

Analiza zagrożeń i ryzyka

1. Bezpieczeństwo danych: Tworzenie systemu do oceny kierunków i uczelni wymaga gromadzenia dużej ilości danych osobowych użytkowników, takich jak informacje dotyczące maila, opinie i dane osobowe. Istnieje ryzyko naruszenia prywatności tych danych, jeśli odpowiednie środki bezpieczeństwa nie zostaną wdrożone. Należy dbać o zabezpieczenie danych poprzez stosowanie odpowiednich protokołów szyfrowania, uwierzytelnianie dwuskładnikowe oraz regularne audyty bezpieczeństwa.

2. Weryfikacja USOS: Korzystanie z weryfikacji USOS, czyli systemu służącego do uwierzytelniania użytkowników za pomocą danych z systemu USOS, może wprowadzić ryzyko, że wystąpią problemy techniczne lub opóźnienia w procesie weryfikacji. W przypadku awarii systemu USOS lub zmian w jego działaniu, funkcjonalność systemu oceny kierunków i uczelni może być zakłócona lub uniemożliwiona. W takiej sytuacji konieczne jest monitorowanie i aktualizacja integracji z systemem USOS, aby zapewnić niezawodność działania.

3. Nieprawdziwe opinie i manipulacje: Dopuszczenie użytkowników do dodawania opinii na temat kierunków i uczelni niesie ryzyko pojawienia się nieprawdziwych opinii lub manipulacji. Może to prowadzić do dezinformacji innych użytkowników i wpłynąć na wiarygodność systemu. Należy wprowadzić środki mające na celu weryfikację i moderację opinii, takie jak weryfikacja kont użytkowników, filtrowanie treści lub raportowanie nieodpowiednich treści.

4. Nieaktualne informacje: System oceny kierunków i uczelni powinien dostarczać aktualne i dokładne informacje. Istnieje ryzyko, że dane takie jak plany studiów, programy nauczania, czy profile uczelni mogą ulec zmianie. Konieczne jest utrzymanie bieżąco aktualizowanych danych i monitorowanie ich dokładności. Można to osiągnąć poprzez regularne synchronizacje z oficjalnymi źródłami danych i wprowadzanie mechanizmów sprawdzających poprawność informacji (nie wszystkie uczelnie posiadają USOSa).

5. Utrzymanie i skalowalność: Jeśli system zyska popularność i dużą liczbę użytkowników, konieczne będzie zapewnienie odpowiedniej wydajności, skalowalności i utrzymania. W przypadku wzrostu obciążenia systemu może pojawić się ryzyko spowolnienia działania lub awarii. Należy monitorować wydajność systemu, optymalizować kod i infrastrukturę serwera, a także regularnie skalować zasoby, aby sprostać rosnącym wymaganiom.

