1. Projekt Secure File Cloud (SFC) ma na celu zapewnienie użytkownikom bezpiecznego i wygodnego miejsca do przechowywania swoich plików w formie chmury internetowej. Głównym celem systemu jest umożliwienie użytkownikom przechowywania, zarządzania i udostępniania plików w sposób bezpieczny oraz intuicyjny.

2. Wymagania:

    2.1. System Targeting:

    Grupą użytkowników systemu Secure File Cloud (SFC), są pracownicy firm, które wykupują usługę zapewnioną przez ten projekt. Ci pracownicy reprezentują różne działy i poziomy hierarchiczne w firmie, ale łączy ich potrzeba bezpiecznego przechowywania i zarządzania plikami online. Korzystając z SFC, mogą oni skutecznie przechowywać, udostępniać i zarządzać swoimi dokumentami oraz danymi firmowymi, czerpiąc korzyści z zapewnionej przez system wysokiej jakości ochrony danych.

    2.2. Opis SPIN (ang. Situation/Problem questions, Implied need/Needs pay off):

    Sytuacja:
    Wiele firm korzysta obecnie z tradycyjnych metod przechowywania danych, takich jak lokalne serwery lub zewnętrzne nośniki. Proces ten może być uciążliwy i niezabezpieczony, szczególnie w kontekście pracy zdalnej i potrzeby dostępu do danych z różnych lokalizacji.

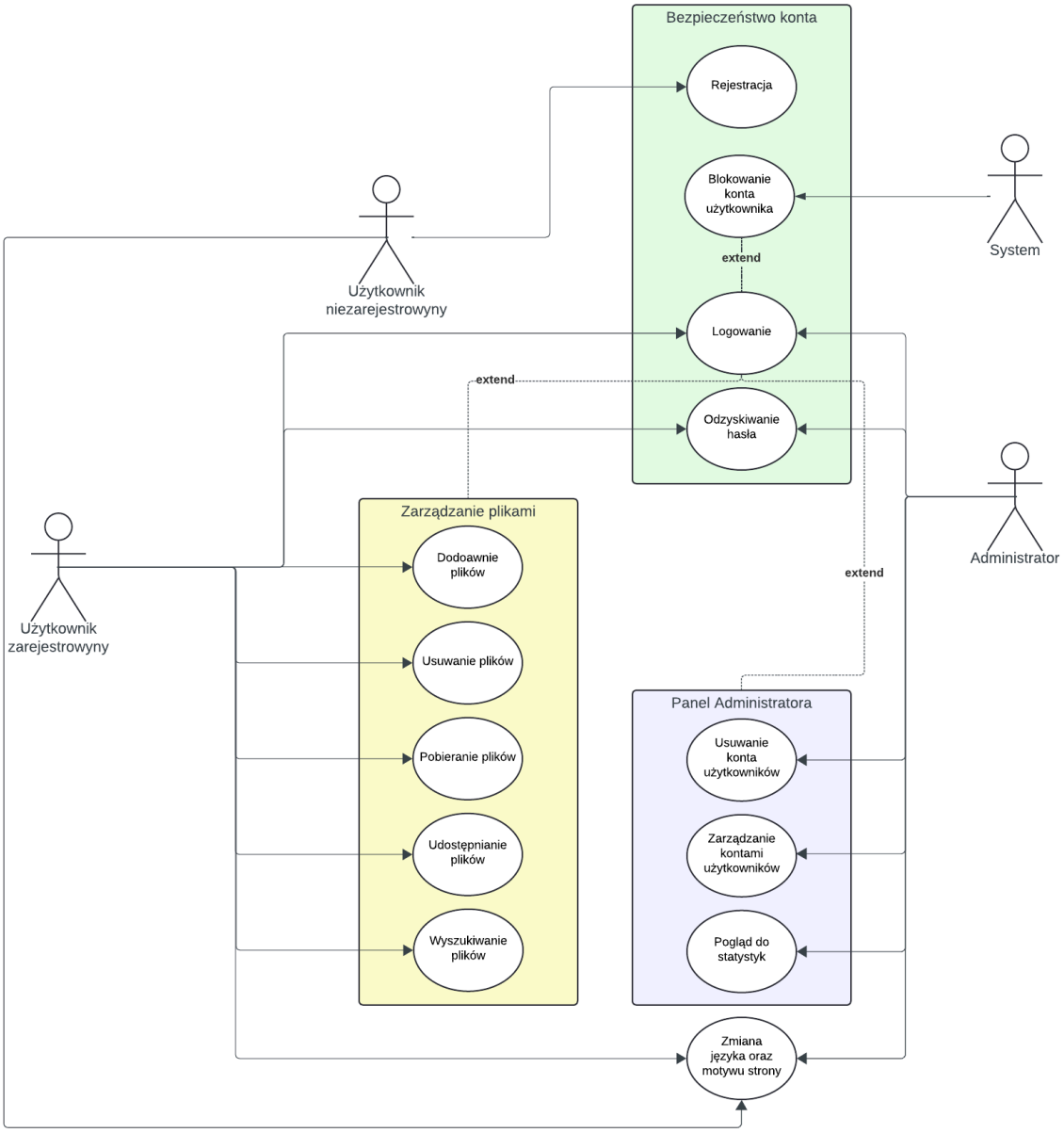
    Problem:
    Szereg problemów związanych z przechowywaniem i zarządzaniem plikami. Brak wygodnego dostępu do danych, ryzyko utraty danych w przypadku awarii sprzętu lub ataku cybernetycznego, oraz brak mechanizmów kontroli dostępu do poszczególnych plików to tylko niektóre z wyzwań, z którymi borykają się użytkownicy.

    Potrzeba:
    Na podstawie obecnych problemów, można wywnioskować, że firmy potrzebują bezpiecznego, łatwego w użyciu i niezawodnego rozwiązania do przechowywania oraz zarządzania swoimi danymi. Istotne jest zapewnienie bezpieczeństwa danych, wygody dostępu oraz kontroli nad udostępnianiem plików.

    Rozwiązanie:
    Zastosowanie Secure File Cloud (SFC) przyniesie firmie szereg korzyści. Dzięki SFC, firma będzie mogła bezpiecznie przechowywać swoje dane w chmurze, z gwarancją szyfrowania, co zapewni ochronę przed utratą danych. Dodatkowo, łatwy dostęp do danych z dowolnego miejsca i urządzenia oraz możliwość

udostępniania plików poprzez generowane linki zwiększy efektywność pracy zespołu. System oferuje także zaawansowane funkcje zarządzania kontami użytkowników, umożliwiając administratorom pełną kontrolę nad dostępem do danych. Dodatkowo, dostępność motywów jasnego i ciemnego oraz dwóch wersji językowych zwiększy komfort użytkowania dla wszystkich pracowników firmy.

3. Specyfikacja wymagań ERS I (ang. Engineering Requirement Specification, cz. 1):
   3.1. diagram użycia Use-Case Diagram



   3.2. tabele przypadków użycia Use-Case Templates

Nazwa przypadku użycia	Rejestracja
Aktorzy	Użytkownik niezarejestrowany
Opis	Użytkownik ma możliwość zarejestrowania się do systemu Secure File Cloud (SFC) w celu uzyskania dostępu do chmury plików.
Warunki początkowe	Użytkownik nie jest zarejestrowany.
Warunki końcowe	Użytkownik jest zarejestrowany do systemu.
Przebieg główny	1.Użytkownik wybiera opcję rejestracji. 2. Użytkownik wprowadza swoje dane rejestracyjne. 3. System weryfikuje dane. 4. Jeśli dane są poprawne, użytkownik zostaje zarejestrowany do systemu.
Rozszerzenia	W przypadku niepoprawnych danych, system wyświetla odpowiedni komunikat błędu.

Nazwa przypadku użycia	Logowanie
Aktorzy	Użytkownik zarejestrowany
Opis	Użytkownik ma możliwość zalogowania się do systemu Secure File Cloud (SFC) w celu uzyskania dostępu do swojej chmury plików.
Warunki początkowe	Użytkownik nie jest zalogowany ale jest zarejestrowany w systemie.
Warunki końcowe	Użytkownik jest zalogowany do systemu.

Przebieg główny	1. Użytkownik wybiera opcję logowania. 2. Użytkownik wprowadza swoje dane logowania. 3. System weryfikuje dane. 4. Jeśli dane są poprawne, użytkownik zostaje zalogowany do systemu.
Rozszerzenia	W przypadku niepoprawnych danych, system wyświetla odpowiedni komunikat błędu.

Nazwa przypadku użycia	Zarządzanie plikami
Aktorzy	Użytkownik zarejestrowany
Opis	Użytkownik ma możliwość dodawania, usuwania, pobierania i zarządzania plikami w swojej chmurze Secure File Cloud (SFC).
Warunki początkowe	Użytkownik jest zalogowany do systemu.
Warunki końcowe	Zmiany w plikach użytkownika są zapisane.
Przebieg główny	1. Użytkownik wybiera opcję zarządzania plikami. 2. Użytkownik dodaje, usuwa lub pobiera pliki. 3. System zapisuje zmiany w plikach użytkownika.
Rozszerzenia	W przypadku problemów z operacją na plikach, system wyświetla odpowiedni komunikat błędu.

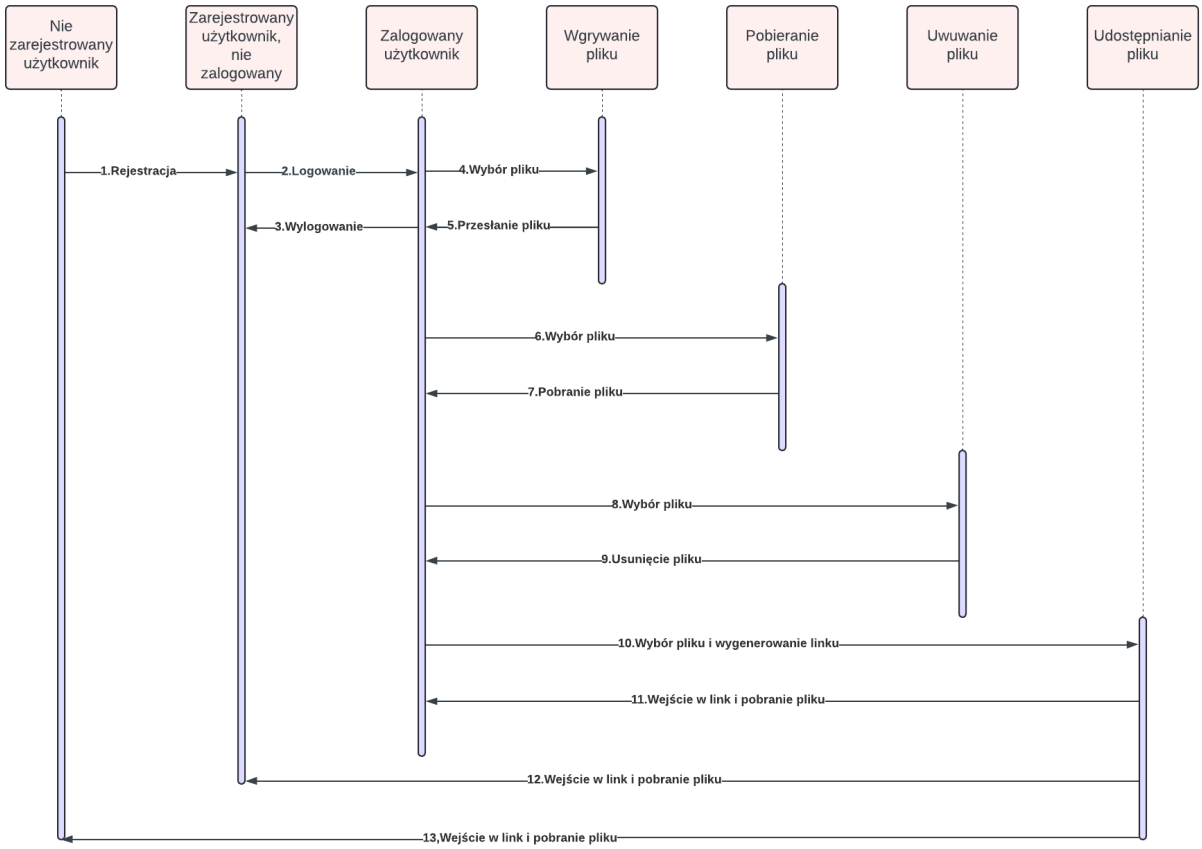
Nazwa przypadku użycia	Udostępnianie plików
Aktorzy	Użytkownik zarejestrowany
Opis	Użytkownik ma możliwość generowania linków udostępniających pliki z chmury Secure File Cloud (SFC), aby inni użytkownicy mogli je pobrać.

Warunki początkowe	Użytkownik jest zalogowany do systemu.
Warunki końcowe	Link udostępniający plik jest wygenerowany i dostępny dla użytkownika.
Przebieg główny	1. Użytkownik wybiera plik, który chce udostępnić. 2. Użytkownik generuje link udostępniający dla wybranego pliku. 3. System generuje unikalny link i udostępnia go użytkownikowi.
Rozszerzenia	W przypadku problemów z generowaniem linku, system wyświetla odpowiedni komunikat błędu.

Nazwa przypadku użycia	Zarządzanie kontami użytkowników przez administratora
Aktorzy	Administrator
Opis	Administrator ma możliwość zarządzania kontami użytkowników w systemie Secure File Cloud (SFC), usuwania istniejących, zmiany przyznanej powierzchni dyskowej itp.
Warunki początkowe	Administrator jest zalogowany do systemu.
Warunki końcowe	Zmiany w kontach użytkowników są zapisane.
Przebieg główny	1. Administrator przechodzi do panelu administracyjnego systemu. 2. Administrator wybiera opcję zarządzania kontami użytkowników. 3. Administrator usuwa lub modyfikuje konta użytkowników, zmieniając ich dostępną wielkość dyskową. 4. System zapisuje zmiany w kontach użytkowników.
Rozszerzenia	W przypadku problemów z operacją na kontach użytkowników, system wyświetla odpowiedni komunikat błędu.

Nazwa przypadku użycia	Blokowanie konta użytkownika po trzykrotnym błędnym wpisaniu hasła
Aktorzy	System
Opis	System zablokuje konto użytkownika na pewien czas jeżeli użytkownik trzykronie podczas próby logowanie wpisze błędne dane logowania.
Warunki początkowe	Użytkownik wprowadza złe dane
Warunki końcowe	Użytkownik zablokowany
Przebieg główny	1. Użytkownik próbuje się zalogować 2.Użytkownik trzykrotnie wprowadza błędne dane logowania 3. Konto użytkownika zostaje zablokowane na 20 min 4. Po upływie 20 min system odblokowuje konto użytkownika
Rozszerzenia	System odblokuje konto użytkownika po 20 min

3.3. Diagram przepływu sterowania Control-Flow Diagram (Sequence Diagram) wraz z opisem



Opis każdego z punktów:

1. Niezarejestrowany użytkownik wybiera opcję rejestracji do systemu. Wypełnia dane i pomyślnie przechodzi proces rejestracji.
2. Zarejestrowany użytkownik wybiera opcję logowania do systemu. Wypełnia dane logowania i pomyślnie przechodzi proces logowania.
3. Zalogowany użytkownik wybiera opcję “Wyloguj” i wylogowuje się z systemu.
4. Zalogowany użytkownik wybiera opcję “Wybierz plik” i wybiera odpowiedni plik.
5. Użytkownik używa opcji “Prześlij plik” i przesyła wcześniej wybrany plik do chmury.
6. Zalogowany użytkownik wybiera plik który chce pobrać z listy plików.
7. Użytkownik używa opcji “Pobierz” przy wybrany wcześniej pliku i pobiera wybrany plik z chmury na swoje urządzenie.
8. Zalogowany użytkownik wybiera plik który chce usunąć z listy plików.
9. Użytkownik używa opcji “Usuń” przy wybrany wcześniej pliku i usuwa wybrany plik z chmury.
10. Zalogowany użytkownik wybiera plik który chce udostępnić z listy plików. Używa opcji “Udostępnij” przy wybrany wcześniej pliku i potem ma opcję “Kopiuj link” i “Przestań udostępniać”. Opcja “Kopiuj link” spowoduje skopiowanie linku udostępniającego plik do schowka. Opcja “Przestań udostępniać” spowoduje unieważnienie wygenerowanego linku udostępniania.

11. Użytkownik przesyła link do innego zalogowanego użytkownika u którego po aktywacji linku pobierze się plik
12. Użytkownik przesyła link do innego zarejestrowanego użytkownika u którego po aktywacji linku pobierze się plik
13. Użytkownik przesyła link do innego niezarejestrowanego użytkownika u którego po aktywacji linku pobierze się plik

3.4. Systematyzacja usług i/lub funkcji w kategorii od najważniejszych do nieistotnych np. typu MOSCOW (Must/Should/Could/Won't Have),

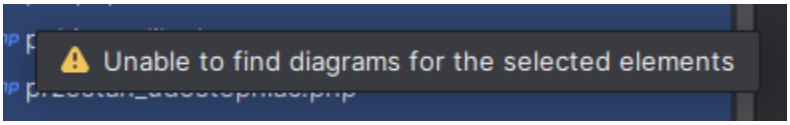
Must (Muszą być):
1. Logowanie/Rejestracja
2. Zapewnienie bezpieczeństwa przechowywanych danych
3. Dodawanie, usuwanie, pobieranie plików
4. Udostępnianie plików przez link
5. Zarządzanie kontami użytkowników przez administratora

Should (Powinny być):
1. Odzyskiwanie hasła
2. Tymczasowe blokowanie dostępu do konta przy paru błędnych próbach logowania
3. Wyszukiwarka plików

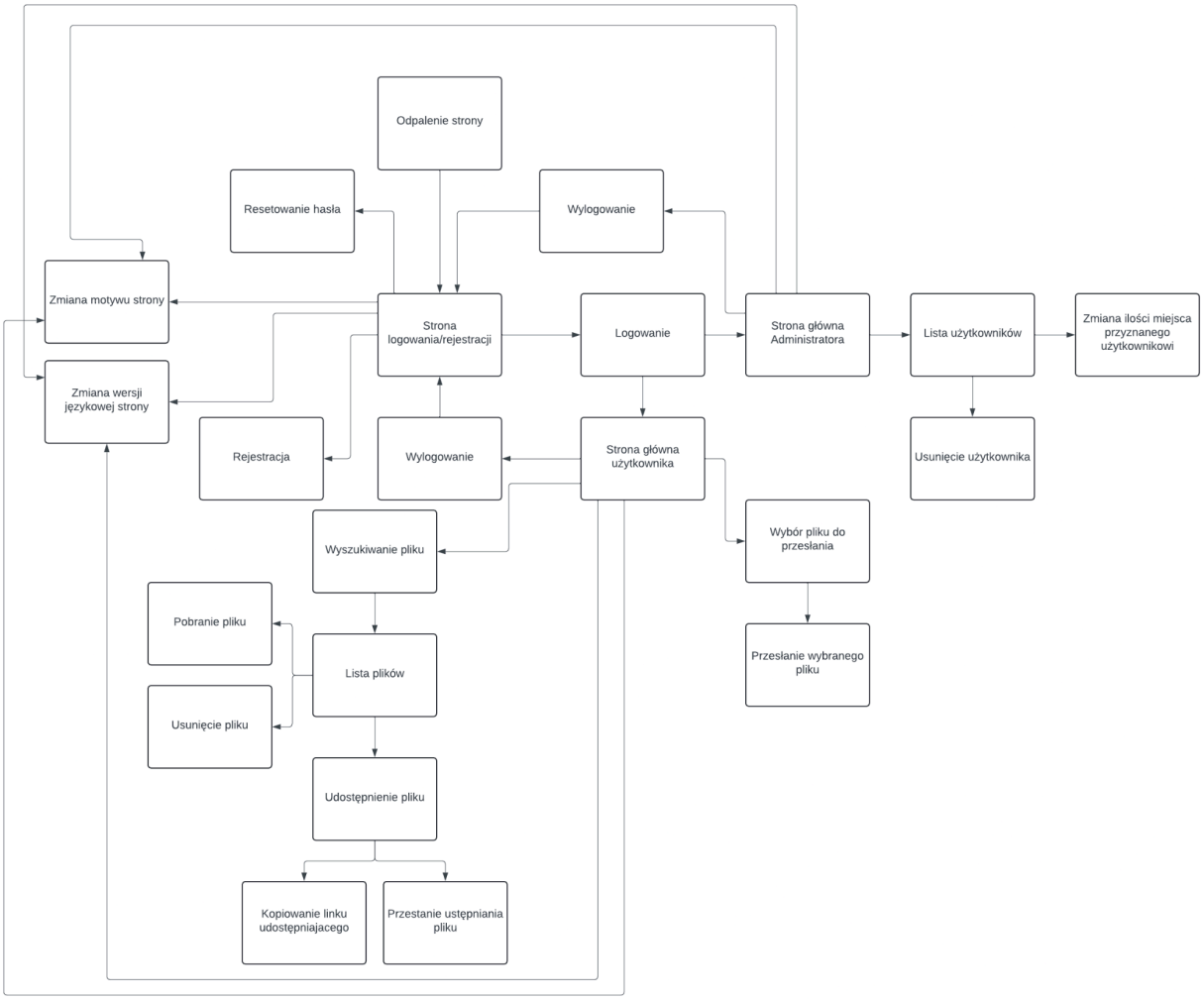
Could (Mogą być):
1. Zarządzanie kontem przez użytkownika
2. Motyw jasny/ciemny
3. Dwujęzyczność (wersje polska i ukraińska)

Won't Have (Nie będą miały):
1. Integracja z innymi aplikacjami
2. Zaawansowane funkcje edycji plików

3.5. Diagram obiektów.
Z powodu wyglądu struktury plików i tego co jest w środku nie można wygenerować diagramu. Programy do generowania też nie są w stanie sobie poradzić:



3.6. Diagram funkcjonalny/strukturalny wraz z opisem.



1.Strona logowania/rejestracji: Początkowy punkt dla użytkowników, gdzie mogą się zalogować lub zarejestrować.

-Logowanie: Umożliwia użytkownikom dostęp do ich kont.

-Rejestracja: Umożliwia nowym użytkownikom utworzenie konta.

-Resetowanie hasła: Opcja dla użytkowników, którzy zapomnieli hasło.

2.Strona główna użytkownika: Po zalogowaniu użytkownicy są przenoszeni na stronę główną, która służy jako punkt startowy dla różnych funkcji.

-Wyszukiwanie plików: Umożliwia użytkownikom wyszukiwanie plików.

-Lista plików: Wyświetla pliki użytkownika znajdujące się na serwerze.

-Pobieranie pliku: Opcja pobierania wybranego pliku.

-Usuwanie pliku: Opcja usunięcia plików z listy.

-Udostępnianie pliku: Opcja udostępniania plików innym użytkownikom.

-Kopiowanie linku udostępnionego pliku: Skopiowanie linku pliku udostępnionego innym.

-Zaprzestanie udostępniania pliku: Możliwość zakończenia udostępniania pliku poprzez dezaktywację linku.

-Wybór pliku do przesłania: Możliwość wyboru pliku do uploadu.

-Przesłanie wybranego pliku: Wysłanie pliku na serwer.

3.Strona główna administratora: Specjalna strona dla użytkowników z uprawnieniami administracyjnymi.

-Lista użytkowników: Wyświetla listę wszystkich użytkowników systemu.

-Usunięcie użytkownika: Opcja usunięcia użytkownika z systemu.

-Zmiana ilości miejsca przyznanego użytkownikowi: Możliwość zmiany limitu przestrzeni dyskowej dostępnej dla użytkownika.

4.Zmiana motywu strony: Opcja zmiany motywu graficznego strony.

5.Zmiana wersji językowej strony: Opcja zmiany języka interfejsu użytkownika.

4. Specyfikacja wymagań ERS II (architektura/harmonogramowanie, cz. 2):

4.1. architektura Systemu SAAM (ang. Software Architecture Analysis Model)

1. Widok modułów:

- Interfejs użytkownika (UI):

  - Odpowiada za prezentację interfejsu użytkownika.

  - Składa się z widoków logowania, rejestracji, przeglądania plików, zarządzania kontami, etc.

- Logika biznesowa:

  - Odpowiada za przetwarzanie danych i logikę aplikacji.

  - Zarządza operacjami takimi jak logowanie, rejestracja, zmiana hasła, dodawanie, usuwanie, udostępnianie i wyszukiwanie plików.

- Warstwa dostępu do danych:

  - Odpowiada za komunikację z bazą danych.

  - Zapewnia dostęp do danych użytkowników, plików itp.

2. Widok komponentów:

- Klient (Client):

  - Interfejs użytkownika (UI).

- Serwer (Server):

  - Logika biznesowa.

- Warstwa dostępu do danych.

3. Widok danych:

- Użytkownik (User):

  - Przechowuje informacje o użytkownikach, takie jak identyfikator, hasło, adres e-mail, rola, przestrzeń dyskowa.

- Plik (File):

  - Przechowuje informacje o plikach, takie jak identyfikator, nazwa, rozmiar, typ, właściciel, data dodania, link dostępu.

4. Widok bezpieczeństwa:

- Autoryzacja i uwierzytelnienie:

  - Weryfikacja tożsamości użytkownika podczas logowania.

  - Kontrola dostępu do operacji na plikach.

- Szyfrowanie danych:

  - Zabezpieczenie przechowywanych danych użytkowników i plików za pomocą odpowiednich mechanizmów szyfrowania.

5. Widok wydajności:

- Optymalizacja operacji na plikach:

  - Zapewnienie szybkiego dostępu do plików i wydajnych operacji takich jak dodawanie, usuwanie i pobieranie.

- Skalowalność:

  - Możliwość skalowania aplikacji w razie wzrostu liczby użytkowników.

6. Widok architektury fizycznej:

- Aplikacja internetowa:

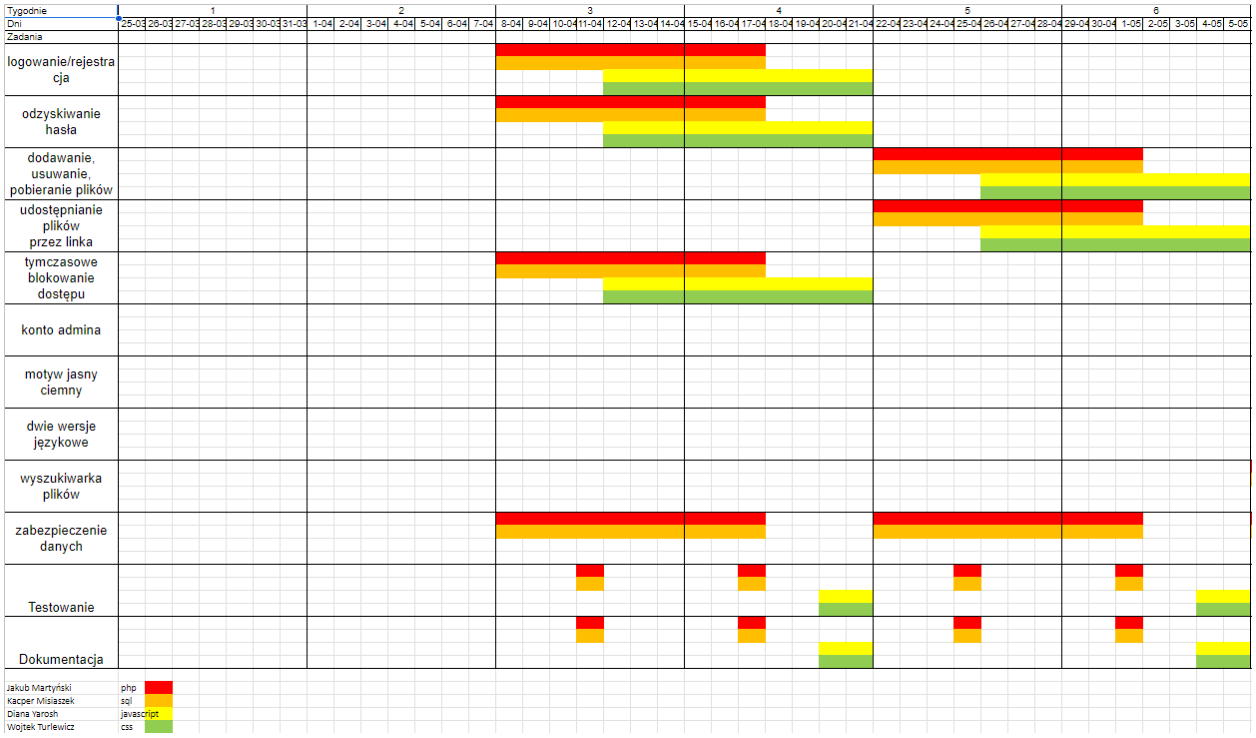
  - Działa na serwerze internetowym.

  - Wykorzystuje bazę danych do przechowywania danych.

- Baza danych:

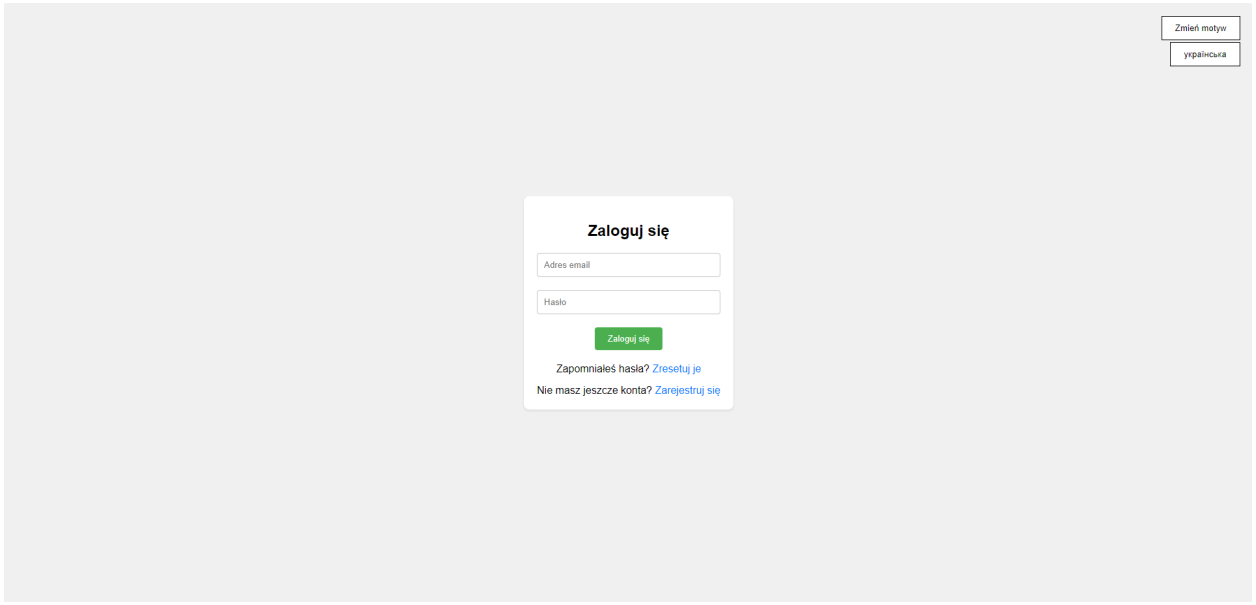
- Przechowuje dane użytkowników, plików i innych informacji związanych z aplikacją.

4.2. harmonogram projektu (Diagram Gantta lub Person-Power-Matrix lub CPM (Critical Path Method)) uwzględniający tzw. Deliverables i milestones,

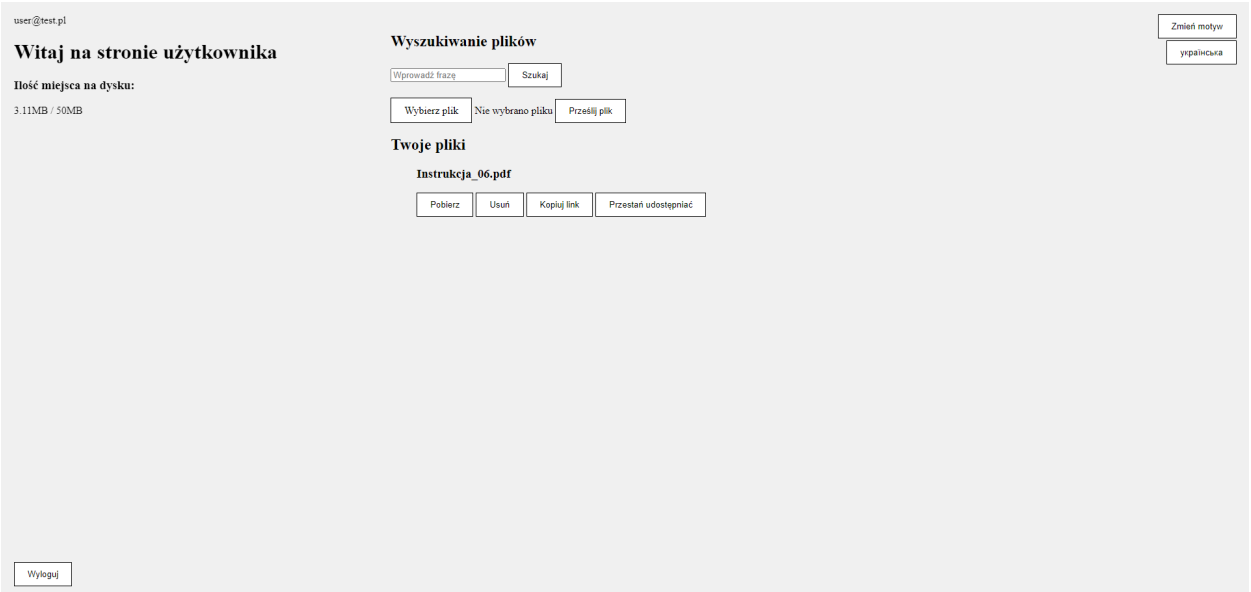


4.3. Projekt Interfejsu (programowego/sieciowego lub użytkownika)

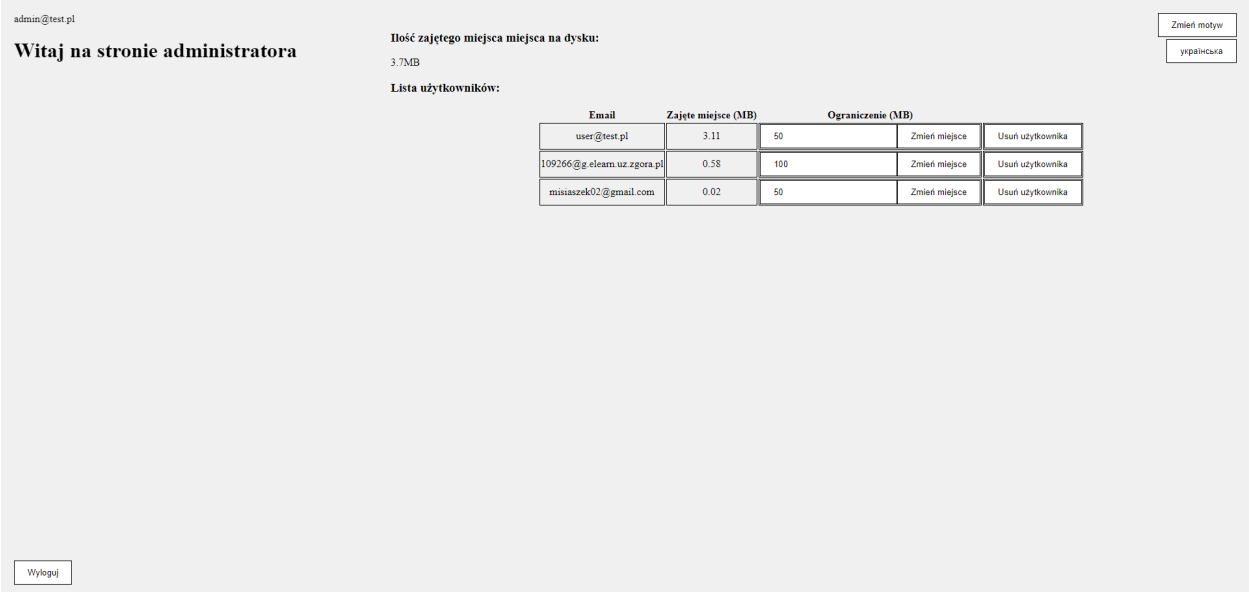
4.3.1. Strona logowania/rejestrowania



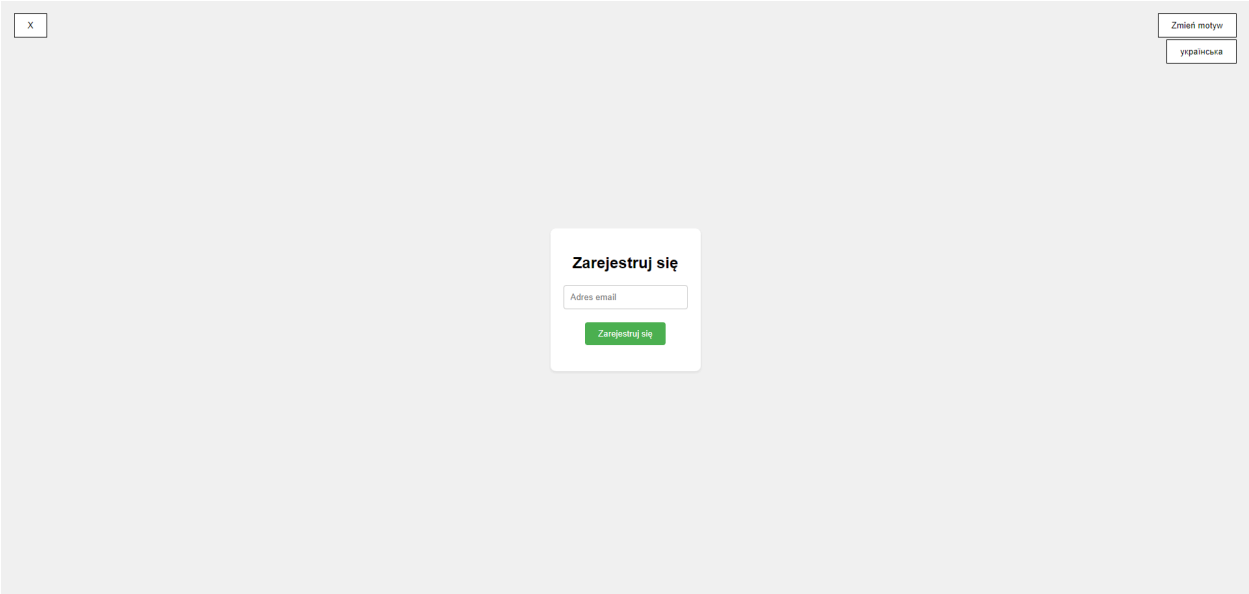
4.3.2. Strona główna użytkownika



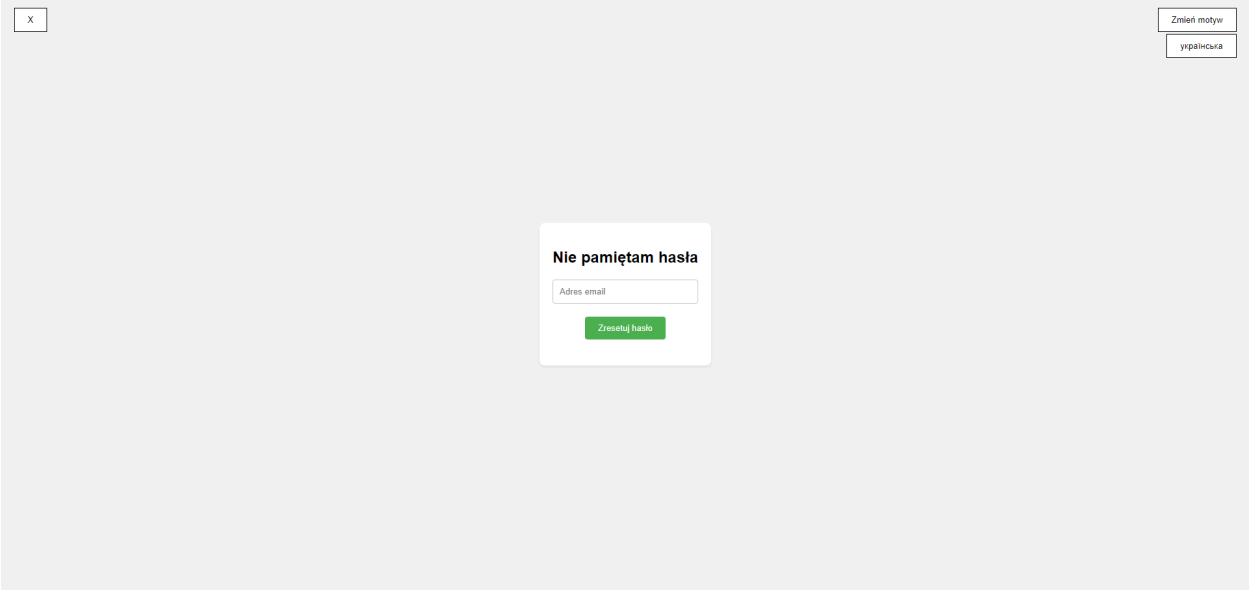
4.3.3. Strona główna administratora



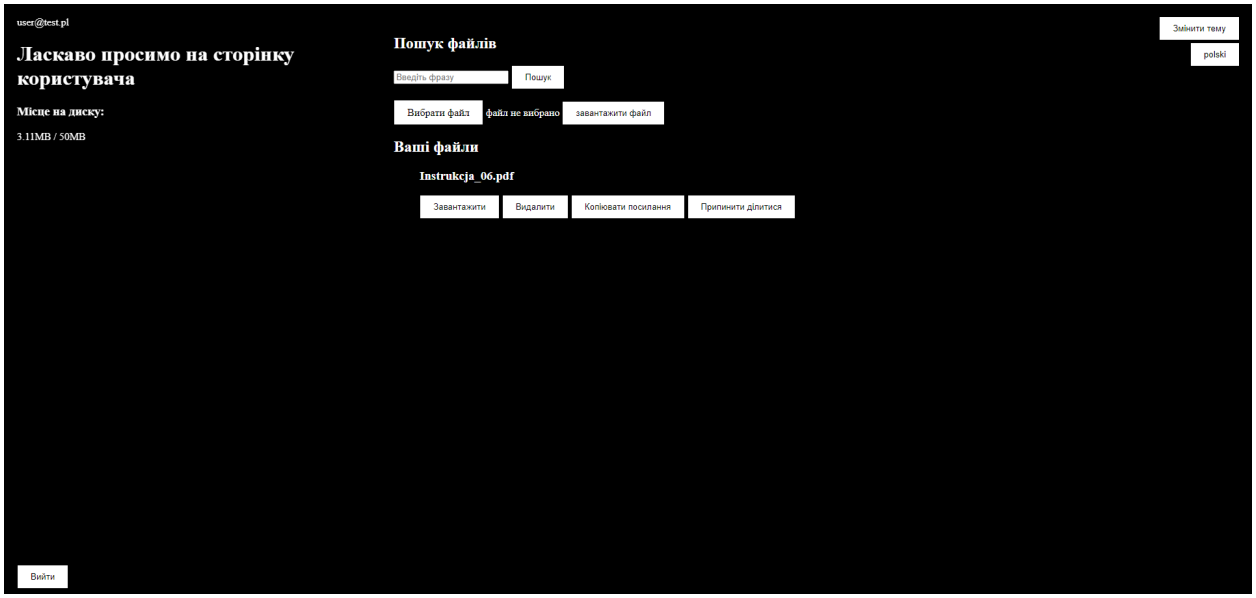
4.3.4. Strona rejestracji



4.3.5. Strona odzyskiwania hasła



4.3.6. Strona z ciemnym motywem i drugą wersją językową



5. Specyfikacja wymagań ERS III (plany zarządzania)
   5.1. plan kosztów (koszty pracy, koszty wspólne, koszty sprzętu, koszty amortyzacji)

Zarobki pracowników:			
Jakub Martyński	45.00 zł	/h	7,200.00 zł
Kacper Misiaszek	35.00 zł	/h	5,600.00 zł
Diana Yarosh	35.00 zł	/h	5,600.00 zł
Wojciech turlewicz	35.00 zł	/h	5,600.00 zł
Koszta oprogramowania:			
domena	72.56 zł	/rok	
oprogramowanie	300.00 zł	/miesiecznie	
Koszta sprzętowe:			
serwer	8,000.00 zł	/jednorazowe	
awaria sprzętu:	8,000.00 zł	/jednorazowe	
Koszta firmowe:			
konto bankowe	200.00 zł	/miesiecznie	
porady prawne	1,000.00 zł	/miesiecznie	
księgowość	1,000.00 zł	/miesiecznie	
utrzymanie czystości	800.00 zł	/miesiecznie	
wynajem biura	5,000.00 zł	/miesiecznie	
integracje zespołowe	1,500.00 zł	/3 miesiace	
szkolenia	8,000.00 zł	/3 miesiace	
premie	2,000.00 zł	/miesiecznie	
elektryczność	1,000.00 zł	/miesiecznie	
marketing	2,000.00 zł	/miesiecznie	
ubezpieczenie	800.00 zł	/miesiecznie	
leasing	2,000.00 zł	/miesiecznie	
dodatkowy support	3,000.00 zł	/miesiecznie	

Koszta za jeden miesiąc działalności:	46,272.71 zł
Koszta jednorazowe:	16,000.00 zł
marża	20.00%
Koszt za projekt(4 miesiące):	241,309.02 zł

5.2. plan jakości - metryka systemu (opisujący standardy jakie spełni system)

1. Bezpieczeństwo danych:
   - Wszystkie dane użytkowników przechowywane będą w sposób zaszyfrowany, zapewniając prywatność i ochronę przed nieautoryzowanym dostępem.
   - System będzie implementować silne mechanizmy uwierzytelniania i autoryzacji, zapewniając, że jedynie uprawnieni użytkownicy będą mieli dostęp do odpowiednich funkcji i danych.
2. Wydajność:
   - System będzie zaprojektowany tak, aby zapewnić szybką odpowiedź na żądania użytkowników, szczególnie w operacjach związanych z przesyłaniem i przetwarzaniem plików.

- Optymalizacja bazy danych oraz algorytmów operacji na plikach pozwoli na szybkie wykonywanie zadań, nawet przy dużej liczbie użytkowników.

3. Dostępność:
   - System będzie działać 24/7, zapewniając dostępność dla użytkowników o różnych porach dnia i nocy.
   - Planowane prace konserwacyjne będą planowane na godziny o niskim obciążeniu systemu, aby minimalizować zakłócenia w dostępie.
4. Testy i kontrola jakości:
   - Przed wdrożeniem systemu zostaną przeprowadzone szczegółowe testy jednostkowe, integracyjne i systemowe, aby zapewnić, że wszystkie funkcje działają zgodnie z oczekiwaniami.
   - Regularne audyty i monitorowanie systemu będą przeprowadzane w celu zapewnienia ciągłości działania oraz wykrywania i usuwania ewentualnych błędów.
5. Obsługa klienta:
   - System będzie zawierał moduł obsługi klienta, umożliwiający użytkownikom zgłaszanie problemów i proponowanie ulepszeń.
   - Zespół wsparcia technicznego będzie reagować na zgłoszenia użytkowników w sposób szybki i skuteczny, dbając o zadowolenie klientów.
6. Elastyczność i skalowalność:
   - Architektura systemu będzie elastyczna i skalowalna, umożliwiając dostosowanie się do zmieniających się potrzeb i wzrostu liczby użytkowników.
   - Będzie istnieć plan na przyszłość dotyczący rozwoju systemu, uwzględniający rosnące wymagania i nowe technologie.
7. Interfejs użytkownika:
   - Interfejs użytkownika będzie intuicyjny i łatwy w obsłudze, zapewniając przyjemne doświadczenie użytkownika podczas korzystania z systemu.
   - System będzie responsywny i dostosowany do różnych urządzeń i rozdzielczości ekranów, zapewniając spójność i funkcjonalność na wszystkich platformach.

5.3. plan testów/ewaluacji analiza ryzyka (ang. Risk Analysis) technologicznego/ekonomicznego

Plan testów/ewaluacji:

1. Testy jednostkowe:
   - Testy jednostkowe zostaną przeprowadzone dla każdej funkcji oddzielnie, sprawdzając poprawność działania poszczególnych modułów systemu.

2. Testy integracyjne:
   - Po zakończeniu testów jednostkowych zostaną przeprowadzone testy integracyjne, aby sprawdzić, czy poszczególne komponenty systemu współpracują ze sobą poprawnie.
3. Testy funkcjonalne:
   - Testy funkcjonalne będą skupiały się na weryfikacji zgodności z wymaganiami funkcjonalnymi systemu, takimi jak logowanie, dodawanie plików, udostępnianie plików itp.
4. Testy wydajnościowe:
   - Testy wydajnościowe zostaną przeprowadzone, aby ocenić, jak system zachowuje się podczas obciążenia, takiego jak równoczesne przesyłanie wielu plików lub dostęp do systemu przez dużą liczbę użytkowników.
5. Testy bezpieczeństwa:
   - Testy bezpieczeństwa zostaną przeprowadzone w celu sprawdzenia, czy system jest odporny na ataki typu SQL Injection.
6. Testy interfejsu użytkownika:
   - Testy interfejsu użytkownika będą oceniały czy interfejs jest intuicyjny i łatwy w obsłudze, a także czy działa poprawnie na różnych urządzeniach i przeglądarkach.

Analiza ryzyka technologicznego/ekonomicznego:

1. Ryzyko utraty danych:
   - Możliwe zagrożenie: Awaria systemu lub bazy danych może spowodować utratę danych użytkowników.
   - Plan działania: Regularne kopie zapasowe danych oraz monitorowanie systemu w celu szybkiego wykrycia i naprawy ewentualnych usterek.
2. Ryzyko naruszenia bezpieczeństwa:
   - Możliwe zagrożenie: Atak hakerski może narazić dane użytkowników na kradzież lub manipulację.
   - Plan działania: Wdrożenie silnych mechanizmów uwierzytelniania, szyfrowania danych oraz regularne aktualizacje oprogramowania w celu zapewnienia ochrony przed atakami.
3. Ryzyko zmiany warunków rynkowych:
   - Możliwe zagrożenie: Zmiany na rynku mogą wymagać dostosowania systemu do nowych wymagań lub trendów.
   - Plan działania: Monitorowanie trendów rynkowych oraz elastyczne podejście do rozwoju systemu, umożliwiające szybką reakcję na zmiany.
4. Ryzyko problemów z zasobami finansowymi:
   - Możliwe zagrożenie: Brak wystarczających zasobów finansowych może ograniczyć możliwości rozwoju i utrzymania systemu.

- Plan działania: Staranne planowanie budżetu, ocena kosztów operacyjnych oraz poszukiwanie alternatywnych źródeł finansowania w razie potrzeby.

5.4. Plan bezpieczeństwa (jakie metody ochrony zasobów i danych będą użyte)

1. Szyfrowanie danych:

Wszystkie dane przechowywane w systemie będą szyfrowane, w tym hasła użytkowników, dane plików oraz wszelkie inne informacje poufne. Szyfrowanie będzie wykonywane z użyciem silnych algorytmów kryptograficznych.

2. Mechanizmy uwierzytelniania:

System będzie wykorzystywał różnorodne mechanizmy uwierzytelniania, takie jak hasła, potwierdzanie dwuetapowe.

3. Autoryzacja i kontrola dostępu:

Autoryzacja będzie kontrolować dostęp do różnych funkcji systemu na podstawie ról użytkowników oraz ich uprawnień. Administrator będzie miał możliwość zarządzania uprawnieniami użytkowników.

4. Regularne kopie zapasowe:

System będzie regularnie tworzył kopie zapasowe danych, aby zapewnić możliwość ich szybkiego przywrócenia w przypadku awarii systemu lub utraty danych.

5. Monitorowanie i logowanie:

System będzie monitorowany pod kątem nieprawidłowości i ataków. Wszelkie działania w systemie będą rejestrowane w dziennikach zdarzeń w celu możliwości audytu oraz wykrywania nieautoryzowanych aktywności.

6. Ochrona przed atakami:

System będzie wyposażony w mechanizmy ochrony przed atakami, takie jak filtracja zapytań, zapobieganie atakom typu SQL Injection oraz atakiom brute force na hasła.

7. Aktualizacje oprogramowania:

Regularne aktualizacje oprogramowania będą przeprowadzane, aby zapewnić, że system jest zabezpieczony przed znanymi lukami i zagrożeniami.

8. Zarządzanie incydentami:

W przypadku wykrycia incydentów bezpieczeństwa, system będzie miał wdrożone procedury reagowania, w tym szybkiej reakcji, analizy incydentów oraz powiadomienia odpowiednich organów i użytkowników.

5.5. Plan konserwacji/warunki licencji (na podstawie licencji GPL)

Plan konserwacji:

1. Regularne aktualizacje:

System będzie regularnie aktualizowany w celu wprowadzenia nowych funkcji, poprawek błędów oraz zapewnienia zgodności z najnowszymi standardami bezpieczeństwa.

2. Wsparcie techniczne:

Dla użytkowników systemu będzie udostępnione wsparcie techniczne w zakresie rozwiązywania problemów, udzielania odpowiedzi na pytania oraz świadczenia pomocy w zakresie konfiguracji i użycia systemu.

3. Naprawa błędów krytycznych:

W przypadku wykrycia błędów krytycznych lub luk w zabezpieczeniach, odpowiednie działania będą podjęte w celu szybkiego ich naprawienia i wydania aktualizacji systemu.

4. Dostosowywanie do zmian:

System będzie dostosowywany do zmieniających się potrzeb i wymagań użytkowników oraz ewoluującej technologii, aby zapewnić jego aktualność i przydatność w dłuższej perspektywie czasowej.

Warunki licencji (na podstawie licencji GPL):

1. Wolność użytkowników:

Użytkownicy będą mieli prawo do swobodnego korzystania z systemu, jego modyfikowania oraz redystrybucji, z zachowaniem odpowiednich zapisów licencyjnych.

2. Otwarty kod źródłowy:

Kod źródłowy systemu będzie dostępny publicznie, umożliwiając każdemu jego przeglądanie, analizę oraz modyfikację zgodnie z warunkami licencji.

3. Utrzymanie licencji:

Wszelkie modyfikacje systemu oraz jego pochodne będą również objęte licencją GPL, co zapewni kontynuację zasady otwartości i wolności oprogramowania.

4. Brak odpowiedzialności:

Twórcy systemu nie ponoszą odpowiedzialności za ewentualne szkody lub straty wynikające z korzystania z systemu, zgodnie z zapisami licencji GPL.

5. Warunki dystrybucji:

Każdy, kto przekazuje kopię systemu lub jego modyfikacji dalej, musi zapewnić również kopię licencji GPL oraz udostępnić kod źródłowy na żądanie.