним для перегляду та введення особистих даних?
a) Перевіряти, чи виглядає веб-сайт стильно та модно
b) Перевіряти наявність знаку "https://" у веб-адресі та шифрування даних
c) Надсилати всі особисті дані через невідомі веб-сайти
d) Ігнорувати попередження безпеки від браузера
Відповідь: b) Перевіряти наявність знаку "https://" у веб-адресі та шифрування даних

Питання: Як уникнути попадання в пастку фішингових веб-сайтів, що виглядають як відомі сервіси?

a) Клікати на всі посилання без перевірки

b) Перевіряти URL-адресу та використовувати офіційні додатки та розширення для браузера

c) Надсилати конфіденційні дані через будь-які підозрілі веб-сайти

d) Використовувати тільки відкриті Wi-Fi для перегляду веб-сайтів

Відповідь: b) Перевіряти URL-адресу та використовувати офіційні додатки та розширення для браузера

Питання: Як розпізнати фейковий телефонний дзвінок від шахраїв, що намагаються отримати ваші особисті дані?

a) Надавати всі відповіді на телефонний дзвінок без перевірки

b) Перевіряти номер телефону та шукати відгуки в інтернеті

c) Вказувати всі свої особисті дані без будь-яких сумнівів

d) Вважати, що всі дзвінки від невідомих номерів є надійними

Відповідь: b) Перевіряти номер телефону та шукати відгуки в інтернеті

Ситуація: Як розпізнати фейковий коментар або відгук на веб-сайті?

a) Перевіряти, чи всі коментарі є позитивними, без жодних негативних відгуків

b) Звертати увагу на стиль написання та граматичні помилки

c) Вважати, що всі коментарі на веб-сайті є правдивими

d) Використовувати однаковий пароль на всіх веб-сайтах для зручності

Відповідь: b) Звертати увагу на стиль написання та граматичні помилки

Ситуація: Користувач отримав посилання на електронну пошту, яке здається підозрілим. Як вчинити?

a) Негайно клікнути на посилання для отримання додаткової інформації

b) Відправити електронного листа в спам та видалити його

c) Перевірити відправника та адресу посилання перед відкриттям

d) Відправити всі свої особисті дані у відповідь на це електронне повідомлення

Відповідь: c) Перевірити відправника та адресу посилання перед відкриттям

8) Кібергігієна персонального комп’ютера

Питання: Як забезпечити безпеку віддаленого доступу до персонального комп'ютера?

a) Включення безпечного режиму віддаленого доступу та використання слабкого пароля

b) Відмова від віддаленого доступу для заощадження енергії

c) Використання найпростіших паролів для віддаленого доступу

d) Встановлення двофакторної аутентифікації та регулярне оновлення паролів

Відповідь: d) Встановлення двофакторної аутентифікації та регулярне оновлення паролів

Питання: Важливо не залишати свій пристрій у ввімкненому (незаблокованому) стані, якщо ви навіть на кілька хвилин відходите від робочого місця. Яка комбінація клавіш дозволяє заблокувати персональний комп’ютер/ноутбук на ОС Windows?

a) Windows +F1

b) Windows + R

c) Windows + L

d) Немає правильної відповіді

Відповідь: c) Windows + L

Ситуація: Користувач помітив підозрілі активності на своєму комп'ютері, що може вказувати на вторгнення. Як вчинити?

a) Продовжити роботу та ігнорувати підозрілу активність

b) Вимкнути комп'ютер та звернутися до інформаційно-технічного відділу

c) Змінити паролі та видалити всі важливі дані

d) Відправити повідомлення хакерам з проханням припинити вторгнення

Відповідь: b) Вимкнути комп'ютер та звернутися до інформаційно-технічного відділу

Ситуація: Користувач помітив, що його веб-камера активується без його дозволу. Як вчинити для захисту приватності?

a) Продовжувати використовувати комп'ютер, оскільки це може бути звичайний збій

b) Пошукати та вимкнути всі процеси, які активують веб-камеру без дозволу

c) Заклеїти веб-камеру стрічкою чи спеціальними наклейками

d) Відправити запит до виробника комп'ютера для вирішення проблеми

Відповідь: b) Пошукати та вимкнути всі процеси, які активують веб-камеру без дозволу

9) Соціальна інженерія

Питання: Ви отримали електронний лист від невідомого вам відправника, який запитує ваш логін та пароль для «оновлення безпеки облікового запису». Як ви вчините?

a) Відправите логін та пароль, оскільки це може бути важливим оновленням безпеки.

b) Зателефонуєте або напишете в службу підтримки, щоб перевірити листа.

c) Негайно відправите лист у спам та ігноруйте його.

d) Відправите логін та пароль, але попередьте колег про це.

Відповідь: b) Зателефонуєте або напишете в службу підтримки, щоб перевірити листа.

Ситуація: Ви отримали запитання від колеги в соціальній мережі, яке просить надати конфіденційну інформацію про проект компанії. Як ви реагуєте?

a) Надаєте інформацію, так як це від вашого колеги.

b) Запитуєте, чому йому/їй потрібна ця інформація та вказуєте на політику конфіденційності компанії.

c) Проігнорюєте запитання та видаляєте повідомлення.

d) Запитуєте, чому він/вона не звернувся до вас напряму в офісі.

Відповідь: b) Запитуєте, чому йому/їй потрібна ця інформація та вказуєте на політику конфіденційності компанії.

Ситуація: Одного дня невідома особа приходить в ваш офіс, представляючись співробітником технічної підтримки і просить вас надати пароль від вашого комп'ютера для "перевірки системи". Як ви дієте?

a) Віддасте пароль, оскільки він вас запросив і виглядає як професіонал.

b) Запитаєте його про ідентифікацію та зверніться до відділу безпеки.

c) Віддасте пароль, але змініть його після його візиту.

d) Запитаєте його про пароль для підтвердження його ідентичності.

Відповідь: b) Запитайте його про ідентифікацію та зверніться до відділу безпеки.

Ситуація: Ви отримали телефонний дзвінок від особи, яка стверджує, що є технічним спеціалістом із відділу IT, і просить ваш логін та пароль для вирішення проблеми з вашим обліковим записом. Як ви реагуєте?

a) Віддасте логін та пароль, оскільки це може допомогти вирішити проблему.

b) Запитуєте його про ідентифікацію та повідомляєте відділ безпеки.

c) Запитуєте, чому він/вона не вирішує проблему через службу підтримки.

d) Просите його надіслати вам листа або повідомлення із запитанням.

Відповідь: b) Запитуєте його про ідентифікацію та повідомляєте відділ безпеки.

Ситуація: Вам надійшов лист від колеги, який просить вас відправити копію конфіденційного документа з клієнтською інформацією. Як ви реагуєте?

a) Негайно відправляєте копію документа, так як це від колеги.

b) Запитуєте про причину і необхідність відправлення цієї інформації.

c) Ігноруєте лист та не відправляєте жодну конфіденційну інформацію.

d) Звертаєтесь до відділу безпеки для перевірки легітимності запитання.

Відповідь: b) Запитуєте про причину і необхідність відправлення цієї інформації.

Ситуація: Під час обіду в кав'ярні невідома особа збирається до вашого столу, представляючись співробітником з іншого відділу і запитує вас про ваші обов'язки та доступ до інформації. Як ви реагуєте?

a) Розповідаєте всю інформацію, так як вам цікаво, хто він/вона.

b) Запитуєте про його/її ідентифікацію та вказуєте, що такі питання потрібно обговорювати в офісі.

c) Завершуєте розмову і переходите до іншого столу.

d) Питаєте про мету цих запитань та чому це важливо.

Відповідь: b) Запитуєте про його/її ідентифікацію та вказуєте, що такі питання потрібно обговорювати в офісі.

Додаток В

Текст програми

main.py

```
from flask import Flask, render_template, request, redirect, url_for, flash,
session, jsonify
import sqlite3
from random import choice
from string import ascii_letters

app = Flask(__name__)
app.secret_key = 'your_secret_key'

# Підключення до бази даних та створення таблиці користувачів
with sqlite3.connect("users.db") as connection:
    cursor = connection.cursor()
    cursor.execute("""
        CREATE TABLE IF NOT EXISTS users (
            id INTEGER PRIMARY KEY AUTOINCREMENT,
            login TEXT NOT NULL,
            password TEXT NOT NULL,
            admin BOOLEAN NOT NULL
        )
    """)
    connection.commit()

def is_admin():
    # Функція для перевірки, чи користувач має права адміністратора
    user_id = session.get('user_id')
    if user_id is not None:
        with sqlite3.connect("users.db") as connection:
            cursor = connection.cursor()
            cursor.execute("SELECT admin FROM users WHERE id=?", (user_id,))
            admin_status = cursor.fetchone()
            return admin_status[0] if admin_status else False
    return False

# Підключення до бази даних та створення таблиць для опитувань
with sqlite3.connect("survey.db") as connection:
    cursor = connection.cursor()
    cursor.execute("""
        CREATE TABLE IF NOT EXISTS topics (
            id INTEGER PRIMARY KEY AUTOINCREMENT,
            name TEXT NOT NULL,
            admin_id INTEGER NOT NULL,
            FOREIGN KEY (admin_id) REFERENCES users (id)
        )
    """)
    connection.commit()

    cursor.execute("""
        CREATE TABLE IF NOT EXISTS questions (
            id INTEGER PRIMARY KEY AUTOINCREMENT,
```

```
            topic_id INTEGER NOT NULL,
            question TEXT NOT NULL,
            answers TEXT NOT NULL,
            docs TEXT,
            correct_answer TEXT NOT NULL,
            FOREIGN KEY (topic_id) REFERENCES topics (id)
        )
    """)
    connection.commit()
    cursor = connection.cursor()
    cursor.execute("""
        CREATE TABLE IF NOT EXISTS user_results (
            id INTEGER PRIMARY KEY AUTOINCREMENT,
            user_id INTEGER NOT NULL,
            question_id INTEGER NOT NULL,
            selected_answer TEXT NOT NULL,
            is_correct BOOLEAN NOT NULL,
            session_id INT NOT NULL,
            FOREIGN KEY (user_id) REFERENCES users (id),
            FOREIGN KEY (question_id) REFERENCES questions (id)
        )
    """)
    connection.commit()

# Головна сторінка - відображення форми для створення теми та питань
@app.route('/create_survey', methods=['GET', 'POST'])
def create_survey():
    if is_admin():
        if request.method == 'POST':
            topic_name = request.form['topic']
            questions_data = request.form.getlist('question')
            answers_data = request.form.getlist('answers')
            docs_data = request.form.getlist('docs')
            correct_answers_data = request.form.getlist('correct_answer')

            with sqlite3.connect("survey.db") as connection:
                cursor = connection.cursor()
                cursor.execute(
                    "INSERT INTO topics (name, admin_id) VALUES (?, ?)",
(topic_name, session['user_id']))
                topic_id = cursor.lastrowid

                for question, answers, docs, correct_answer in
zip(questions_data, answers_data, docs_data, correct_answers_data):
                    cursor.execute("""
                        INSERT INTO questions (topic_id, question, answers,
docs, correct_answer)
                        VALUES (?, ?, ?, ?, ?)
                    """, (topic_id, question, answers, docs, correct_answer))

                connection.commit()

                flash('Тема і питання успішно додані!', 'success')
                return redirect(url_for('create_survey'))
```

```
        return render_template('create_survey.html')
    else:
        flash('Недостатньо прав для створення опитування. Потрібен статус
адміністратора.', 'danger')
        return redirect(url_for('index'))

@app.route('/choose_survey')
def choose_survey():
    if session.get('user_id') is not None:
        with sqlite3.connect("survey.db") as connection:
            cursor = connection.cursor()
            cursor.execute("SELECT id, name FROM topics")
            topics = cursor.fetchall()
            return render_template('choose_survey.html', topics=topics)
    else:
        flash('Для вибору опитування необхідно увійти в систему.', 'danger')
        return redirect(url_for('login'))

# Обробка вибору опитування та відображення питань
@app.route('/take_survey/<int:topic_id>', methods=['GET', 'POST'])
def take_survey(topic_id):
    if session.get('user_id') is not None:
        if request.method == 'POST':
            session['session_id'] = ''.join(
                choice(ascii_letters) for _ in range(10))
            user_id = session['user_id']
            for question_id, selected_answer in request.form.items():
                with sqlite3.connect("survey.db") as connection:
                    cursor = connection.cursor()
                    cursor.execute("""
                        INSERT INTO user_results (user_id, question_id,
selected_answer, is_correct, session_id)
                        VALUES (?, ?, ?, ?, ?)
                    """, (user_id, question_id, selected_answer,
selected_answer == get_correct_answer(question_id), session['session_id']))
                    connection.commit()
            flash('Опитування успішно заповнено!', 'success')
            return redirect(url_for('survey_results',
session_id=session['session_id'], topic_id=topic_id))
        else:
            with sqlite3.connect("survey.db") as connection:
                cursor = connection.cursor()
                cursor.execute(
                    "SELECT id, question, answers FROM questions WHERE
topic_id=?", (topic_id,))
                questions = cursor.fetchall()
                return render_template('take_survey.html', topic_id=topic_id,
questions=questions)
    else:
        flash('Для заповнення опитування необхідно увійти в систему.',
'danger')
        return redirect(url_for('login'))
```

```
# Отримання правильної відповіді на питання з бази даних
def get_correct_answer(question_id):
    with sqlite3.connect("survey.db") as connection:
        cursor = connection.cursor()
        cursor.execute(
            "SELECT correct_answer FROM questions WHERE id=?",
(question_id,))
        return cursor.fetchone()[0]

# Сторінка старту опитування
@app.route('/start_survey/<int:topic_id>')
def start_survey(topic_id):
    if session.get('user_id') is not None:
        return render_template('start_survey.html', topic_id=topic_id)
    else:
        flash('Для початку опитування необхідно увійти в систему.', 'danger')
        return redirect(url_for('login'))

# Відображення результатів опитування
@app.route('/survey_results/<string:session_id>/<int:topic_id>')
def survey_results(session_id, topic_id):
    with sqlite3.connect("survey.db") as connection:
        cursor = connection.cursor()
        cursor.execute("""
                SELECT * FROM user_results WHERE user_results.session_id=?
            """, (session_id,))
        user_results = cursor.fetchall()
        print(user_results)
        cursor.execute("""
                SELECT * FROM questions WHERE questions.topic_id=?
""", (topic_id,))
        questions = cursor.fetchall()
        print(questions)
        results = {}
        for question in questions:
            results[question[2]] = []
            for user_result in user_results:
                if user_result[2] == question[0]:
                    results[question[2]].append(
                        (user_result[3], user_result[4], question[3],
question[4]))
        print(results)
        total_score = 0
        for question, answers in results.items():
            for answer in answers:
                total_score += answer[1]
        docs = {}
        for question, answers in results.items():
            for answer in answers:
                docs[answer[3]] = answer[1]
        print(docs)
        return render_template('survey_results.html', results=results,
total_score=total_score, docs=docs, strf=str)
```

```
# Головна сторінка
@app.route('/')
def index():
    user_id = session.get('user_id')
    if user_id is not None:
        with sqlite3.connect("users.db") as connection:
            cursor = connection.cursor()
            cursor.execute("""
                SELECT login FROM users WHERE id=?
            """, (user_id,))
            user = cursor.fetchone()
            if is_admin():
                return render_template('admin_index.html', username=user[0])
            if user:
                username = user[0]
                return render_template('index.html', username=username)

    return render_template('pls_login.html')

# Сторінка видалення опитування
@app.route('/del_survey_menu')
def del_survey_menu():
    return render_template('del_survey_menu.html')

# Сторінка входу в систему
@app.route('/login', methods=['GET', 'POST'])
def login():
    if request.method == 'POST':
        login = request.form['login']
        password = request.form['password']

        with sqlite3.connect("users.db") as connection:
            cursor = connection.cursor()

            cursor.execute("""
                SELECT * FROM users WHERE login=?
            """, (login,))
            user = cursor.fetchone()

            if user and user[2] == password:
                session['user_id'] = user[0]
                flash('Вхід успішно виконано!', 'success')
                return redirect(url_for('index'))
            else:
                flash(
                    'Неправильні облікові дані. Будь ласка, спробуйте ще
раз.', 'danger')

    return render_template('login.html')

# Сторінка виходу з системи
@app.route('/logout')
def logout():
    session.pop('user_id', None)
```

```
    flash('Ви успішно вийшли з системи.', 'info')
    return redirect(url_for('index'))

# Сторінка видалення опитування
@app.route('/delete_survey/<string:topic_name>', methods=['POST', 'GET'])
def delete_survey(topic_name):
    if is_admin():
        with sqlite3.connect("survey.db") as connection:
            cursor = connection.cursor()
            cursor.execute("""
                DELETE FROM topics WHERE name=?
            """, (topic_name,))
            connection.commit()
            return "Опитування успішно видалено! <a
href='/del_survey_menu'>Назад</a>"
    else:
        return redirect(url_for('index'))

# Сторінка реєстрації
@app.route('/register', methods=['GET', 'POST'])
def register():
    if request.method == 'POST':
        login = request.form['login']
        password = request.form['password']

        with sqlite3.connect("users.db") as connection:
            cursor = connection.cursor()

            cursor.execute("""
                SELECT id FROM users WHERE login=?
            """, (login,))
            existing_user = cursor.fetchone()
            if existing_user:
                flash(
                    'Користувач з таким логіном вже існує. Виберіть інший
логін.', 'danger')
            else:
                cursor.execute("""
                    INSERT INTO users (login, password, admin) VALUES (?, ?,
?)
                """, (login, password, False))
                connection.commit()

                flash(
                    'Реєстрація успішно виконана! Тепер ви можете увійти.',
'success')
                return redirect(url_for('login'))

    return render_template('register.html')

# Запуск додатка
if __name__ == '__main__':
    app.run(debug=True)
```

add_admin.py

```
from sys import argv
import sqlite3 as sql

db = sql.connect("users.db")
conn = db.cursor()

conn.execute("""CREATE TABLE IF NOT EXISTS users (
    id INTEGER PRIMARY KEY AUTOINCREMENT,
    login TEXT NOT NULL,
    password TEXT NOT NULL,
    admin BOOLEAN NOT NULL
)""")

if len(argv) == 2:
    conn.execute("UPDATE users SET admin = 1 WHERE login=?", (argv[1],))
    db.commit()
else:
    print("Usage: python add_admin.py username")

db.close()
input()
```

ІЛЮСТРАТИВНА ЧАСТИНА
ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ОЦІНЮВАННЯ РІВНЯ КІБЕРГІГІЄНИ ОСОБИ

СХЕМА ПРОЦЕСІВ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ

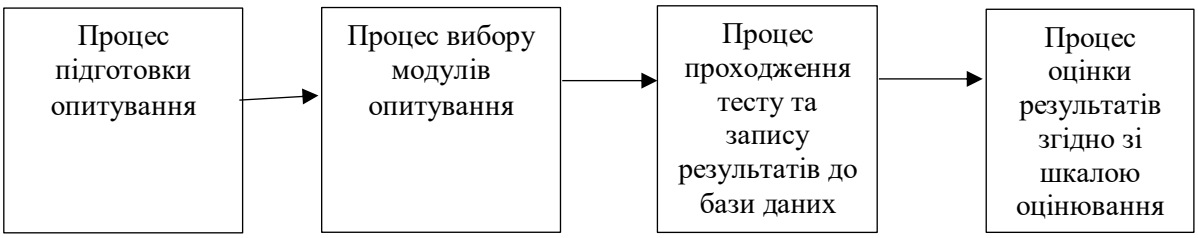

СХЕМА АРХІТЕКТУРИ СИСТЕМИ

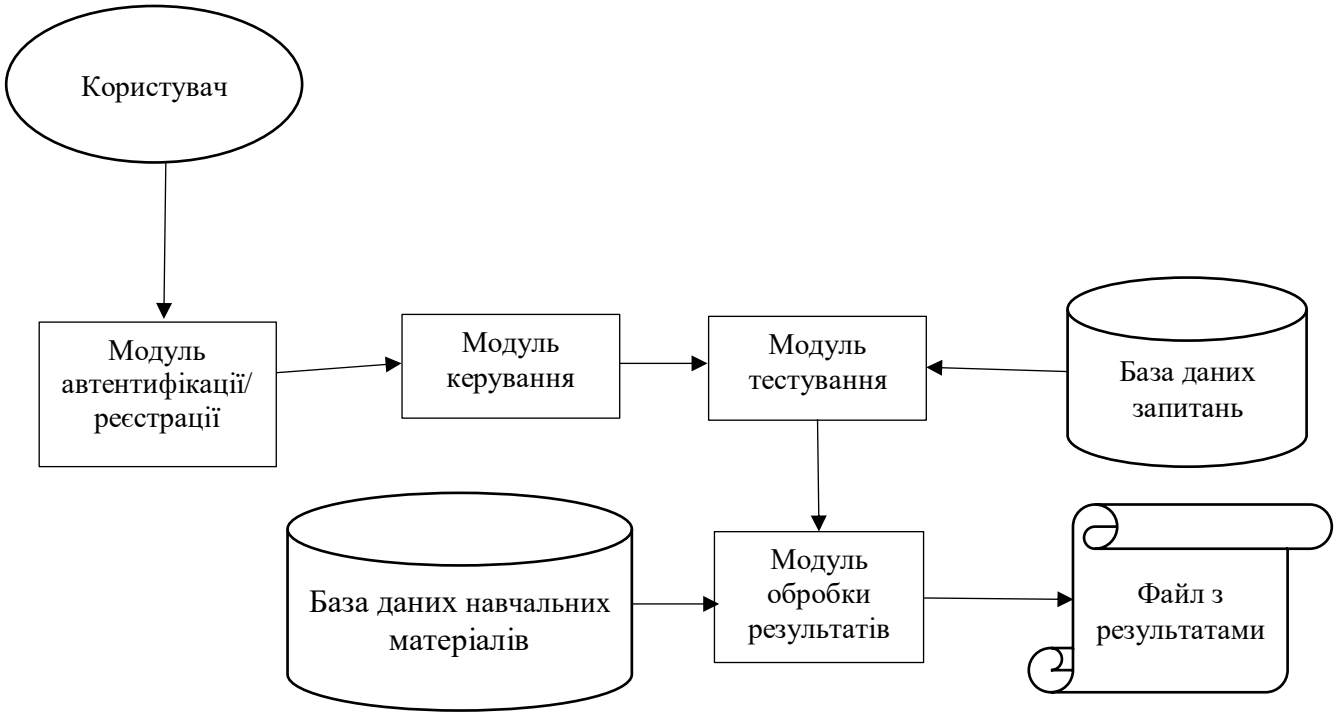

СХЕМА РОБОТИ МОДУЛЯ АВТЕНТИФІКАЦІЇ/АВТОРИЗАЦІЇ

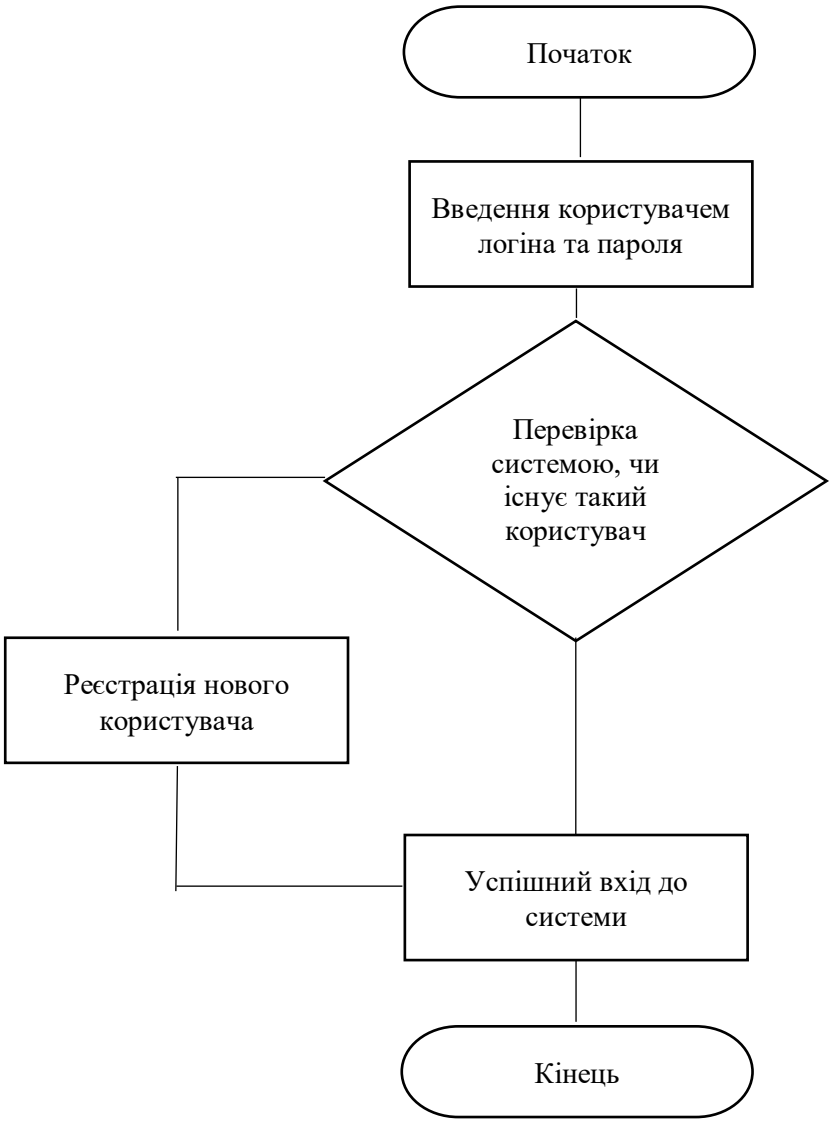

СХЕМА РОБОТИ МОДУЛЯ КЕРУВАННЯ

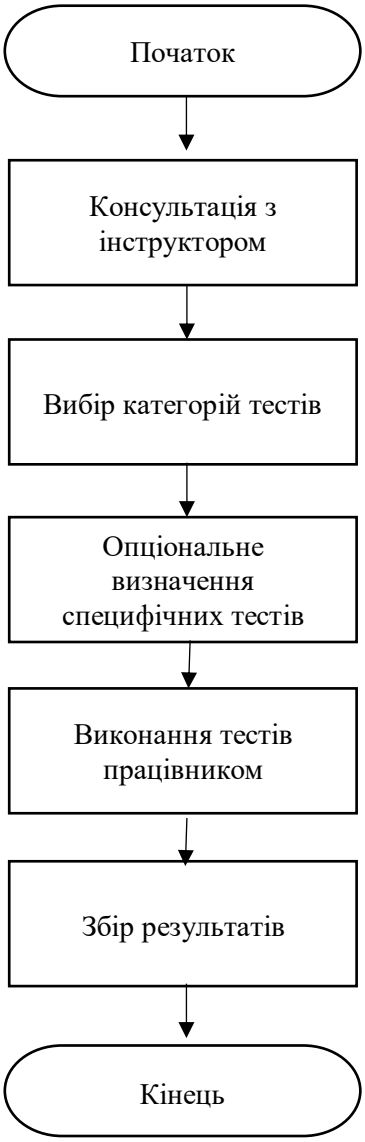

СХЕМА РОБОТИ МОДУЛЯ ОЦІНКИ РЕЗУЛЬТАТІВ

ШКАЛА ОЦІНЮВАННЯ РІВНЯ КІБЕРГІГІЄНИ ОСОБИ

Рівень знань	Відсоток правильних відповідей	Оцінка	Рекомендації
Низький	До 60%	D	Особа має низький рівень кібергігієни та не допущена до роботи.
Середній	60-74%	C	Особа має середній рівень кібергігієни та недопущена до роботи, рекомендується проходження курсу з інструктором та повторне проходження тесту.
Достатній	75-89%	B	Особа має достатній рівень кібергігієни та допущена на посаду після проходження тренінгу з інструктором.
Високий	90-100%	A	Особа має високий рівень кібегігієни та допущена на посаду.

ПОРІВНЯЛЬНА ТАБЛИЦЯ ЗАСОБІВ ОЦІНКИ РІВНЯ КІБЕРГІГІЄНИ

№	Назва	Тематика	Вартість	Країна розробки	Наявність сертифіката з результатами
1.	Дія.Освіта	Основи кібергігієни для держслужбовців	Безкоштовно	Україна	Так
2.	Дія.Освіта	Персональна кібергігієна, безпека в мережі Інтернет	Безкоштовно	Україна	Так
3.	Дія.Освіта	Кібергігієна для дітей	Безкоштовно	Україна	Ні
4.	Дія.Освіта	Кібергігієна під час війни	Безкоштовно	Україна	Ні
5.	Здолати шахрая	58 кейсів шахрайства в мережі Інтернет	Безкоштовно	Україна	Ні
6.	Cyberacademy	Кібергігієна для підприємств	Платний інтенсив	Україна	Так
7.	Як?	Практичні поради з цифрової безпеки	Безкоштовно	Україна	Ні
8.	Цифрограм. Твоя кібергігієна	Телеграм бот з тестами на різні напрямки кібергігієни	Безкоштовно	Україна	Ні
9.	Google Jigsaw	Тест на розпізнавання фішингових листів	Безкоштовно	Україна	На
10.	Cybereducation	Базові правила безпеки в цифровому середовищі	Безкоштовно	Великобританія	Ні
11.	Єшко	Цифрова безпека	3713 грн.	Україна	Так

ВІДПОВІДНІСТЬ ПОСАДИ ДО НАПРЯМКІВ КІБЕРГІГІЄНИ

Напрямок / Посада	Паролі	Персональний комп'ютер	Мобільні пристрої	Електронна пошти	Соцмережі та месенджерів	Електронні платежі	Технологія WI-FI	Споживання інформації	Соціальна інженерія
Бухгалтер	+	+	-	+	-	+	+	+	+
Менеджер	+	+	+	+	+	-	+	+	+
Рекрутер	+	+	+	+	+	-	+	+	+
Секретар	+	+	+	+	-	-	+	+	+
Юрист	+	+	-	+	-	-	+	+	+