МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітня програма: «Обслуговування комп'ютерних систем і мереж»

Група: 4КС-56

Дипломний проект

здобувача освіти денної форми навчання
КС.56.17.000.ДП

Осадчого Володимира Ігоровича

м. Одеса
2023 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**

Освітня програма: «**Обслуговування комп'ютерних систем і мереж»**

Група: **4КС-56**

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи) на тему:

Розробка backend-частини Web-сайту з дослідження напряму безпеки України

Проектний матеріал складається з пояснювальної записки на 69 сторінках та графічного (презентаційного) матеріалу на 12 аркушах (слайдах).

Дипломник _____ (Осадчий В.І)

Керівник _____ (Стайкуца С.В.)

Консультанти:

з економічної частини _____ (Копайгородська Т.Г.)

з охорони праці _____ (Чорновол Н.І.)

з дотримання вимог ЄСКД _____ (Петрашова В.І.)

старший консультант _____ (Кривченко Ю.В.)

До захисту допущений

Голова циклової комісії _____ (Кривченко Ю.В.)

Завідувач відділення _____ (Скорнякова О.В.)

Захист «22» червня 2023 р. Протокол ДКК № 4

Оцінка ДКК відмінно

Секретар ДКК _____

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення **комп'ютерних систем** Комісія **КТ та ПІ**

Спеціальність **123 «Комп'ютерна інженерія»**

Освітня програма **«Обслуговування комп'ютерних систем і мереж»**

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР Беркань І.В.

"_____" _____ 2023 р.

ЗАВДАННЯ

на дипломний проект (роботу)

Здобувачеві (здобувачці) освіти Осадчого Володимира Ігоровича

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи)) Розробка backend-частини веб-сайту з дослідження напрямку безпеки України.

затверджена наказом по коледжу від "17" **жовтня** 2022 р. № **235-А2-ОД**

2. Термін здачі закінченого проекту (роботи) 12.06.2023р

3. Вихідні данні до проекту (роботи):

Об'єктами аналізу є складові комплексної системи безпеки

Мови розробки бек-енд частини веб-сайту: C#

Кількість цільових груп в напрямку безпеки 5.

Програмні засоби розробки бек-енд частини веб-сайту: Visual Studio

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити)

Провести аналіз стану ринку безпеки України.

Провести аналіз поняття комплексної системи безпеки та її складових.

Провести аналіз рішень щодо прототипування web-сайту та аналіз прототипу

Розібрати питання щодо рішень створення frontend-частини web-сайту.

5. Перелік графічного (презентаційного) матеріалу (з точним зазначенням обов'язкових креслень, кількості слайдів)

Комплексна система забезпечення безпеки підприємства(КСЗБП). Аналіз складових КСЗБП. Аналіз стану ринку безпеки сучасної України. Тезово перерахуємо фундаментальні загрози (економічні) малому бізнесу станом на червень 2022 року. Аналіз рішень щодо прототипування сайту.Сайт який ми використовуємо називається Figma. Цільова аудиторія нашого сайту. Основні частини прототипу сайту.Основні частини прототипу Web-сайту. Аналіз засобів для створення backend-частини Web-сайту.Аналіз мови програмування C#. Розробка backend-частини веб-сайту з дослідження напрямку безпеки України.

6. Консультанти по проекту (роботі), із зазначенням розділів проекту, що їх стосується

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Вступ, 1	Стайкуца С.В.		
2	Копайгородська Т.Г.		
3	Чорновол Н.І.		
Нормоконтроль	Петрашова В.І.		

7. Дата видачі завдання 01 травня 2023 р.

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/р	Назва етапів дипломного проекту (роботи)	Термін виконання етапів дипломного проекту (роботи)	Відмітка про виконання
1.	Вступ. Постановка мети та задач проектування	22.05.2023	вик.
2.	Формування кінцевого завдання на розробку. Вступна частина дипломного проекту.	24.05.2023	вик.
3.	Огляд літератури. Огляд існуючих рішень.	25.05.2023	вик.
4.	Технологічний розділ. Прототипування web-сайту з використанням Figma	28.05.2023	вик.
5.	Технологічний розділ. Розробка серверної частини web-сайту з використанням C#	03.06.2023	вик.
6.	Технологічний розділ. Дослідження рішень для покращення серверної частини за допомогою C#	08.06.2023	вик.
7.	Економічний розділ.	05.06.2023	вик.
8.	Виконання розділу «Охорона праці».	08.06.2023	вик.
9.	Підготовка доповіді та презентації для захисту	09-11.06.2023	вик.
10.	Підготовка до попереднього захисту, підготовка до захисту	12-15.06.2023	вик.
11.	Отримання рецензії, відповіді на зауваження рецензента	16-17.06.2023	вик.
12.	Захист роботи	19-30.06.2023	вик.

Дипломник _____
(підпис)

Керівник _____
(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			КС 56. 17 000. 00 ДП	Дипломний проект		
А4			КС 56. 17 000. 00 ДП ПЗ	Пояснювальна записка	1	

Зм.	Арк.	№ докум.	Підпис	Дата	КС 56. 17 000. 00 ДП		
Розробив		Осадчий В.І.			Розробка backend-частини веб-сайту з дослідження напрямку безпеки України.	Літ.	Аркуш 3 / Аркушів 74
Перевірив		Стайкуца С.В.				Н Д П	
Н. Контр.		Петрашова В.І.				ВСП "ОТФК ОНТУ" гр.4КС-56	
Затверд.		Кривченко Ю.В.					

ЗМІСТ

ВСТУП

Web-сайт з дослідження напрямку безпеки України є абсолютно актуальним бо в нього немає аналогів. Такий web-сайт є необхідним для сьогоденного суспільства, бо користуючись саме ним користувачі зможуть із найбільшою швидкість отримати відповіді на інтересуючи їх питання з приводу безпеки на території України. Користувачі зможуть швидко отримати стислу інформацію про самі поняття безпеки. А також найбільш важливо те, що вони отримають велику і зручну базу із даними щодо компаній що працюють в Україні по різним напрямкам безпеки і у різних містах.

Прикладне значення роботи полягає у забезпеченні суспільства необхідними інструментами щодо напрямку безпеки в Україні. Робота збільшить ступінь інформованості суспільства у цьому напрямку, а також посприяє збагачуванню ринку безпеки України завдяки залученню нових користувачів у цю галузь

Мета роботи полягає у створені зручного інструменту для навігації по інформаційному просторі безпеки в Україні.

Завдання роботи полягає у створенні web-сайту що зможе надати користувачам можливості для зручної навігації по ринку безпеки України.

У коло питань роботи входять такі пункти: аналіз стану ринку безпеки України, аналіз поняття комплексної системи безпеки та її складових, аналіз рішень щодо прототипування web-сайту та аналіз прототипу, аналіз рішень щодо створення web-сайту.

1.1 Аналіз сучасного стану ринку безпеки України

1.1.1 Базові відомості щодо напрямків безпеки підприємства

Нормальне, планове функціонування підприємства, підприємства, банку, магазину та інших організацій (далі – фірм, об'єктів) – одне з головних турбот їх керівників. Стійка робота будь-якої фірми неможлива без забезпечення належного рівня її безпеки – здатності функціонувати без шкоди та при цьому постійно протистояти всіляким загрозам.

У сучасних умовах проблема забезпечення безпеки будь-якого об'єкта виходить у розряд пріоритетних, що обумовлено низкою причин:

- зростання злочинності у країні;
- активізація терористичної та диверсійної діяльності націоналістичних та підривних організацій;
- збільшення кількості нещасних випадків, стихійних лих та техногенних аварій;
- нагальна необхідність реструктуризації бізнесу на базі новітніх інформаційних технологій, що сприяють появі обладнання інформаційно-обчислювального та телекомунікаційного призначення, що потребує особливого захисту;
- необхідність підвищення конкурентоспроможності фірми.

В останні десятиліття багато керівників все більше усвідомлюють необхідність забезпечення безпеки забезпечення безпеки, про що свідчить збільшення витрат на ці цілі. Водночас зростання «невиробничих» витрат, до яких найчастіше відносять витрати на безпеку, є навіть приводом для тих керівників, які будують свою безпекову політику в основному на традиційному використанні «живої сили». Тому в даний час як ніколи актуальним є питання про підвищення рівня захисту та оптимізації системи безпеки фірми.

Поняття безпеки включає безліч різних аспектів. Зупинимося докладніше на таких як технічна укріпленість об'єкта, інформаційна безпека

Під технічною системою охорони (ТСО) у разі розуміється система раннього виявлення загроз фірмі від стихійних лих, несанкціонованого проникнення порушників і помилкових чи неправомірних дій обслуговуючого персоналу чи клієнтів фірми. При цьому виявлення, а найчастіше нейтралізація і навіть ліквідація загроз здійснюється за допомогою різних технічних засобів (ТЗ) і методів. Для того, щоб не було боляче за безцільно витрачені гроші, необхідно вибирати правильні, оптимальні напрями побудови такої системи. При цьому вибір повинен ґрунтуватися на концептуальному підході до аналізу особливостей об'єкта та можливостей сучасних технологій, на ретельному маркетинговому опрацюванні.

Інформаційна безпека (InfoSec) дозволяє організаціям та підприємствам захищати цифрову та аналогову інформацію. InfoSec забезпечує покриття криптографії, мобільних обчислень, соціальних мереж, а також інфраструктури та мереж, що містять приватну, фінансову та корпоративну інформацію. Кібербезпека з іншого боку захищає як необроблені, так і значущі дані, але тільки від інтернет-загроз.

Організації приділяють значну увагу питанням інформаційної безпеки з багатьох причин. Основним призначенням InfoSec є забезпечення конфіденційності, цілісності та доступності інформації про підприємство. Оскільки InfoSec охоплює багато областей, вона часто включає в себе реалізацію різних типів безпеки, включаючи безпеку додатків, безпеку інфраструктури, криптографію, реагування на інциденти, управління вразливістю та аварійне відновлення.

InfoSec або інформаційна безпека – це набір інструментів та методів, що використовуються для захисту своєї цифрової та аналогової інформації. InfoSec охоплює цілу низку IT-областей, включаючи інфраструктуру та мережеву безпеку, аудит та тестування. Він використовує такі інструменти, як автентифікація та дозволи, щоб обмежити несанкціонований доступ користувачів до приватної інформації. Ці заходи допоможуть вам запобігти шкоді, пов'язані з крадіжкою, зміною або втратою інформації.

Кібербезпека та інформаційна безпека охоплюють різні цілі та області, але й мають деякі спільні риси. Інформаційна безпека – це ширша категорія захисту, що охоплює криптографію, мобільні обчислення та соціальні мережі. Вона пов'язана із забезпеченням інформаційної безпеки, яка використовується для захисту інформації від загроз, не пов'язаних з людиною, таких як збої серверів або стихійні лиха. У свою чергу, кібербезпека охоплює лише інтернет-загрози та цифрові дані. Крім того, кібербезпека забезпечує захист необроблених, несекретних даних, тоді як інформаційна безпека – ні.

Існує три основні цілі, що захищаються інформаційною безпекою, у сукупності відомої як CIA:

Конфіденційність – запобігає несанкціонованому доступу користувачів до інформації для захисту конфіденційності інформаційного контенту. Конфіденційність забезпечується за рахунок обмежень доступу. Порушення конфіденційності може статися через людську помилку, навмисний обмін інформацією або зловмисне проникнення.

Цілісність – забезпечує достовірність та точність інформації. Цілісність підтримується шляхом обмеження прав на редагування чи можливості змінювати інформацію. Втрата цілісності може статися, коли аналогова інформація не захищена від зовнішніх умов, цифрова інформація не надсилається належним чином або коли користувачі вносять незатверджені зміни.

Доступність – гарантує, що авторизовані користувачі можуть отримати доступ до інформації. Доступність підтримується через безперервність процедур доступу, резервного копіювання або дублювання інформації, а також обслуговування апаратних засобів та мережевих з'єднань. Втрата доступності може статися, коли мережі зазнають атак через стихійні лиха або коли клієнтські пристрої виходять з ладу.

Для створення оптимальної ефективної системи безпеки об'єкта необхідно насамперед розробити обґрунтовану концепцію, яка визначає цілі захисту, характер можливих загроз та ймовірність їх появи, основні напрямки вирішення завдань захисту тих чи інших цінностей від аварій, стихійних лих та неправомірних дій потенційних порушників.

Предмет захисту – конкретні цінності фірми, які підлягають захисту за допомогою тієї чи іншої системи.

До таких цінностей відносяться:

– люди - персонал об'єкта, відвідувачі та клієнти фірми;

– матеріальні та фінансові цінності (гроші, цінні папери, документи, обладнання);

– інформація конфіденційного характеру.

Пріоритети зазначених цінностей великою мірою обумовлені характером діяльності фірми.

Об'єкт захисту - фізичний простір, де зосереджені ті чи інші цінності, багато в чому визначає можливі дії порушника безпеки та заходи щодо запобігання загрозам безпеки фірми.

Звернемося до визначення комплексна безпека

Сама назва «Комплексна система забезпечення безпеки підприємства» здається, на перший погляд, досить хитромудрою і наукоподібною… Але давайте розберемося в кожному основному терміні, з якого складається ця назва. Це необхідно для того, щоб автор і читач «розмовляли однією мовою».

Рисунок 1.1 - КСЗБП

Створити та змусити функціонувати на підприємстві систему взаємопов'язаних між собою структурних елементів, яка б адекватно реагувала на ризики, небезпеки та загрози, що виникають, а також дозволяла власнику бізнесу оцінити витрати для їх нейтралізації.

Створення комплексної системи забезпечення безпеки підприємства включає в себе такі елементи

1. Відповідальний керівник КСЗБП

2. Рада з безпеки;

3. Спеціалізований структурний підрозділ, який займається питаннями безпеки.

4. Персонал.

5. Технічні засоби.

6. Регламенти.

7. Ресурси.

8. Інформація.

9. Сторонні (залучені) сили.

Під час створення на підприємстві комплексної системи забезпечення безпеки виникне неминуче питання: які принципи функціонування мають бути започатковані в цю систему?

Таблиця 1.1 – Принципи функціонування КСЗБП

Назва принципу	Опис
Законність	Діяльність системи безпеки має ґрунтуватися на існуючих у країні законах. Тільки це дозволить підприємству відчувати надійність свого існування та компенсувати зазнані збитки з найменшим ризиком.
Розумна достатність	Ступінь загрози має викликати адекватний рівень реакції. Тобто якщо людині на голову села метелик, можна її просто зігнати, а не бити по голові молотком.
Швидкість реагування	Ключовим словом під час запровадження цього принципу має бути слово «негайно».
Комплексність	Система безпеки має задіяти всі наявні для підприємства різноманітні ресурси для забезпечення реагування на загрози.
Ефективність	Система безпеки повинна не бути даниною моді, а повинна реально мінімізувати втрати і, за умови правильної постановки справи, приносити дохід.

Створити та змусити функціонувати на підприємстві систему взаємопов'язаних між собою структурних елементів, яка б адекватно реагувала на ризики, небезпеки та загрози, що виникають, а також дозволяла власнику бізнесу оцінити витрати для їх нейтралізації.

Створення комплексної системи забезпечення безпеки підприємства включає в себе такі елементи

1. Відповідальний керівник КСЗБП

2. Рада з безпеки;

3. Спеціалізований структурний підрозділ, який займається питаннями безпеки.

4. Персонал.

5. Технічні засоби.

6. Регламенти.

7. Ресурси.

8. Інформація.

9. Сторонні (залучені) сили.

1.1.2 Аналіз складових в комплексній безпеці

Комплекс системи безпеки базується на цілій низці компонентів, які в тій чи іншій мірі можуть використовуватися або всі разом або окремо. Розглянемо 9 основних груп, які надалі будуть реалізовані програмно в нашій роботі:

Технічні засоби безпеки – це сукупність пристроїв, систем та програмного забезпечення, розроблених для забезпечення безпеки та захисту різних об'єктів та інформації. Вони призначені для виявлення, запобігання та

реагування на загрози, а також для забезпечення захисту від небажаного доступу, пошкодження, крадіжки або втрати даних.

Технічні засоби безпеки можуть включати різні компоненти, такі як відеоспостереження, системи контролю доступу, системи оповіщення і пожежної сигналізації, датчики руху і т.д. Вони можуть бути встановлені як усередині приміщень, і на відкритих просторах.

Використання технічних засобів безпеки допомагає запобігати злочинам, забезпечувати безпеку персоналу та майна, виявляти інциденти та реагувати на них швидко та ефективно. Це важливий аспект у сфері безпеки, який допомагає захистити цінності та забезпечити безпечне середовище для роботи та життя людей.

Служби безпеки, або охоронні агентства, є організаціями або компаніями, що спеціалізуються на наданні послуг із забезпечення безпеки. Вони наймаються охорони різних об'єктів, включаючи комерційні, державні чи приватні установи, житлові комплекси, торгові центри, події тощо.

Охоронні агенції пропонують широкий спектр послуг, спрямованих на забезпечення фізичної безпеки та захист людей, майна та інформації.

Охоронні агенції виконують такі послуги:

Таблиця 1.2 – Послуги охоронних агенцій

Назва послуги	Визначення
Фізична охорона	Наймані охоронці та охоронні служби забезпечують фізичну присутність для захисту об'єктів, контролю доступу, запобігання крадіжкам та незаконним діям.
Відеоспостереження	Служби безпеки можуть

	встановлювати системи відеоспостереження для безперервного контролю та запису того, що відбувається на об'єкті.
Контроль доступу	Реалізація системи контролю доступу, таких як електронні пропускні системи, біометричні зчитувачі або кодові замки, щоб обмежити доступ до певних зон або приміщень.
Патрулювання	Охоронці можуть виконувати патрулювання об'єктів з метою виявлення потенційних загроз або неправильної поведінки.
Реагування на інциденти	Охоронні агенції готові швидко реагувати на події, включаючи напади, пожежі, крадіжки та інші надзвичайні ситуації.
Консультації з безпеки	Деякі охоронні агенції пропонують послуги консультацій та аналізу уразливостей об'єктів для розробки комплексних систем безпеки.Цель служб безопасности – обеспечить защиту людей, имущества и

Пожежна безпека – це комплекс заходів та процедур, спрямованих на запобігання виникненню пожеж, мінімізацію їх наслідків та захист людей, майна та навколишнього середовища від вогню.

Пожежна безпека включає широкий спектр послуг:

Таблиця 1.3 – Послуги пожежної безпеки

Назва послуги	Визначення
Профілактика	Це включає розробку та впровадження пожежних норм та правил, навчання персоналу заходам запобігання пожежам, регулярні перевірки та обслуговування пожежної техніки та систем, а також створення пожежно-технічного режиму на об'єктах.
Пожежний захист	Це означає наявність та правильне функціонування систем пожежної сигналізації, пожежогасіння, автоматичного пожежогасіння, систем оповіщення та евакуації, а також систем пожежної вентиляції.
Планування евакуації	Розробка планів евакуації та проведення тренувань для персоналу та відвідувачів, щоб забезпечити швидку та безпечну евакуацію під час пожежі.
Навчання та навчальні програми	Проведення навчання персоналу в галузі пожежної безпеки, щоб вони знали, як запобігати пожежам, як використовувати засоби пожежогасіння та як правильно діяти

	у разі виникнення пожежі.
Пожежна техніка та засоби	Забезпечення наявності необхідної пожежної техніки, такої як вогнегасники, гідранти, пожежні крани, пожежні рукави та інші засоби для гасіння пожеж.
Пожежна безпека у будівництві	Дотримання відповідних будівельних та проектних норм та вимог, включаючи правильне розміщення систем пожежогасіння, використання вогнестійких матеріалів, встановлення автоматичних систем пожежогасіння тощо.

Мета пожежної безпеки – запобігання пожежам, захист життя та здоров'я людей, збереження майна та навколишнього середовища. Це важливий аспект безпеки, який потребує постійної уваги, навчання та дотримання відповідних заходів та нормативів.

Детективні агенції – це приватні організації, що спеціалізуються на наданні професійних детективних послуг. Вони надають широкий спектр послуг у галузі розвідки, розслідування та виявлення інформації для різних клієнтів, включаючи приватних осіб, компанії та організації.

Детективні агенції можуть надавати такі послуги:

Таблиця 1.4 – Послуги детективних агенцій

Назва послуги	Визначення
Розслідування ділової безпеки	Вони допомагають компаніям та підприємцям захистити свої бізнес-

	інтереси, виявити злочини, внутрішні шахрайства, корупцію чи порушення комерційної конфіденційності.
Пошук зниклих осіб	Детективи можуть шукати зниклих людей, включаючи зниклих родичів, боргових боржників чи свідків.
Розкриття сімейних та особистих справ	Детективні агентства можуть допомогти у розслідуванні справ, пов'язаних із розлученнями, аліментами, визначенням несумлінних дій подружжя та іншими сімейними питаннями.
Розслідування злочинів	Детективи можуть допомогти правоохоронним органам у розслідуванні злочинів, надаючи додаткові ресурси, фахівців та методи виявлення доказів, збору інформації та пошуку свідків.
Консультації та аналіз безпеки	Детективні агенції можуть надавати послуги консультацій та аналізу безпеки для компаній та приватних осіб, щоб виявити вразливості та рекомендувати заходи щодо покращення безпеки.

Мета детективних агентств – надати клієнтам інформацію та докази, допомогти їм вирішити питання безпеки та захистити їх інтереси. Вони працюють у рамках закону та використовують різні методи, такі як

спостереження, збір інформації, інтерв'ю, аналіз даних тощо. Важливо відзначити, що детективні агенції не мають права здійснювати арешти або вживати заходів, прерогатива яких належить правоохоронним органам.

Кадрова безпека – це область безпеки, пов'язана із захистом організації від загроз, пов'язаних з діяльністю співробітників, контроль доступу до інформації та запобігання витоку конфіденційних даних або зловживань з боку персоналу.

Під кадровою безпекою мається на увазі таке:

Таблиця 1.5 – Послуги кадрової безпеки

Назва послуги	Визначення
Контроль доступу	Регулювання та обмеження доступу співробітників до конфіденційної інформації, приміщень або систем, які можуть загрожувати організації. Це може включати використання різних методів автентифікації, наприклад пропускних систем, біометричних технологій або паролів.
Верифікація персоналу	Перевірка минулого досвіду, референцій та професійної репутації потенційних співробітників перед їх наймом для мінімізації ризиків, пов'язаних із наданням доступу до чутливої інформації або активів організації.
Навчання та обізнаність	Навчання персоналу в галузі

	кадрової безпеки, щоб вони розуміли свої обов'язки, правила та процедури з обробки та захисту конфіденційної інформації, а також обізнаність про потенційні загрози та методи атак.
Моніторинг та аудит	Регулярне контролю та аудит дій персоналу, щоб виявити незаконні чи підозрілі активності, порушення політик безпеки або несанкціонований доступ до інформації.
Управління доглядом співробітників	Розробка та реалізація процедур, пов'язаних із звільненням чи відходом співробітників, щоб забезпечити повернення всіх наданих доступів, захист конфіденційної інформації та запобігання завданню шкоди організації.

Мета кадрової безпеки – запобігання загрозам, пов'язаним з персоналом, та мінімізація ризиків, пов'язаних з доступом до конфіденційної інформації, активів та бізнес-процесів організації. Це важливий аспект загальної безпеки, який допомагає запобігти витоку даних, шахрайства, внутрішніх загроз і зберегти репутацію і довіру до організації.

Інформаційна безпека – це область безпеки, пов'язана із захистом інформації та інформаційних систем від загроз, включаючи несанкціонований доступ, використання, розкриття, зміну або знищення інформації.

Під інформаційною безпекою мається на увазі наступне:

Таблиця 1.6 – Послуги інформаційної безпеки

Назва послуги	Визначення
Конфіденційність	Забезпечення захисту конфіденційності інформації, тобто гарантування, що інформація доступна лише тим особам, які мають право на її отримання. Це включає обмеження доступу до конфіденційної інформації, шифрування даних та контроль доступу.
Цілісність	Гарантування цілісності інформації, тобто забезпечення її незмінності та непідробності. Це включає захист від несанкціонованої модифікації, пошкодження або втрати даних, а також перевірку цілісності інформації у процесі передачі чи зберігання.
Доступність	Забезпечення доступності інформації та інформаційних систем для авторизованих користувачів у потрібний час. Це включає захист від збоїв у системах, шкідливого програмного забезпечення або дій зловмисників, які можуть спричинити недоступність інформації.

Аутентифікація	Перевірка автентичності користувачів, щоб переконатися в їхній ідентичності перед наданням доступу до інформаційних ресурсів. Це включає використання паролів, біометричних даних, двофакторної автентифікації та інших методів ідентифікації.
Керування вразливістю	Ідентифікація, оцінка та управління вразливістю інформаційних систем, щоб запобігти можливості несанкціонованого доступу або використання вразливостей зловмисниками.
Навчання та обізнаність	Навчання співробітників у галузі інформаційної безпеки, щоб вони розуміли загрози, правила використання інформаційних систем, процедури резервного копіювання даних та інші заходи безпеки.

Мета інформаційної безпеки – забезпечити захист інформації, інформаційних систем та пов'язаних з ними ресурсів від загроз та ризиків, пов'язаних із несанкціонованим доступом, використанням або розкриттям інформації. Це важливий аспект для запобігання витоку даних, кібератак, шахрайства та збереження довіри до інформаційних ресурсів організації.

Промислова безпека – це область безпеки, пов'язана із запобіганням аваріям, травмуванню працівників, пошкодженню обладнання та заподіянню

шкоди навколишньому середовищу в промислових об'єктах, таких як заводи, фабрики, склади та інші виробничі підприємства.

Під промисловою безпекою мається на увазі таке:

Таблиця 1.7 – Послуги промислової безпеки

Назва послуги	Визначення
Безпека працівників	Забезпечення безпечних умов праці та захисту працівників від небезпек, пов'язаних із виконанням робіт на виробничому об'єкті. Це включає дотримання норм і правил з охорони праці, навчання персоналу в галузі безпеки, використання відповідного захисного екіпірування та проведення регулярних перевірок щодо дотримання безпеки.
Захист обладнання та матеріалів	Запобігання пошкодженню та поломці обладнання, машин, інструментів та матеріалів, що використовуються на промисловому об'єкті. Це включає регулярне технічне обслуговування, перевірку працездатності обладнання, застосування правильних методів зберігання та поводження з матеріалами.
Запобігання аваріям	Розробка та реалізація заходів для запобігання аварійним ситуаціям, таким як пожежі, вибухи, витікання

	небезпечних речовин та інших нещасних випадків. Це включає встановлення систем попередження та гасіння пожеж, систем виявлення витоків, дотримання правил безпеки під час роботи з небезпечними речовинами та технологіями.
Управління ризиками	Оцінка та управління ризиками, пов'язаними з промисловою діяльністю. Це включає ідентифікацію потенційних небезпек, аналіз ризиків, розробку та впровадження заходів щодо їх зниження чи усунення, а також створення системи моніторингу та контролю ризиків.
Відповідність нормативним вимогам	Дотримання законодавчих та нормативних вимог щодо промислової безпеки. Це включає дотримання правил, норм, стандартів та сертифікаційних вимог, встановлених відповідними органами та організаціями.

Мета промислової безпеки – запобігання аваріям, травмуванню працівників, пошкодженню обладнання та мінімізації негативних впливів на навколишнє середовище в процесі промислової діяльності. Це важливий аспект забезпечення безпеки працівників та збереження стабільності та ефективності промислових процесів.

Техніка безпеки та охорона праці (ТВ та ОП) – це область, пов'язана із забезпеченням безпечних та здорових умов праці для працівників на робочих місцях. Вона включає застосування технічних і організаційних заходів для запобігання виробничим травмам, захворюванням, аварійним ситуаціям і створенню безпечного і здорового робочого середовища.

Під технікою безпеки та охороною праці мається на увазі наступне:

Таблиця 1.8 – Послуги техніки безпеки та охорони праці

Назва послуги	Визначення
Аналіз та оцінка ризиків	Ідентифікація потенційних небезпек та ризиків на робочих місцях, проведення аналізу ризиків та оцінка їх впливу на здоров'я та безпеку працівників. Це дозволяє визначити необхідні заходи щодо запобігання та управління ризиками.
Планування та впровадження заходів безпеки	Розробка та реалізація заходів та програм безпеки, які спрямовані на запобігання виробничим травмам та захворюванням. Це може включати розробку стандартів, процедур та інструкцій щодо безпечного виконання робіт, використання захисного обладнання, організації евакуації та ін.
Навчання та поінформованість	Навчання працівників правилам безпеки та охорони праці, а також поінформованість про потенційні небезпеки на робочому місці та

	методи їх запобігання. Регулярні тренінги та інформаційні кампанії допомагають підвищити обізнаність та знизити ризики.
Технічні заходи безпеки	Впровадження та використання спеціального обладнання, систем та пристроїв, що забезпечують безпеку на робочих місцях. Це може включати протипожежне обладнання, засоби індивідуального захисту, системи контролю та моніторингу, автоматичні системи безпеки та інші технічні засоби.
Контроль та аудит	Організація системи контролю та аудиту дотримання правил безпеки та охорони праці. Регулярні перевірки, інспекції та аудити допомагають виявити можливі порушення та недоліки, а також вжити заходів щодо їх усунення.

Мета техніки безпеки та охорони праці – запобігання травмуванню працівників, зниження ризиків та створення безпечного та здорового робочого середовища. Це важливий аспект забезпечення благополуччя та захисту здоров'я працівників у робочому середовищі.

Кібербезпека – це область безпеки, пов'язана із захистом комп'ютерних систем, мереж, даних та інформації від загроз, пов'язаних із цифровими технологіями та кіберзлочинністю. Вона включає в себе заходи, методи та

технології, спрямовані на запобігання несанкціонованому доступу, крадіжці, знищенню, пошкодженню або зміні цифрової інформації.

Під кібербезпекою мається на увазі наступне:

Таблиця 1.9 – Послуги кібербезпеки

Назва послуги	Визначення
Захист інформаційних систем	Забезпечення безпеки комп'ютерних систем, мереж та інфраструктури від кіберзагроз, таких як віруси, шкідливе програмне забезпечення, атаки хакерів і кібершпигунство. Це включає використання антивірусних програм, брандмауерів, систем виявлення вторгнень, керування доступом та інших технічних засобів.
Захист даних	Забезпечення конфіденційності, цілісності та доступності цифрової інформації. Це включає шифрування даних, резервне копіювання, встановлення правильних політик доступу, контроль використання інформації та заходи щодо запобігання витоку даних.
Ідентифікація та автентифікація	Перевірка автентифікації користувачів та пристроїв для забезпечення правильного доступу до систем та даних. Це включає використання паролів, двофакторної

	автентифікації, біометричних даних та інших методів ідентифікації.
Навчання та обізнаність	Навчання співробітників та користувачів у сфері кібербезпеки, щоб вони розуміли загрози та ризики, пов'язані з цифровим середовищем, і знали, як запобігати атакам та захищати свої дані. Це включає поінформованість про фішингові атаки, соціальну інженерію та інші методи кіберзлочинності.
Моніторинг та реагування на інциденти	Створення системи моніторингу, виявлення та реагування на кіберінциденти. Це включає моніторинг мережевої активності, аналіз журналів подій, реагування на підозрілу активність та відновлення після інцидентів.

Мета кібербезпеки – захист цифрових ресурсів та даних від загроз, забезпечення безпеки інформаційних систем та підтримка довіри до цифрових технологій.

1.1.3 Аналіз стану ринку безпеки сучасної України

Стан бізнес-середовища України після 24.02.2022

24 лютого 2022 року, приблизно о 5 годині ранку за київським часом, російські війська увійшли на територію України з Росії, Криму та Білорусії, також до бойових дій включилися війська Донецької Народної Республіки (ДНР) та Луганської Народної Республіки (ЛНР). Війська почали наступ за

чотирма основними напрямками — з півночі у напрямку Києва, з північного сходу у напрямку Харкова, з південного сходу з Донбасу та з півдня з Криму. Подіям передували концентрація російських військ біля російсько-українського кордону та криза у відносинах Росії та України внаслідок цього.

21 лютого 2022 року Росія визнала незалежність ДНР та ЛНР. Вранці 24 лютого відбулося звернення президента Росії Володимира Путіна щодо початку «спеціальної військової операції». Обґрунтуванням вторгнення Володимир Путін заявив про необхідність захисту ДНР і ЛНР і самої Росії, а також використав не відповідну дійсності характеристику України як неонацистської держави.

Вторгнення викликало велику міграційну кризу: за даними ООН, Україну залишило 6,7 млн біженців (станом на 26 травня), а ще близько 8 млн людей стали внутрішньо переміщеними особами (станом на 3 травня). Низка журналістів назвали вторгнення найбільшим військовим конфліктом у Європі із закінчення Другої світової війни.

Фактично, на місяць роботи бізнесу в Україні зупинилася. Причини – бойові дії, руйнування транспортної інфраструктури, перебої з паливом, масовий виїзд людей (співробітників) за межі України чи внутрішня міграція. На сьогодні, незважаючи на всі складнощі, малий бізнес намагається запускати роботу та підтримувати ключові бізнес-процеси.

Загальні прямі втрати малого та середнього бізнесу за чотири тижні війни оцінюються у 80 мільярдів доларів. А їхня оцінка скорочення ВВП України у 2022 році внаслідок зниження ділової активності – 21%. Лише 17% підприємців сподіваються хоча б зберегти обсяги продажів по відношенню до 2021 року. 34% не бачать можливості мати суттєвих обсягів діяльності цього року. Основними потребами бізнесу залишається доступ до фінансів. Також критичним є збереження ключових співробітників для функціонування бізнесу.

Кількість непрацюючих представників малого бізнесу скоротилася із 42% місяць тому до 26%.

Про це свідчать результати другої хвилі опитування Європейської Бізнес Асоціації серед представників малого та середнього бізнесу – учасників проекту Unlimit Ukraine.

Із опитаних малих бізнесів 17% уже відновили роботу після тимчасового припинення та ще 23% готуються до відновлення.

Також збільшилася кількість підприємців, які працюють у повному обсязі – з 13 до 20%.

Серед вимушених обмежень – скорочення географії діяльності, перехід до онлайн, закриття частини відділень/торгових точок. Відновити повноцінну роботу компанії не можуть здебільшого через відсутність замовлення, зниження активності клієнтів, скорочення проектів.

Дещо покращилася оцінка підприємцями власної фінансової стійкості. Наразі 40% повідомляють, що їх фінансових резервів вистачить на кілька місяців, раніше таких було 32%. Ще 15% мають резерви на місяць. У той же час 12% повідомляють, що зможуть протриматися півроку, а 6% – рік і більше.

Кількість бізнесів, які вже вичерпали свої фінансові резерви, практично не змінилася і становить 26% від загальної кількості респондентів.

Кількість бізнесів, які вже вичерпали свої фінансові резерви, практично не змінилася і становить 26% від загальної кількості респондентів.

Ситуація із виплатою заробітних плат співробітникам майже не зазнала змін за останній місяць. Заробітну плату у повному обсязі виплачують 25% компаній, причому 5% продовжують це робити з додатковими чи авансовими виплатами. Втім, 27% були змушені скоротити виплати, а 22% не мають ресурсів для виплати заробітної плати, тож 15% відправляють співробітників у неоплачувану відпустку, а 9% змушені частково чи повністю звільняти персонал.

Переважна більшість МСБ підприємців, а саме 71% нікуди не перевозили свій офіс чи виробництво, лише 11% здійснили релокейт на захід України, а 4% – за кордон. Також окремі підприємці повідомляли про релокейт у центральні регіони України.

Втрати бізнесу від війни 40% респондентів оцінюють до 10 тисяч доларів, ще близько третини, а саме 28% – у діапазоні 10-50 тисяч, 15% – більше 100 тисяч. Про відсутність втрат повідомляють близько 6% МСБ.

При цьому 20% опитаних нами бізнесів повідомляють про шкоду майну чи активи безпосередньо внаслідок бойових дій. Орієнтовна сукупна сума збитків, заподіяна підприємцям-учасникам опитування – близько 2 млн. доларів.

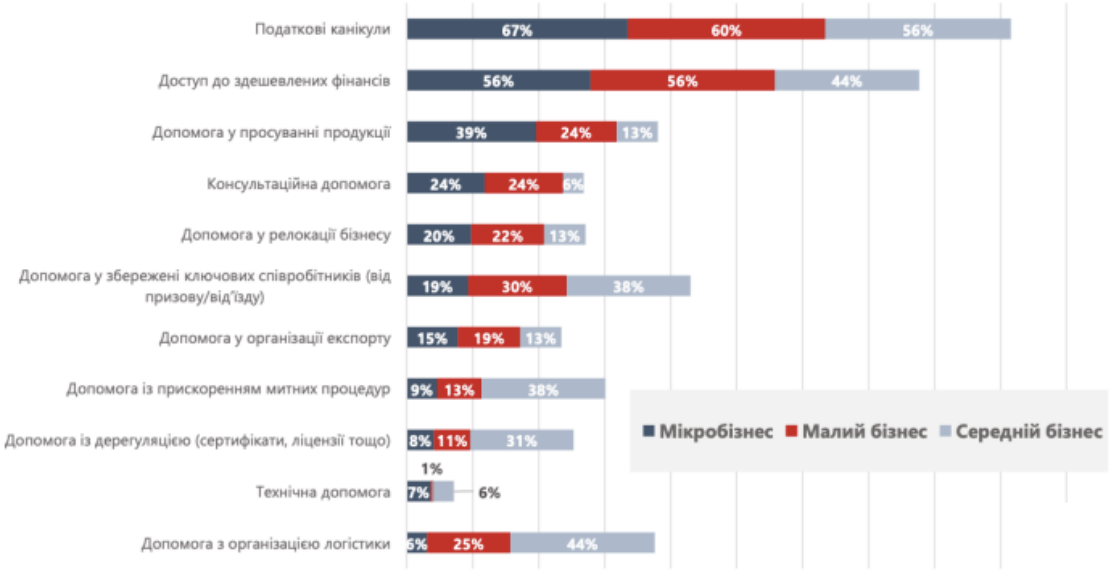


Рисунок 1.2 - Потреби бізнесу за розмірами

Тезово перерахуємо фундаментальні загрози (економічні) малому бізнесу станом на червень 2022 року. До них відносяться:

1. Війна - і всі ризики, з нею пов'язані

2. Відсутність інвестицій в Україну

3. Дорогі енергоносії

4. Проблеми з логістикою – руйнування інфраструктури як наслідок бойових дій, блокування портів

5. Проблеми з паливом

6. Відсутність ключових співробітників – виїзд за межі України, заклик до ЗСУ, поранення чи смерть внаслідок бойових дій

7. Падіння низки секторів економіки, наприклад, сільське госп-во, виробництво, металургія

Особливості та компонентний склад ринку безпеки України

Ринок безпеки в Україні є одним з найбільш важливих секторів економіки країни, що динамічно розвиваються. Він охоплює широкий спектр послуг та продуктів, пов'язаних із забезпеченням безпеки держави, бізнесу та громадян.

Ситуація під час військового конфлікту східної України у 2014 році значно вплинула на безпековий ринок. Конфлікт призвів до зростання загроз тероризму, протидії сепаратистським рухам, контрабанді зброї та наркотиків, а також зростання потреби у забезпеченні безпеки об'єктів критичної інфраструктури.

У відповідь на нові виклики уряд України активно розробляє та реалізує стратегії та програми зі зміцнення безпеки. Він також стимулює розвиток місцевої галузі безпеки, створюючи умови для залучення інвестицій та розвитку інноваційних технологій.

Розвиток ринку безпеки в Україні супроводжується зростанням кількості компаній, що пропонують послуги у цій сфері, а також розвитком та впровадженням нових технологій. Компанії активно співпрацюють із закордонними партнерами, щоб привнести передовий досвід та передові технології в український ринок безпеки.

Проте виклики, пов'язані зі збройним конфліктом та російською агресією, залишаються актуальними. Україна продовжує працювати над зміцненням своєї безпеки та співпрацею з міжнародними партнерами для забезпечення стабільності та захисту інтересів країни.

Звичайно ж, з початком повноцінного збройного конфлікту і ринок безпеки постраждав як і інші галузі. Зменшилася кількість співробітників та фінансування та ділова активність загалом знизилася.

1.2. Розробка прототипу сайту

1.2.1 Аналіз рішень щодо прототипування сайту.

Прототипування сайтів – це процес створення попереднього моделювання або пробного екземпляра майбутнього веб-сайту або веб-програми. Прототип служить для візуалізації інтерфейсу користувача (UI) і користувальницького досвіду (UX) до фактичної розробки та запуску проекту.

Головна мета прототипування сайтів полягає в тому, щоб надати команді розробників, дизайнерів та замовникам можливість ранньої візуалізації та оцінки майбутнього сайту. Ось кілька причин, чому прототипування важливе:

Візуалізація концепції: Прототип допомагає візуалізувати ідеї та концепції, дозволяючи всім учасникам проекту мати загальне уявлення про те, як виглядатиме та працюватиме сайт.

Тестування досвіду користувача: Прототип дозволяє оцінити користувальницький досвід і зручність використання сайту. Це включає оцінку навігації, розташування елементів, зрозумілість інтерфейсу та інші фактори, які можуть впливати на взаємодію користувачів із сайтом.

Отримання зворотного зв'язку та участь замовника: Прототип надає можливість отримати зворотний зв'язок від замовника та зацікавлених сторін, перш ніж розпочати фінальну розробку сайту. Це дозволяє внести зміни та покращення на ранніх стадіях проекту, що економить час та ресурси.

Скорочення помилок та підвищення ефективності: Прототипування допомагає виявити потенційні проблеми та помилки у дизайні сайту на ранніх етапах розробки. Це дозволяє знизити ризики та покращити якість кінцевого продукту.

Прототипи сайтів можуть бути створені за допомогою різних інструментів та технік, включаючи спеціалізовані програми для прототипування, графічні редактори або онлайн-платформи. Ці інструменти дозволяють створювати інтерактивні прототипи з переходами між сторінками, анімацією елементів та іншими функціями, щоб точно передати кінцевий результат розробки сайту.

Короткий опис кількох популярних рішень для створення прототипу сайту:

Таблиця 1.10 – Рішення для створення прототипу веб-сайту.

№	Назва	Опис сайту
1	AdobeXD	Це інструмент, розроблений Adobe, який пропонує функції для створення макетів, прототипів та дизайну інтерфейсу
2	Sketch	Це інструмент для створення макетів та прототипів, розроблений спеціально для користувачів macOS
3	InVision	Це платформа, призначена для створення інтерактивних прототипів та спільної роботи над проектами.
4	Axure RP	Це інструмент для створення прототипів з широкими можливостями та гнучкими функціями
5	Marvel	Це простий у використанні інструмент для створення прототипів та дизайну інтерфейсу.
6	Balsamiq	Це інструмент для створення прототипів з упором на начерки та швидке моделювання.
7	Proto.io	Це онлайн платформа для створення інтерактивних прототипів. Proto.io надає широкий вибір елементів дизайну та функцій.
8	Justinmind	Це інструмент, призначений для створення складних прототипів із широким набором функцій.
9	Framer	Це інструмент для створення прототипів з акцентом на дизайн та анімацію.
10	Figma	Це онлайн-сервіс для розробки інтерфейсів та прототипування з можливістю організації спільної роботи в режимі реального часу.

Кожен із цих інструментів має свої переваги та унікальні функції. Вибір залежить від ваших індивідуальних переваг, потреб проекту та ступеня командної роботи.

Тепер детальніше про Figma, яка була обрана для створення прототипу сайту.

Figma - це потужний веб-додаток для створення макетів, дизайну та прототипування. Воно стало популярним інструментом серед дизайнерів та розробників завдяки своїм унікальним функціям та перевагам. На малюнку 1.3 показано переваги цього сайту конструктора

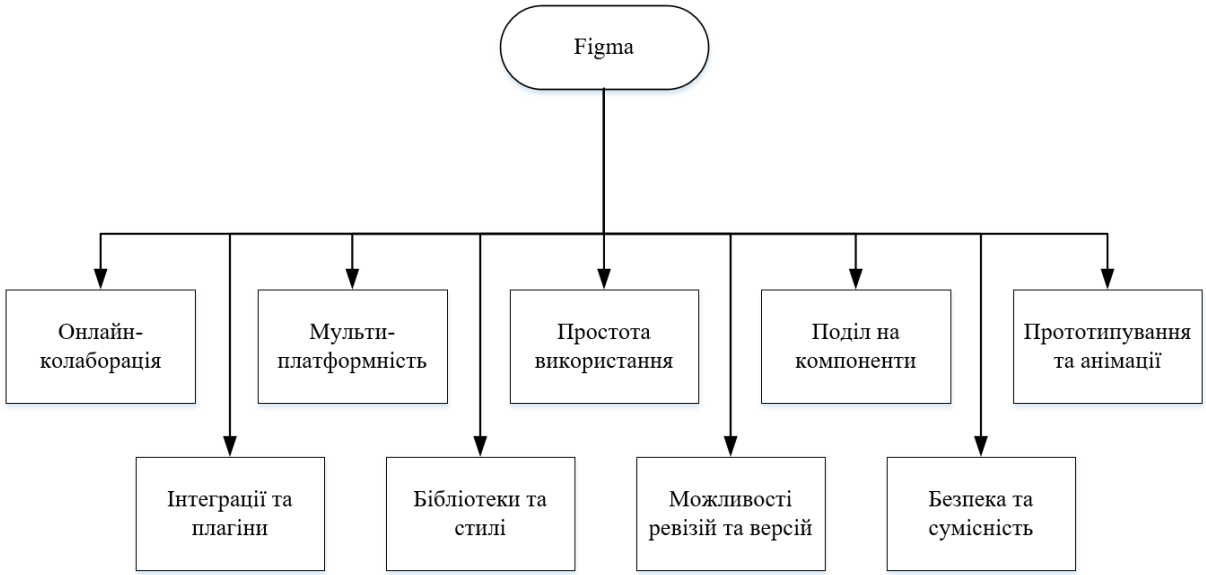


Рисунок 1.3 Переваги сайту Figma

Далі я докладніше розповім про кожну перевагу:

Таблиця 1.11 – Переваги Figma.

Тип переваги	Опис переваги
Онлайн-колаборація	Однією з ключових переваг Figma є можливість роботи в режимі реального часу з командою
Мультиплатформність	Figma доступний як веб-додаток та має версії для Windows та macOS.
Простота використання	Інтерфейс Figma інтуїтивно зрозумілий та простий у використанні
Поділ на компоненти	Figma дозволяє створювати компоненти, які можна використовувати на всіх сторінках макета.

Прототипування та анімації	Figma надає потужні інструменти для створення інтерактивних прототипів та анімацій
Інтеграції та плагіни	Figma пропонує широкий вибір інтеграцій з іншими інструментами розробки, такими як Jira, Trello, Slack та GitHub. Крім того, Figma підтримує плагіни..
Бібліотеки та стилі	Figma дозволяє створювати бібліотеки компонентів та стилів, що полегшує підтримку та оновлення дизайну.
Можливості ревізій та версій	Figma надає можливість зберігати та відстежувати зміни в макеті.
Безпека та сумісність	Figma забезпечує високий рівень безпеки даних та сумісність з іншими інструментами розробки

1.2.2 Розробка маркетингової складової сайту.

Наш сайт може допомогти компаніям знайти для них той тип безпеки, який їм потрібен. Список безпеки, який ми допоможемо знайти:

- Технічні засоби безпеки: продаж обладнання, проектування, монтаж
- Служба безпеки (охоронні агенції)
- Пожежна безпека
- Детективні агенції
- Кадрова безпека: підбір персоналу, перевірка персоналу
- Інформаційна безпека
- Промислова безпека
- Техніка безпеки та охорона праці
- Кібербезпека

Мета сайту зібрати потрібну інформацію про компанії, які можуть надати послугу безпеки в одному місці, щоб її було зручніше знайти. Також

подивитися різні відгуки про якісь компанії і подивитися рейтинг які виставляють інші користувачі.

Цільова аудиторія послуг безпеки може бути різноманітною і залежить від конкретних послуг та рішень, які пропонує компанія. Ось кілька прикладів потенційних цільових аудиторій для різноманітних видів послуг безпеки:

Таблиця 1.12 – Потенційні цільові аудиторії веб-сторінки.

Вид послуг	Опис послуги
Корпоративні клієнти	Великі та середні підприємства, які потребують комплексних рішень щодо забезпечення безпеки своїх фізичних та інформаційних ресурсів. Це може включати фірми охорони, системи відеоспостереження, контроль доступу, кібербезпеку та управління ризиками.
Малі та середні підприємства	Власники малого бізнесу, яким потрібні простіші та доступніші рішення безпеки. Це може включати системи відеоспостереження, охоронну сигналізацію, безпеку мережі та консультаційні послуги з безпеки.
Приватні особи	Люди, яким потрібна індивідуальна безпека для себе, свого житла та майна. Включає послуги із забезпечення особистої безпеки, встановлення домашньої безпеки, моніторинг та тривожні системи.
Державні та громадські організації	Державні установи, муніципалітети, школи, університети та інші публічні установи, які потребують послуг безпеки для захисту своїх співробітників, студентів та громадської власності.
Фінансові інститути	Банки, страхові компанії, інвестиційні фірми та інші фінансові установи, які потребують високорівневого захисту своєї інформації, фінансових транзакцій та клієнтських даних.

1.2.3 Дослідження основних частин прототипу сайту.

Прототип веб-сайту складається з наступних базових елементів: заголовок веб-сторінки, панель навігації сайту, основний вміст веб-сторінки, нижній колонтитул.

Заголовок веб-сторінки - Як правило велика смуга зверху з великим заголовком та/або логотипом. Саме тут зазвичай розміщується базова інформація про веб-сайт.

Панель навігації сайту - посилання на розділи сайту зазвичай представлені кнопками меню, посиланнями або вкладками. Як і заголовок, цей контент зазвичай залишається незмінним при переході з однієї веб-сторінки на іншу.

Основний вміст веб-сторінки - Велика область в центрі, яка містить більшу частину унікального контенту даної веб-сторінки, наприклад, відео, яке ви хочете подивитися, або розповідь, яку ви читаєте і т.д. сайту, яка безумовно буде змінюватися від сторінки до сторінки.

Нижній колонтитул - смуга в нижній частині сторінки, яка часто містить дрібний шрифт, повідомлення про авторські права або контактну інформацію.

Веб-сайт складається з двох сторінок: “Головна сторінка” та “Про безпеку”.

Розберемо склад сторінки “Головна сторінка”.

1. Заголовок веб-сторінки.

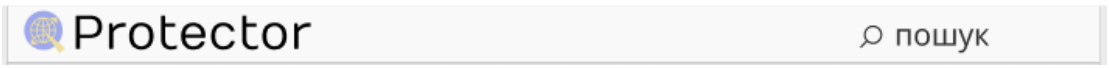


Рисунок 1.4 – Заголовок веб-сторінки.

Окрім стандартного логотипу із назвою веб-сайту, також реалізується функція пошуку по основному вмісту веб-сторінки.

2. Панель навігації по веб-сайту.

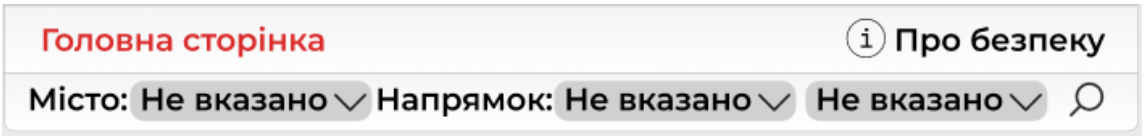


Рисунок 1.5 – Панель навігації веб-сторінки.

У першому рядку знаходиться сама панель навігації по веб-сайту що дозволяє в один клік переміщатися по сторінках веб-сайту, а також розуміти на якій сторінці зараз знаходиться користувач завдяки виділенню кольором обраної сторінки.

У другому рядку реалізовується функція сортування та пошуку по категоріям по основному вмісту веб-сторінки. У користувача завдяки цій панелі буде можливість обрати інтересуюче його місто, та напрямок безпеки який йому потрібен.

3. Основний вміст веб-сторінки

Рисунок 1.6 – Основний вміст веб-сторінки.

В основному розділі веб-сторінки розташовуватиметься по вісім блоків інформації про різні кампанії, які відносяться до напряму безпеки та знаходяться в Україні.

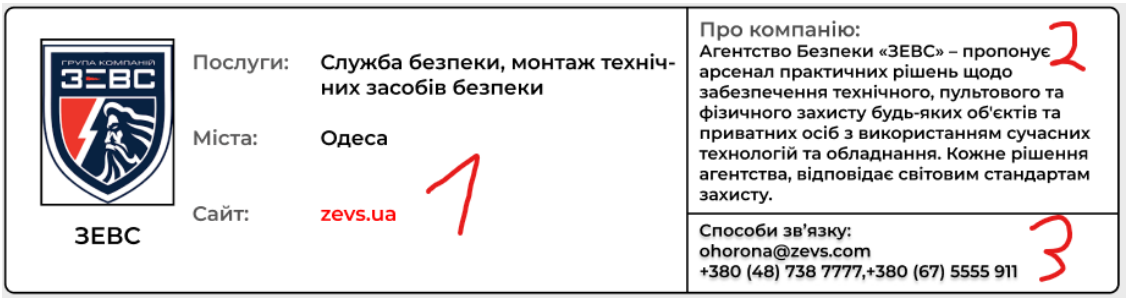


Рисунок 1.7 – Розбір блоку основного вмісту.

Кожен блок інформації поділено на три відділи. У першому, найбільшому, знаходиться логотип кампанії, назва, місце розташування та посилання на веб-сайт. У другому міститься короткий опис кампанії. На третьому відділі розташовуються методи зв'язку з цією кампанією

4. Нижній колонтитул.

Рисунок 1.8 – Нижній колонтитул.

Нижнього колонтитулу як такого на сайті не має. В його області розташована панель що дозволяє переходити на інші сторінки у рамках “Головної сторінки”, та дозволяє користувачам зрозуміти на якій сторінці вони знаходяться.

Розберемо склад сторінки “Про безпеку” .

1. Заголовок веб-сторінки.

Рисунок 1.9 – Заголовок веб-сторінки.

Заголовок веб-сторінки залишився таким самим як і на першій сторінці.

2. Панель навігації веб-сайту.

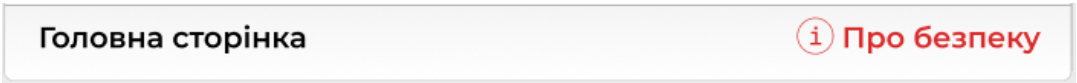


Рисунок 1.10 – Панель навігації веб-сторінки.

На панелі навігації зникло меню із можливістю проводити пошук по категоріям.

3. Основний вміст веб-сторінки.

У цьому випадку основний вміст веб-сторінки поділяється на два блоки.

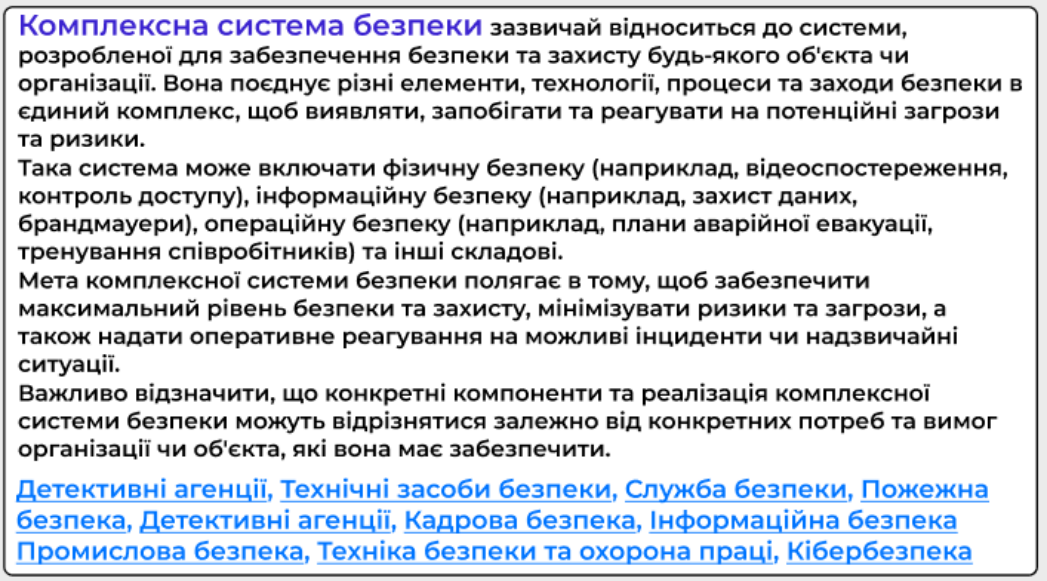


Рисунок 1.11 – Основний вміст веб-сторінки. Перший блок.

Перший блок з основного вмісту веб-сторінки інформує користувача про саме поняття комплексна система безпеки. Та крім того текст що розташовано у нижній частині блоку є посиланням на наступні блоки.

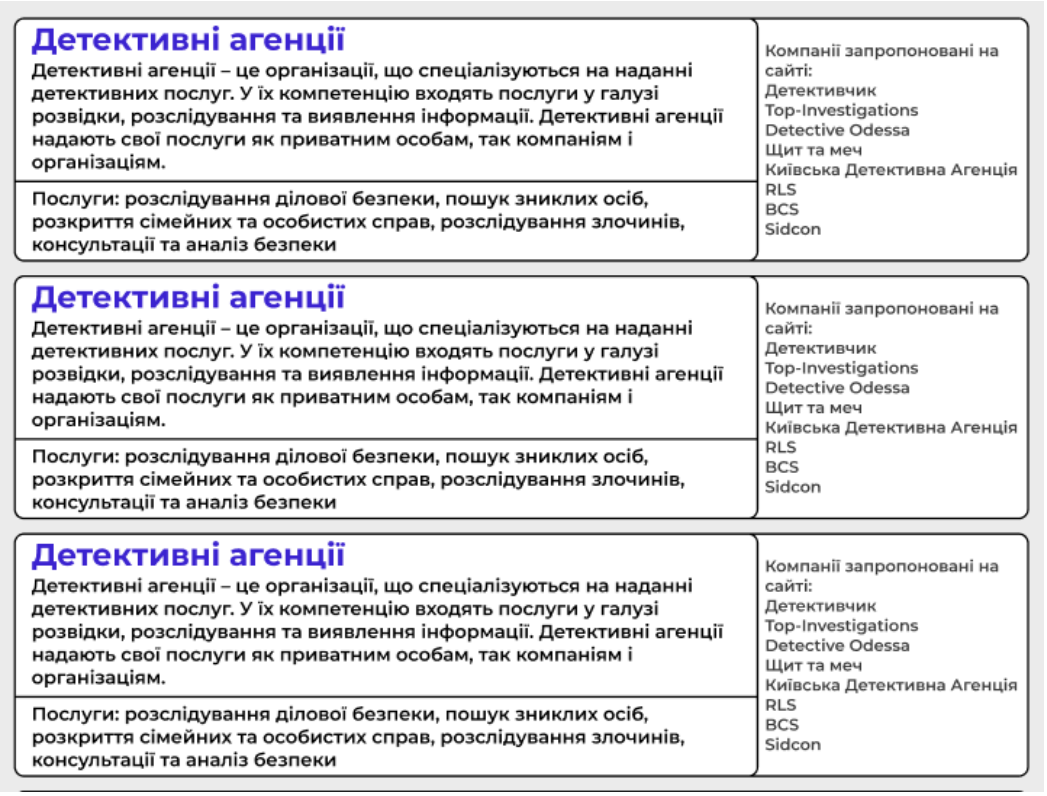


Рисунок 1.12 – Основний вміст веб-сторінки. Другий блок.

Ці блоки створені для того щоб коротко проінформувати користувача про окремі складові комплексної системи безпеки, а також у їх правій частині

розташовано невеликий блок із компаніями які функціонують у цій сфері та занесені на веб-сайт. Крім того посилання з першого великого блоку допоможуть користувачам у навігації по потрібній інформації.

1.3 Аналіз мов програмування розробки back-end частини

1.3.1 Аналіз сучасних мов програмування backend частини

На сьогоднішній день існує велика кількість мов програмування, які можна використовувати для розробки backend (серверної) частини програмного забезпечення. Ось кілька з найпопулярніших мов та їх особливості:

1. Java: Мова програмування Java є дуже популярним вибором для розробки backend (серверної) частини програмного забезпечення. Ось деякі причини, чому Java є затребуваною мовою для цієї цілі:

Таблиця 1.13 Переваги мови програмування Java

Назва переваги	Опис переваги
Кросплатформенність	Java працює на віртуальній машині Java (JVM), що дозволяє їй бути кросплатформенною. Це означає, що код, написаний на Java, може працювати на різних операційних системах, таких як Windows, macOS та Linux, без необхідності переписувати його.
Велика екосистема	Java має велику кількість бібліотек, фреймворків та інструментів, що спрощують розробку backend додатків. Наприклад, фреймворк Spring є одним з найпопулярніших в світі для створення веб-додатків на Java. Він надає широкі можливості для управління залежностями, обробки HTTP-

	запитів, роботи з базами даних тощо.
Висока продуктивність	Java пропонує високу продуктивність та швидкість виконання. Вона використовує JIT (Just-In-Time) компіляцію, що дозволяє оптимізувати виконання коду під час роботи програми. Крім того, Java має потужну збирач мусору, що автоматично вивільняє пам'ять, спрощуючи управління ресурсами.
Безпека	Java має вбудовану підтримку для безпеки, що робить її популярним вибором для розробки місіонерських критичних додатків. Вона має механізми для управління доступом, шифрування даних, підписування та перевірки цифрових підписів, аутентифікації тощо.
Велика спільнота розробників	Java має велику та активну спільноту розробників, що означає, що ви зможете знайти багато ресурсів, підручників, форумів та інших джерел підтримки та допомоги.
Надійність та масштабованість	Java є мовою з високою стійкістю та надійністю. Вона підтримує конкурентні операції та багатопоточність, що робить її відмінним вибором для розробки високонавантажених та масштабованих додатків.

Хоча Java має багато переваг, варто зазначити, що вибір мови програмування для backend залежить від ваших потреб, досвіду та вимог проекту.

2. Python: Мова програмування Python є дуже популярним вибором для розробки backend (серверної) частини програмного забезпечення. Ось деякі причини, чому Python є затребуваною мовою для цієї цілі:

Таблиця 1.14 Переваги мови програмування Python

Назва переваги	Опис переваги
Простота та читабельність	Python має простий та зрозумілий синтаксис, що робить його дуже легким для вивчення та використання. Код на Python зазвичай більш читабельний, що сприяє розробці та підтримці проектів.
Багата екосистема	Python має велику кількість бібліотек та фреймворків, що допомагають розробникам швидко створювати серверні додатки. Фреймворки, такі як Django і Flask, надають потужні засоби для розробки веб-додатків з підтримкою баз даних, маршрутизації, шаблонів тощо.
Широке застосування	Python широко використовується в таких галузях, як наука про дані, штучний інтелект, машинне навчання та аналіз даних. Це робить його привабливим вибором для розробки додатків, що взаємодіють з такими технологіями.
Швидкість розробки	Python відомий своєю високою продуктивністю та швидкістю розробки. Завдяки простоті синтаксису та великій кількості сторонніх бібліотек, розробка на Python може бути швидкою та ефективною.
Підтримка асинхронного	З введенням бібліотеки asyncio в стандартну бібліотеку Python, мова стала більш підходящою для асинхронного

програмування	програмування. Це дає змогу ефективно виконувати багатоопераційні завдання та робити взаємодію з багатьма клієнтами одночасно.
Велика спільнота розробників	Python має одну з найбільших спільнот розробників у світі. Це означає, що ви зможете легко знайти підтримку, ресурси та багато сторонніх модулів, які спростять розробку вашого проекту.

Хоча Python має багато переваг для розробки backend, важливо враховувати специфічні потреби вашого проекту та ваш досвід в роботі з мовою програмування.

3. JavaScript: Мова програмування JavaScript спочатку була розроблена для використання у браузерах як мова для реалізації клієнтської логіки. Проте, з введенням Node.js, JavaScript також став популярним вибором для розробки серверної (backend) частини додатків. Ось деякі причини, чому JavaScript використовується для backend:

Таблиця 1.15 Переваги мови програмування JavaScript

Назва переваги	Опис переваги
Єдина мова на фронтенді та бекенді	Використання JavaScript на обох сторонах - фронтенді та бекенді - дозволяє розробникам використовувати одну мову для програмування як на клієнтській, так і на серверній стороні. Це спрощує перехід від фронтенд-розробки до backend-розробки і забезпечує зручну інтеграцію між двома частинами додатку.
Велика екосистема	JavaScript має широку екосистему бібліотек, фреймворків та інструментів, які полегшують розробку backend. Наприклад, Express.js є одним з

	найпопулярніших фреймворків для розробки серверних додатків на JavaScript. Він надає потужні можливості для маршрутизації, обробки HTTP-запитів та роботи з базами даних.
Асинхронний код	JavaScript має вбудовану підтримку асинхронного програмування, що є важливим аспектом при роботі зі зберіганням даних, мережевими запитами та іншими асинхронними операціями у backend. З використанням промісів або асинхронних функцій (async/await), можна ефективно управляти асинхронним кодом і уникнути блокування виконання.
Швидкість розробки	JavaScript має динамічну та гнучку природу, що сприяє швидкості розробки. Розробка на JavaScript може бути досить ефективною та простою, завдяки зручному синтаксису та великій кількості сторонніх модулів.
Широке застосування	JavaScript є широко використовуваною мовою веб-розробки, і вона має значну підтримку для розробки мобільних додатків, десктопних додатків та навіть IoT-проектів. Це робить JavaScript гнучким вибором для розробки різноманітних типів проектів.

Хоча JavaScript має багато переваг для backend, варто враховувати, що вибір мови програмування залежить від ваших потреб, досвіду та вимог проекту.

4. Ruby: Мова програмування Ruby є ще одним популярним вибором для розробки backend (серверної) частини програмного забезпечення. Ось деякі причини, чому Ruby є затребуваною мовою для цієї цілі:

Таблиця 1.16 Переваги мови програмування Ruby

Назва переваги	Опис переваги
Елегантний та приємний синтаксис	Ruby має дуже зрозумілий та елегантний синтаксис, що допомагає розробникам писати зрозумілий та ефективний код. Він базується на принципі "Читається, як розмова" (Readability Counts), що робить його приємним для програмування.
Продуктивність розробки	Ruby відомий своєю високою продуктивністю розробки. Він має потужну стандартну бібліотеку та велику кількість сторонніх бібліотек і гемів, що спрощують розробку різноманітних функцій та функціональності.
Фреймворк Ruby on Rails	Ruby on Rails (часто називають просто Rails) є одним з найпопулярніших фреймворків для розробки веб-додатків на Ruby. Він пропонує зручність у розробці, стандартизацію та швидкість розробки. Rails надає потужні можливості для маршрутизації, роботи з базами даних, генерації HTML-сторінок, валідації даних та багато іншого.
Зручність роботи з базами даних	Ruby має зручність у роботі з реляційними базами даних. Він надає ORM (об'єктно-реляційне відображення) через ActiveRecord в Ruby on Rails, що дозволяє розробникам працювати з базами даних у зручний та об'єктно-орієнтований спосіб.
Дружність для	Ruby має активну та підтримувану спільноту розробників, яка пропонує багато ресурсів,

розробників	документацію та підтримку. Розробники Ruby сприймають принцип "Спільнота над конкуренцією" (Community over Competition) і допомагають один одному у вирішенні проблем та поширенні знань.

Хоча Ruby має багато переваг для розробки backend, важливо враховувати специфічні потреби вашого проекту та ваш досвід в роботі з мовою програмування.

5. Go: Мова програмування Golang (або просто Go) стала все більш популярною для розробки backend (серверної) частини програмного забезпечення. Ось деякі причини, чому Golang є привабливим вибором для цієї цілі:

Таблиця 1.17 Переваги мови програмування Golang

Назва переваги	Опис переваги
Висока продуктивність	Golang розроблена з орієнтацією на високу продуктивність. Вона володіє ефективною системою збирання сміття, оптимізованою обробкою пам'яті та швидкою компіляцією. Це дозволяє створювати швидкі та ефективні серверні додатки.
Простота та легкість використання	Синтаксис Golang є простим і легким для вивчення. Вона володіє чистим та зрозумілим синтаксисом, що сприяє швидкому розумінню коду. Golang пропонує компактну стандартну бібліотеку, яка містить у собі багато необхідних функцій для розробки серверних додатків.
Конкурентність та	Golang надає потужну підтримку для

паралельність	конкурентного програмування та паралельного виконання. Вона включає в себе вбудовану підтримку горутин (goroutines) та каналів (channels), які дозволяють ефективно керувати багатопотоковим виконанням та забезпечувати безпечну взаємодію між горутинами.
Надійність	Golang ставить перед собою завдання забезпечити надійність у своїй роботі. Вона включає в себе механізми перевірки помилок під час компіляції, а також пропонує стандартні засоби для обробки помилок та відновлення після них. Це допомагає створювати стійкі та надійні серверні додатки.
Розширюваність	Golang підтримує створення бінарних виконуваних файлів без залежностей, що дозволяє легко розповсюджувати та встановлювати серверні додатки на різних платформах. Вона також має вбудовану підтримку для створення пакетів (packages) та модулів (modules), що полегшує розширення та повторне використання коду.

Хоча Golang має багато переваг для розробки backend, варто враховувати, що вибір мови програмування залежить від ваших потреб, досвіду та вимог проекту.

6. PHP: Мова програмування PHP є однією з найпопулярніших мов для розробки backend (серверної) частини веб-додатків. Ось деякі причини, чому PHP є популярним вибором для цієї цілі:

Таблиця 1.18 Переваги мови програмування PHP

Назва переваги	Опис переваги
Широке поширення та підтримка	PHP є однією з найбільш поширених мов програмування для розробки веб-додатків. Це означає, що ви зможете знайти велику спільноту розробників, багато сторонніх ресурсів, документацію та підтримку.
Простота вивчення та використання	PHP має простий синтаксис, який легко вивчити, навіть для початківців. Це дозволяє швидко розпочати розробку веб-додатків. Крім того, вона має велику кількість вбудованих функцій та бібліотек, що полегшує використання готових рішень для розробки.
Велика кількість фреймворків	PHP має розширену екосистему фреймворків, які спрощують процес розробки веб-додатків. Найпопулярніші з них включають Laravel, Symfony, CodeIgniter та Yii. Ці фреймворки надають широкі можливості для маршрутизації, бази даних, аутентифікації, шаблонізації та багато іншого.
Робота з базами даних	PHP має вбудовану підтримку для багатьох реляційних баз даних, таких як MySQL, PostgreSQL, SQLite та інші. Вона надає легкий доступ до бази даних, дозволяє виконувати запити та керувати даними.
Швидкість виконання	PHP відомий своєю швидкістю виконання, особливо в контексті веб-розробки. Завдяки розширенням, таким як OPCache, PHP може кешувати та прискорювати виконання коду, що поліпшує продуктивність веб-додатків.

Хоча PHP має багато переваг для розробки backend, варто враховувати, що вибір мови програмування залежить від ваших потреб, досвіду та вимог проекту.

Це лише кілька з багатьох мов програмування, які можна використовувати для розробки backend. Вибір мови залежить від ваших потреб, досвіду та вимог проекту. Кожна з цих мов має свої переваги та особливості, тому важливо зробити докладне дослідження перед вибором.

1.3.2 Аналіз мови програмування C#

Є також ще одна мова програмування і її назва це C#, цю мову я використовую як головну в написанні сайту.

C# (C sharp) - це сучасна, об'єктно-орієнтована мова програмування, розроблена компанією Microsoft. Вона була представлена в 2000 році як одна з основних мов для розробки програмного забезпечення на платформі Microsoft .NET. Назва "C#" вказує на її розміщення в лінійці мов програмування C, а також символ, який використовується для позначення акорду в музиці.

Ось деякі основні риси та характеристики мови програмування C# які показані у таблиці 1.19:

Назва риси	Опис риси
Об'єктно-орієнтований підхід	C# підтримує об'єктно-орієнтовану парадигму програмування, що дозволяє створювати класи, об'єкти, спадкування, поліморфізм та інші концепції ООП. Це дозволяє розробникам створювати більш організований і повторно використовуваний код.
Мультиплатформеність	Починаючи зі створення .NET Core, C# можна використовувати на різних платформах, таких як Windows, macOS і Linux. Це дозволяє розробникам

	створювати кросплатформенні програми, які працюють на різних операційних системах.
Управління пам'яттю	C# використовує автоматичне управління пам'яттю, що дозволяє розробникам зосередитися на логіці програми, не турбуючись про вручне виділення та звільнення пам'яті. Механізм збирача сміття автоматично визначає непотрібні об'єкти та звільняє пам'ять, зменшуючи ризик витоку пам'яті.
Багатий стандартний набір бібліотек	C# має широкий набір стандартних бібліотек, що надають доступ до різноманітних функціональних можливостей, таких як робота з мережами, робота з базами даних, графічний інтерфейс користувача і багато іншого. Це спрощує розробку програм та дозволяє використовувати готові компоненти для реалізації різних завдань.
Інтеграція з платформою .NET	C# використовується в платформі .NET, що забезпечує широкий спектр інструментів, бібліотек і сервісів для розробки програмного забезпечення. Розробники можуть використовувати такі інструменти, як Visual Studio, для створення, налагодження і впровадження програм на C#.

Таблиця 1.19 Основні риси та характеристики мови програмування C#

C# став популярним вибором для розробки різних видів програм, від десктопних додатків до веб-програм та мобільних додатків. Він надає потужні можливості для створення надійних, ефективних і сучасних програмних рішень.

Мова програмування C# є потужним і широко використовуваним інструментом для розробки backend (серверної) частини програмного забезпечення. Ось деякі причини, чому C# є популярним вибором для цієї цілі які описані у таблиці 1.20:

Таблиця 1.20 Перелік причин вивчення мови програмування C#

Назва причини	Опис
Розширена платформа .NET	C# є однією з основних мов програмування платформи .NET. Це означає, що ви можете використовувати багато фреймворків та бібліотек, які надаються в рамках екосистеми .NET, таких як ASP.NET, Entity Framework, LINQ і багато інших. Це спрощує розробку, підтримку та інтеграцію з іншими компонентами системи.
Сильна типізація та безпека	C# є мовою зі строгою типізацією, що дозволяє виявляти помилки під час компіляції і забезпечує безпеку типів в процесі виконання. Це допомагає уникнути багатьох помилок та забезпечити стабільність та надійність програмного забезпечення.
Масштабованість та продуктивність	C# надає потужні механізми для масштабування серверних додатків. Крім того, C# забезпечує широкі можливості для оптимізації продуктивності та виконання операцій з великими обсягами даних.
Інтеграція з Microsoft-екосистемою	C# є мовою, яку рекомендує Microsoft для розробки веб-додатків на платформі .NET. Це означає, що ви можете використовувати

	інструменти, такі як Visual Studio, для зручної розробки, налагодження та впровадження. Крім того, C# добре інтегрується з іншими продуктами Microsoft, такими як Microsoft SQL Server, Azure та інші.
Підтримка спільноти та ресурсів	C# має велику спільноту розробників, яка пропонує багато ресурсів, форумів, бібліотек та документації. Це означає, що ви можете швидко знайти відповіді на свої питання та рішення для своїх задач.

Хоча C# має багато переваг для розробки backend, варто враховувати, що вибір мови програмування залежить від ваших потреб, досвіду та вимог проекту.

Мова програмування C# має кілька переваг, які роблять її привабливою для розробників. Ось деякі з них:

Таблиця 1.21 Переваги мови програмування C#

Назва переваги	Опис переваги
Широке застосування	C# є однією з основних мов для розробки програмного забезпечення на платформі Microsoft .NET. Вона використовується для створення різних типів програм, включаючи десктопні додатки, веб-додатки, мобільні додатки, хмарні служби і багато іншого. Це дозволяє розробникам працювати в різних областях із застосуванням однієї мови.
Безпека та надійність	Строга типізація мови C# допомагає уникнути багів, пов'язаних з типами даних, на етапі компіляції. Це забезпечує більшу безпеку та надійність програм.

	Крім того, C# має вбудовану підтримку винятків, що дозволяє керувати помилками та виконувати гарячу обробку виключень.
Легкість вивчення	C# має синтаксис, подібний до інших мов з сімейства мов C (наприклад, C, C++), що робить його відносно легким для вивчення для розробників, які вже знайомі з цими мовами. Крім того, наявність інтегрованого середовища розробки, такого як Visual Studio, спрощує процес написання, налагодження та тестування коду на C#.
Широкий набір бібліотек та фреймворків	Спільна платформа .NET надає розробникам доступ до великої кількості стандартних бібліотек і фреймворків, які спрощують розробку програмного забезпечення. Ці бібліотеки мають готовий код для роботи з базами даних, мережами, графікою, безпекою та багатьма іншими аспектами розробки програм.
Підтримка асинхронного програмування	C# надає потужні засоби для асинхронного програмування за допомогою ключових слів async та await. Це дозволяє розробникам створювати швидкодіючі програми, які ефективно використовують ресурси системи та забезпечують плавний інтерфейс користувача.

Загалом, C# є потужною мовою програмування з великим спектром можливостей і широким застосуванням. Вона надає розробникам зручність, надійність та продуктивність при створенні різноманітних програмних рішень.

1.4 Розробка backend-частини веб-сайту з дослідження напрямку безпеки України.

Прописую код для того щоб якщо зараз перейти на несправжню сторінку то видавало помилку яка показана на рисунку 1.21:

```
@page
@model ErrorModel
@{
    ViewData["Title"] = "Error";
}

<h1 class="text-danger">Error.</h1>
<h2 class="text-danger">An error occurred while processing your request.</h2>
```

Рисунок 1.21 Код що викликає помилку користувачу

Роблю функцію щоб можна було викликати файли між собою яка показана на рисунку 1.22

```
@using Protector
@namespace Protector.Pages
@addTagHelper *, Microsoft.AspNetCore.Mvc.TagHelpers
```

Рисунок 1.22 Код що може викликати файли з другої папки

Створюю код для того щоб була кнопка яка повертає на головну сторінку який показаний на рисунку 1.23

```
app.MapControllerRoute(
    name: "default",
    pattern: "{controller}/{action=Index}/{id?}");

app.MapFallbackToFile("index.js"); ;
```

Рисунок 1.23 Код для кнопки додому

2 Економічна частина

В дипломному проекті створений веб-сайт дослідження напрямку безпеки.

Веб-сайт дослідження напрямку безпеки України є актуальним та затребуваним у сучасності, тому що аналогів такому веб-сайту майже не має. Суспільству потрібен Web-сайт на якому буде можливість із легкістю, швидко знайти інформацію, щодо напрямків безпеки України, крім того ще й отримати контакти кампаній, що його заінтересують у цьому на-прямку. Аналогів такому Web-сайту майже не має, тому що є подібні Web-сайти, але набагато менш охоплюючі. Тобто Web-сайти конкретного міста, чи конкретного напрямку з напрямку безпеки України.

При оцінці ефективності створюваного сайту виходимо з того, що залежно від характеру ефекту, що досягається, можуть бути визначені наступні види ефективності сайту: економічна, функціональна та соціальна ефективність.

Створений веб-сайт не є комерційним тому економічна ефективність не може бути розрахована. Визначаємо загальні витрати ($В_з$) на створення сайту, що складаються з декількох параметрів:

$$В_з = В_р + В_в + В_е \ , \qquad (2.1)$$

де $В_р$ – витрати на розробку сайту;

$В_в$ – витрати на впровадження сайту;

$В_е$ – витрати на експлуатацію сайту;

Витрати на розробку сайту ($В_р$) є одноразовими та складаються з вартості наступних видів робіт зі створення сайту :

1. Розробка дизайну сайту: розробка макетів дизайну для головної та внутрішньої сторінок сайту; розробка фірмового стилю, логотипу
2. Наповнення сайту інформацією: наповнення та форматування web-сторінок; обробка малюнків для публікації на web-сторінках, верстка (переклад в HTML-формат) web-сторінок

3. Програмна розробка сайту: створення програмного коду сайту, програмування динамічних елементів (анімаційних елементів, флеш-заставок)
4. Реалізація пошукових можливостей сайту: настройка модуля пошуку по сайту; створення карти сайту; настройка виведення шляху по сайту

Для визначення витрат на розробку сайту ($В_р$) розраховуємо оплату праці виконавців, безпосередньо притягнених до її виконання. Для реалізації проекту Web-системи використовуються наступні спеціалісти: веб-дизайнер, frontend-розробник, backend-розробник,

Для визначення трудомісткості розробки сайту ($В_р$) складено план-графік по розробці web-сайту і тривалості виконання робіт. Розподіл робіт по етапах і видах виконавців наведено в таблиці 2.1.

Таблиця 2.1 – План-графік по розробці Web-сайту

№	Назва етапу	Час виконання (годин)	Посада виконавця
1	Створення дизайну елементів для веб-сайту.	10	Веб-дизайнер
2	Створення макету веб-сайту.	10	Веб-дизайнер
3	Розробка frontend-частини веб-сайту.	50	Frontend-розробник
4	Наповнення веб-сайту інформацією	6	Backend-розробник
5	Реалізація пошукових можливостей веб-сайту	6	Frontend-розробник
6	Розробка backend-частини веб-сайту.	50	Backend-розробник
ВСЬОГО:		132 години	

Розрахунок трудомісткості здійснений в наступній послідовності:

1. Складений перелік всіх етапів і видів робіт, які необхідно виконати в ході даної розробки. Після узгодження з керівником проекту допущено виключення, доповнення, об'єднання окремих етапів і видів робіт;

2. По кожному виду робіт визначений кваліфікаційний рівень виконавців. В разі виконання однієї роботи виконавцями різної кваліфікації, робота розподілена на ряд паралельних конкретних робіт для кожної категорії виконавця.

В умовах відсутності нормативної бази тривалість виконання окремих робіт розраховуємо на основі вірогідних оцінок робіт, що задаються виконавцями.

Розмір заробітної плати розраховуємо виходячи з чисельності різних категорій виконавців, трудомісткості, що витрачається ними на виконання різних видів робіт, а також їх середньої заробітної плати (ставки) за годину.

При визначенні вартості виконуваних робіт орієнтуємося на мінімальну заробітну плату, встановлену Відповідно до «Закону про Державний бюджет України» (станом на 1.01 поточного року), враховуючи кваліфікацію виконавців, Витрати на заробітну плату приведені в таблиці 3.2. (мінімальна заробітна плата в місяць - 6700 грн; в годину - 40,43 грн)

Таблиця 2.2 – Витрати на заробітну плату

№	Персонал	Етапи розробки	Кількість робочих годин	Погодинна ставка грн.	Заробітна плата, грн.
1	Веб-дизайнер	Дизайн елементів, створення макету	20	110	2200
2	Frontend-розробник	frontend-розробка, реалізація пошуку	56	120	6720
3	Backend-розробник	backend-розробка, наповнення інформацією	56	120	6720
ВСЬОГО:					$В_{зп}$ = 15640

До складу витрат на оплату праці також включаються податки, збори і інші обов'язкові платежі, встановлені системою оподаткування що діє. Розмір єдиного соціального внеску складає 22% від заробітної плати, розраховується за наступною формулою:

$$В_{єсв} = В_{зп} \text{ x } 0,22 \quad (2.2)$$

$$В_{єсв} = 15640 \text{ x } 0,22 = 3128$$

Загальні витрати ($В_р$) на розробку веб-сайту розраховуються як сума витрат на заробітну плату праці персоналу ($В_{зп}$) та єдиного соціального внеску ($В_{єсв}$):

$$В_р = В_{зп} + В_{єсв} \quad (2.3)$$

$$В_р = 15640 + 3128 = 18768$$

Витрати на впровадження сайту ($В_в$) складаються з двох складових :

- витрати на реєстрацію доменного імені на 1 рік ($В_{в1}$);
- витрати на реєстрацію в пошукових системах ($В_{в2}$), наприклад, Yandex, Google, Rambler и т.п.)

$$В_в = В_{в1} + В_{в2} \quad (2.4)$$

$$В_в = 2748 + 0 = 2748$$

Витрати на експлуатацію сайту (Ве) включають вартість робіт з підтримки сайту в робочому стані і вартість послуг по продовженню доменного імені на 1 рік.

Роботи по підтримці сайту в робочому стані включають в себе:

1. Оновлення даних на сайті;
2. Створення нових розділів на сайті;
3. Видалення застарілої інформації з сайту;
4. Налаштування параметрів сервера хостингу;
5. Моніторинг роботи сервера хостингу;
6. Забезпечення щомісячного захисту сайту;

У таблиці 2.3 визначаються постійні витрати як сума витрат на впровадження та експлуатацію сайту протягом року.

Таблиця 2.3 – Постійні витрати

№	Стаття витрат	Вартість за рік, грн.
1	Актуалізація інформації на веб-сайті	24,000
2	Взаємодія із хостингом	18,000
3	Забезпечення захисту сайту	20,000
Всього:		$В_{пост}$ = 62, 000

Загальні витрати ($В_з$) на розробку, впровадження та експлуатацію веб-сайту розраховуються за наступною формулою:

$$В_з = В_р + (В_в + В_е) = (62000 + 2748) + 18768 = 83516$$

Функціональна ефективність веб-сайту з дослідження напрямку безпеки України проявляється:

- в забезпеченні повноти, точності і доступності інформації про напрямки безпеки в Україні, діяльність компаній що її забезпечують, товари і послуги що стосуються напрямку безпеки у будь-який слушний для користувача час доби;

- в оптимізації пошукових процесів звичайних користувачів;

Соціальна ефективність веб-сайту з дослідження напрямку безпеки України виражається у наступному:

1. Покращення показників швидкості знаходження потрібної інформації стосовно впровадження заходів безпеки в Україні

2. Інформування найбільшого числа зацікавлених осіб про безпеку в України.

3. Формування більш усвідомленого суспільства.

3 Охорона праці

3.1 Вступ

Охорона праці на виробництві є важливою галуззю, що займається забезпеченням безпеки та здоров'я працівників на робочому місці. Її роль полягає в усуненні або зниженні ризиків, пов'язаних з виробничою діяльністю, та встановленні необхідних заходів для запобігання нещасним випадкам та професійним захворюванням.

Охорона праці спрямована на зменшення ризику виникнення нещасних випадків на робочому місці. Це досягається шляхом впровадження безпечних процесів, використання захисного обладнання, проведення навчання та інформування працівників про можливі ризики та виконання протиаварійних заходів, а також оцінки ризиків, контролю за умовами праці та впровадженням заходів щодо попередження захворювань.

В даному дипломному проекті проведено аналіз умов праці працівника на робочому місці за комп'ютером. Даний вибір обумовлений темою мого дипломного проекту.

3.2 Аналіз та безпека умов праці працівника із комп’ютером

Праця за комп'ютером стала невід'ємною частиною багатьох професій. Основною метою такого аналізу є виявлення потенційних ризиків, пов'язаних з роботою за комп'ютером, та розробка заходів щодо їх попередження або зниження.

Основні шкідливі та небезпечні виробничі чинники, які мають дію на працівника під час роботи:

- Робота за комп'ютером може викликати навантаження на очі;

- Довготривала робота за комп'ютером може призводити до мускульно-скелетних проблем, таких як тунельний синдром, запалення сухожиль, біль у шиї і спині;

- Належно налаштоване робоче місце користувача ПК;

- Шкідливі речовини, такі як пил, алергени, випромінювання екрану, статична електрика тощо;

- належне навчання та інформування робітників з питань безпеки.

3.3 Організація робочого місця працівника із комп’ютером

При організації робочого місця із комп’ютером та периферійними пристроями (клавіатура, маніпулятор «миша», принтер, тощо), слід передбачити:

Стіл та стільці: Робочий стіл повинен бути достатньо широким і міцним для розташування комп'ютера, клавіатури, миші та інших необхідних предметів. Він повинен мати достатньо простору для розміщення рук і ніг працівника. Стілець повинен бути зручним, з належною підтримкою спини і можливістю регулювання висоти.

Монітор: Монітор повинен бути розташований на відстані від очей працівника, звернутим у напрямку знизу догори на кут приблизно 10-20 градусів. Рекомендується використовувати монітор з антиблисковим покриттям, щоб зменшити втому очей.

Клавіатура та миша: Клавіатура та миша повинні бути розташовані на такій висоті та відстані, щоб працівник міг використовувати їх без напруження. Клавіатура повинна бути розташована на рівні підлокітників, а миша - поруч з клавіатурою.Робоче місце повинно мати належне освітлення. Якщо можливо, слід використовувати природне освітлення, уникати слабкого або перекошеного освітлення, а також блисків на екрані комп'ютера.

3.4 Електробезпека

Перед підключенням комп'ютера до електричної розетки потрібно переконатися, що вхідне напруга відповідає вимогам вашої системи, використовувати надійний блок безперебійного живлення (UPS) для захисту комп'ютера від перепадів напруги та можливих перебоїв в електропостачанні.

Кабелі живлення та інші кабелі мають бути в хорошому стані, без пошкоджень. Потрібно уникати перетягування кабелів, що може призвести до

виривання їх з розеток. Не перегинати та не ставити важкі предмети на кабелі, щоб уникнути пошкоджень ізоляції.

Заземлення є важливим для захисту від статичної електрики та може допомогти запобігти можливим пошкодженням компонентів.

3.5 Вимоги до освітлення

Належне освітлення допомагає запобігати зрячим напруженням, покращує концентрацію та забезпечує комфорт під час роботи за комп'ютером.:

Рекомендована яскравість освітлення в зоні робочого місця з комп'ютером зазвичай становить приблизно 500-750 люксів. Варто враховувати, що яскравість може варіюватися в залежності від типу робіт та вікових особливостей працівника. Забезпечення регульованої яскравості, наприклад, за допомогою ламп з диммером або використання природного освітлення, є бажаним.

Важливо, щоб світло рівномірно розподілялося на робочому столі. Уникайте яскравих плям, тіней або блисків на екрані комп'ютера. Використання антиблискових екранів або регульованого напрямлення світла може допомогти уникнути непотрібного відблиску.

Використання природного світла є бажаним, оскільки воно допомагає знизити втомлюваність і покращує настрій працівника. Якщо природного світла недостатньо, слід використовувати штучне освітлення. Рекомендується використовувати світлодіодні або люмінесцентні лампи, оскільки вони енергоефективні та надають яскраве та однорідне світло.

Кольорова температура світла також важлива. Рекомендується використовувати світло з кольоровою температурою приблизно 5000-6500 Кельвінів, оскільки воно наближене до природного денного світла та сприяє ясності зору.

Джерела світла слід розташовувати так, щоб вони не створювали тіней або блисків на екрані комп'ютера. Оптимальне розташування полягає в тому, щоб світло спадало зверху або з боку, не забезпечуючи прямого відблиску на екран.

3.6 Мікроклімат

Основні аспекти мікроклімату, які слід враховувати, включають температуру, вологість, швидкість повітря та якість повітря.

Рекомендована температура в робочих приміщеннях, де працюють з комп'ютерами, зазвичай коливається в межах 20-24°C. Приміщення повинні бути належним чином опалюваними або охолоджуваними, щоб забезпечити комфортні умови для працівників.

Відносна вологість повітря також впливає на комфорт працівників. Рекомендовані значення вологості зазвичай становлять 40-60%. Занадто сухе повітря може спричинити сухість очей і шкіри, а занадто вологе повітря може створити відчуття дискомфорту. Використання вологозберігаючих пристроїв або вологозберігаючих рослин може допомогти підтримувати оптимальний рівень вологості.

Швидкість руху повітря в приміщенні також має значення. Занадто сильний потік повітря може створити дискомфорт, спричинити сухість очей та висихання слизових оболонок. Рекомендована швидкість повітря зазвичай не перевищує 0,25 м/с.

Якість повітря в приміщенні є важливим аспектом мікроклімату. Добре провітрювання приміщення та наявність систем вентиляції допомагають забезпечити свіжий повітря та видалити шкідливі речовини, такі як випари з меблів, друкуючих пристроїв тощо. Регулярне очищення та обслуговування систем вентиляції також важливо.

3.7 Пожежна безпека

Оскільки у випадку роботи з комп'ютером загальні характеристики приміщення не є вибухо-пожежонебезпечними, в основному для цих типів приміщень не встановлюється вибухонебезпечна зона та пожежонебезпечний клас.

Однак, незалежно від категорії приміщення, завжди рекомендується приймати заходи щодо попередження пожеж та забезпечення безпеки. Для цього можна використовувати такі засоби:

1. Засоби пожежної сигналізації: Це можуть бути димові датчики, теплові датчики, вогнегасники з автоматичним спрацьовуванням, пожежні спринклерні системи тощо. Вибір засобів залежить від конкретних умов приміщення та рекомендацій місцевих нормативів.

2. Засоби пожежогасіння: Для малих робочих приміщень можуть використовуватись первинні вогнегасники, наприклад, порошкові або вуглекислотні вогнегасники..

Важливо зазначити, що вибір конкретних засобів пожежогасіння та пожежної сигналізації повинен здійснюватись згідно з місцевими нормами, стандартами та рекомендаціями, а також з урахуванням конкретних умов та потреб вашої організації.

ВИСНОВКИ

Підчас виконання роботи вдалося більш детально проаналізувати такі питання як: стан ринку безпеки України, поняття комплексної системи безпеки та її складових, рішення щодо прототипування web-сайту та аналіз прототипу, рішення щодо створення web-сайту. Крім того вже на практиці закріпити отримані теоретичні знання щодо створення web-сайтів з точки зору backend-розробника.

Мета роботи була досягнена тобто був створений зручний інструмент для навігації по інформаційному простору безпеки в Україні.

Завдання роботи було виконане тобто було створено web-сайт, що зможе надати користувачам можливості для зручної навігації по ринку безпеки України.

Крім того було розроблено план подальшого розвитку створеного web-сайту з дослідження напрямку безпеки України. До цього плану входять такі пункти: зв’язати сайт з сервером, добавити до сайту базу даних, зробити екран завантаження, переробити вікно помилки, і так далі.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Козлов С. Стаття "Організація комплексної системи забезпечення безпеки підприємства" [Електронний ресурс] / Сергій Козлов. – 2012. – Режим доступу до ресурсу: http://nta.com.ua/article-busines-safe/.

2.Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В.Л. Бурячок,В. Б. Толубко, В. О. Хорошко, С.В. Толюпа]; за заг.ред. д-ра техн. наук, професора В. Б. Толубка.- К.: ДУТ, 2015.- 288с

3. Троелсен Э. Мова програмування C# 9 и платформа .NET 5 / Э. Троелсен, Ф. Джепікс., 2022. – 632 с. – (10).

4. Васильєв О. Програмування на C# для початківців. / Олексій Васильєв., 2021. – 592 с.

5.Грибан В. Г., Негодченко О. В Охорона праці. Навч. посіб. 2-ге вид-К.: Центр учбової літератури, 2011.- 280с.

6. Когут Ю. Кібербезпека та ризики цифрової трансформації компаній / Юрій Когут., 2021- 372 с.

Додаток А. Слайди мультимедійної презентації

Комплексна система забезпечення безпеки підприємства(КСЗБП)

КСЗБП - це комплекс що складається з багатьох складових, але для початку розберемося у тому які саме принципи функціонування закладені у цій системі.

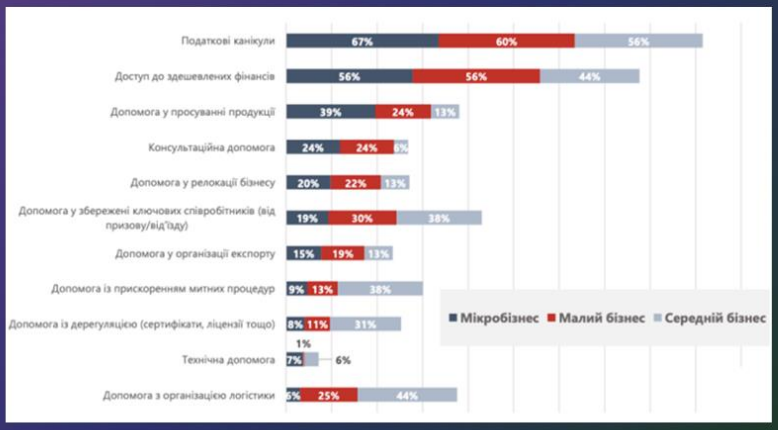
Назва принципу	Опис
Законність	Діяльність системи безпеки має ґрунтуватися на існуючих у країні законах. Тільки це дозволить підприємству відчувати надійність свого існування та компенсувати зазнані збитки з найменшим ризиком.
Розумна достатність	Ступінь загрози має викликати адекватний рівень реакції. Тобто якщо людині на голову села метелик, можна її просто зігнати, а не бити по голові молотком.
Швидкість реагування	Ключовим словом під час запровадження цього принципу має бути слово «негайно».
Комплексність	Система безпеки має задіяти всі наявні для підприємства різноманітні ресурси для забезпечення реагування на загрози.
Ефективність	Система безпеки повинна не бути даниною моді, а повинна реально мінімізувати втрати і, за умови правильної постановки справи, приносити дохід.

Аналіз складових КСЗБП

КСЗБП складається з таких складових:

- Пожежна безпека
- Детективні агенції
- Охоронні агенції
- Кібербезпека
- Технічні засоби безпеки
- ТБ та охорона праці
- Кадрова безпека
- Інформаційна безпека
- Промислова безпека

Аналіз стану ринку безпеки сучасної України



Тезово перерахуємо фундаментальні загрози (економічні) малому бізнесу станом на червень 2022 року. До них відносяться:

1. Війна - і всі ризики, з нею пов'язані

2. Відсутність інвестицій в Україну

3. Дорогі енергоносії

4. Проблеми з логістикою – руйнування інфраструктури як наслідок бойових дій, блокування портів

5. Проблеми з паливом

6. Відсутність ключових співробітників – виїзд за межі України, заклик до ЗСУ, поранення чи смерть внаслідок бойових дій

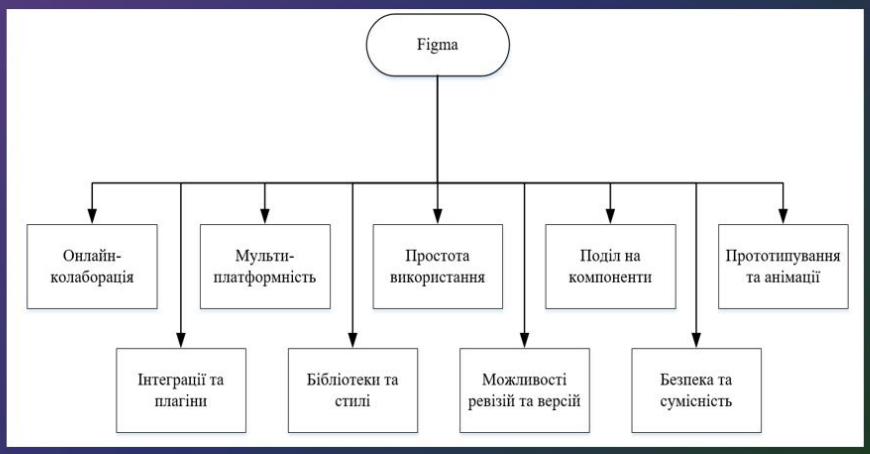
7. Падіння низки секторів економіки, наприклад, сільське госп-во, виробництво, металургія

Аналіз рішень щодо прототипування сайту.

- Популярні сайти конструктори

№	Назва	Опис сайту
1	AdobeXD	Це інструмент, розроблений Adobe, який пропонує функції для створення макетів, прототипів та дизайну інтерфейсу
2	Sketch	Це інструмент для створення макетів та прототипів, розроблений спеціально для користувачів macOS
3	InVision	Це платформа, призначена для створення інтерактивних прототипів та спільної роботи над проектами.
4	Axure RP	Це інструмент для створення прототипів з широкими можливостями та гнучкими функціями
5	Marvel	Це простий у використанні інструмент для створення прототипів та дизайну інтерфейсу.
6	Balsamiq	Це інструмент для створення прототипів з упором на начерки та швидке моделювання.
7	Proto.io	Це онлайн платформа для створення інтерактивних прототипів. Proto.io надає широкий вибір елементів дизайну та функцій.
8	Justinmind	Це інструмент, призначений для створення складних прототипів із широким набором функцій.
9	Framer	Це інструмент для створення прототипів з акцентом на дизайн та анімацію.
10	Figma	Це онлайн-сервіс для розробки інтерфейсів та прототипування з можливістю організації спільної роботи в режимі реального часу.

Figma



Цільова аудиторія нашого сайту

Види ЦА нашого сайту:

Вид послуг	Опис послуги
Корпоративні клієнти	Великі та середні підприємства, які потребують комплексних рішень щодо забезпечення безпеки своїх фізичних та інформаційних ресурсів. Це може включати фірми охорони, системи відеоспостереження, контроль доступу, кібербезпеку та управління ризиками.
Малі та середні підприємства	Власники малого бізнесу, яким потрібні простіші та доступніші рішення безпеки. Це може включати системи відеоспостереження, охоронну сигналізацію, безпеку мережі та консультаційні послуги з безпеки.
Приватні особи	Люди, яким потрібна індивідуальна безпека для себе, свого житла та майна. Включає послуги із забезпечення особистої безпеки, встановлення домашньої безпеки, моніторинг та тривожні системи.
Державні та громадські організації	Державні установи, муніципалітети, школи, університети та інші публічні установи, які потребують послуг безпеки для захисту своїх співробітників, студентів та громадської власності.
Фінансові інститути	Банки, страхові компанії, інвестиційні фірми та інші фінансові установи, які потребують високорівневого захисту своєї інформації, фінансових транзакцій та клієнтських даних.

Основні частини прототипу сайту

Заголовок веб-сторінки - Як правило велика смуга зверху з великим заголовком та/або логотипом. Саме тут зазвичай розміщується базова інформація про веб-сайт.

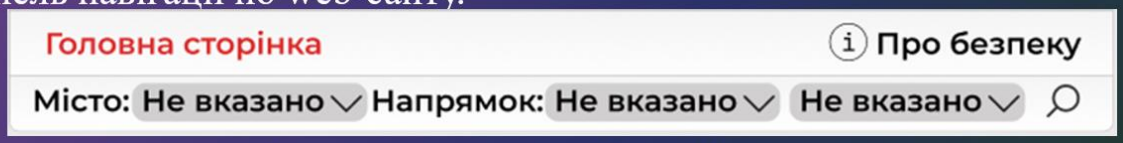
Панель навігації сайту - посилання на розділи сайту зазвичай представлені кнопками меню, посиланнями або вкладками. Як і заголовок, цей контент зазвичай залишається незмінним при переході з однієї веб-сторінки на іншу.

Основний вміст веб-сторінки - Велика область в центрі, яка містить більшу частину унікального контенту даної веб-сторінки, наприклад, відео, яке ви хочете подивитися, або розповідь, яку ви читаєте і т.д. сайту, яка безумовно буде змінюватися від сторінки до сторінки.

Нижній колонтитул - смуга в нижній частині сторінки, яка часто містить дрібний шрифт, повідомлення про авторські права або контактну інформацію.

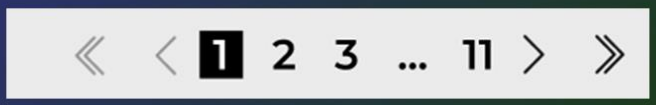
Заголовок web-сторінки.

Панель навігації по web-сайту.



Основний вміст web-сторінки.

Нижній колонтитул.



Аналіз засобів для створення backend-частини Web-сайту.

Аналіз мови програмування C#

Розробка backend-частини веб-сайту з дослідження напрямку безпеки України. Видавання сторінки помилки

```
@page
@model ErrorModel
@{
    ViewData["Title"] = "Error";
}

<h1 class="text-danger">Error.</h1>
<h2 class="text-danger">An error occurred while processing your request.</h2>
```

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

ВІДГУК

керівника на дипломний проект здобувача (здобувачки) освіти

відділення комп'ютерних систем

Осадчого Володимира Ігоровича

(прізвище, ім`я та по батькові)

Спеціальність: *123 "Комп'ютерна інженерія"*

Освітня програма: *«Обслуговування комп'ютерних систем і мереж»*

Тема дипломного проекту: *Розробка backend-частини веб-сайту з дослідження напрямку безпеки України.*

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ

а) обсяг і якість виконання проекту (графічного матеріалу і розрахунково-пояснювальної записки) *Дипломний проект виконано відповідно технічному завданню. Пояснювальна записка містить 69 сторінок. У пояснювальній записці наведено етапи створення захищеного інформаційного середовища на основі міжнародних стандартів та рекомендацій. Графічна частина складається з слайдів мультимедійної презентації, які також містять креслення, передбачені технічним завданням. Якість виконання пояснювальної записки та графічної частини добра, розробку виконано в повному обсязі.*

б) самостійність роботи над проектом: *Протягом всього строку дипломного проектування та переддипломної практики здобувач освіти Осадчий В.І. поступово та послідовно виконував всі етапи розробки. Всі роботи студент виконував самостійно, з оглядом на рекомендації керівника*

в) теоретична підготовка випускника (випускниці): *Здобувач освіти Осадчий В.І. під час роботи над дипломним проектом вивчив достатню кількість літературних джерел та матеріалів за даною тематикою.*

Вважаю, що теоретична підготовка дипломника добра і він готовий до захисту дипломного проекту

г) вміння розв'язувати виробничі та конструкторські питання _____

Під час дипломного проектування здобувач освіти Осадчий В.І. мав змогу самостійно приймати окремі рішення з вибору оптимальних рішень зі стандартів та показав вміння організовано працювати над поставленим завданням, складати креслення, вивчати програмні рішення в напрямку систем протидії витокам, апаратні реалізації в напрямку технічних засобів охорони об'єктів тощо

Оцінка розрахункової частини *Відмінно*

Оцінка графічної частини *Відмінно*

Загальна оцінка *Відмінно*

Прізвище, ім'я, по батькові керівника дипломного проекту _____

Стайкуца Сергій Володимирович

Місце роботи і посада керівника дипломного проекту _____

"Державний університет інтелектуальних технологій і зв'язку",
доцент кафедри кібербезпеки та технічного захисту інформації,
помічник декана факультету інформаційних технологій та кібербезпеки

Підпис _____

«12» червня 2023 р.

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

РЕЦЕНЗІЯ

на дипломний проект (роботу) здобувача (здобувачки) освіти

відділення комп'ютерних систем

Осадчого Володимира Ігоровича

(прізвище, ім`я та по батькові)

Спеціальність 123 "Комп'ютерна інженерія"

Освітня програма «Обслуговування комп'ютерних систем і мереж»

Керівник дипломного проекту (роботи) Стайкуца Сергій Володимирович

(прізвище, ім`я та по батькові)

Тема дипломного проекту (роботи) Розробка backend-частини веб-сайту з дослідження напрямку безпеки України.

Обсяг розрахунково-пояснювальної записки 69 сторінок

Обсяг графічної (презентаційної) частини 12 аркушів (слайдів)

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ (РОБОТИ)

а) заключення про ступінь відповідності виконаного дипломного проекту (роботи) завданню

Представлений на рецензію дипломний проект повністю відповідає меті проектування та технічному завданню. Тематика дипломного проекту є актуальною та присвячена вибору оптимальних методів та засобів розробки сайту з боку серверної частини

б) характеристика виконання кожного розділу дипломного проекту (роботи)

Дипломний проект складається зі вступу, трьох розділів, висновків, переліку використаних джерел. У технологічному розділі виконано огляд і аналіз сучасного стану ринку безпеки України, розробка прототипу сайту з дослідження безпеки України

в) оцінка якості виконання пояснювальної записки та графічної частини дипломного проекту (роботи) Графічна частина виконана на достатньо високому рівні у вигляді презентації із використанням офісного пакету Microsoft PowerPoint та Visio. Пояснювальна записка виконана акуратно та у відповідності до норм оформлення документів із використанням офісного пакету Microsoft Word. Загальна якість виконання документації – добра, академічного плагіату у роботі не виявлено

г) перелік позитивних якостей дипломного проекту (роботи)

1. Детально розглянуто ринок безпеки України
2. Виконання рекомендацій для вибору мов програмування

д) основні недоліки дипломного проекту (роботи)

1. Розглянуто не всі способи роботи з сервером
2. При розгляді мови програмування треба було принести більше інформації

Оцінка розрахункової частини відмінно

Оцінка графічної частини відмінно

Загальна оцінка відмінно

Прізвище, ім'я, по батькові рецензента Кривченко Юрій Вікторович

Місце роботи і посада рецензента Одеський технічний фаховий коледж ОНТУ, голова ЦК КТ та ПІ

Підпис:

«16» червня 2023 р.

ДОЗВІЛ
НА РОЗМІЩЕННЯ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
В ЕЛЕКТРОННОМУ РЕПОЗИТАРІЇ ВСП «ОТФК ОНТУ»

Ми, що нижче підписалися,

Осадчий Володимир Ігорович
здобувач освіти гр. КС-56, та

Стайкуца Сергій Володимирович,
керівник дипломного проекту,

не заперечуємо щодо розміщення електронного варіанту пояснювальної записки до випускної кваліфікаційної роботи фахового молодшого бакалавра на тему:

«Розробка backend-частини веб-сайту з дослідження напрямку безпеки України» ***(автор роботи – Осадчий В.І., керівник роботи – Стайкуца С.В.)***

виконаного у ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету» в 2023 році, у повному обсязі в електронному репозитарії ВСП «ОТФК ОНТУ» для вільного доступу через мережу Інтернет.

Несемо відповідальність за ідентичність електронного та друкованого варіантів випускної кваліфікаційної роботи, і даємо згоду на обробку персональних даних.

Виконавець _____ / Осадчий В.І./

Керівник _____ / Стайкуца С.В./

«12» червня 2023 р.

UNICHECK

Ім'я користувача:
Наталія Вікторівна Копусь

ID перевірки:
1015563716

Дата перевірки:
12.06.2023 13:47:35 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
12.06.2023 13:56:22 EEST

ID користувача:
100011688

Назва документа: 4КС-56 Осадчий Володимир

Кількість сторінок: 70 Кількість слів: 10484 Кількість символів: 80547 Розмір файлу: 824.32 KB ID файлу: 1015215276

10.1%
Схожість

Найбільша схожість: 1.95% з Інтернет-джерелом (https://www.unian.ua/economics/finance/maliy-biznes-v-ukrajini-pove.

10.1% Джерела з Інтернету | 200 ..... Сторінка 72

Не знайдено джерел з Бібліотеки

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел