**WOJSKOWA AKADEMIA TECHNICZNA**

**im. Jarosława Dąbrowskiego**

#### WYDZIAŁ CYBERNETYKI



Dokumentacja organizacji projektu

Projekt PSBI 2022/2023

Autorzy:

Grupa: WCY21IH1S4 + WCY21IM1S4

**Warszawa 2022**

Spis treści

[Skład zespołu projektowego 4](#_Toc124202874)

[Szablon dokumentacyjny 6](#_Toc124202875)

[Organizacja repozytorium projektowego 7](#_Toc124202876)

[**3.1.** **Realizacja** 7](#_Toc124202877)

[**3.2.** **Podział i uprawnienia** 7](#_Toc124202878)

[**3.3.** **Bezpieczeństwo** 10](#_Toc124202879)

[**3.4.** **Wersjonowanie** 10](#_Toc124202880)

[**3.5.** **Kopie bezpieczeństwa** 10](#_Toc124202881)

[Harmonogram prac projektowych 12](#_Toc124202882)

[**Tabelaryczny harmonogram prac projektowych** 13](#_Toc124202883)

[Project Quality Plan 14](#_Toc124202884)

[**5.1 Sposoby oceniania jakości** 14](#_Toc124202885)

[**5.2 Rodzaje prowadzonych kontroli i przeglądów realizacji przedsięwzięcia** 14](#_Toc124202886)

[**5.3 Normy stosowane podczas realizacji przedsięwzięcia** 15](#_Toc124202887)

[**5.4 Sposoby rozstrzygania sporów zleceniodawca-wykonawca** 16](#_Toc124202888)

[**5.5 Procedury wyszukiwania i zgłaszania błędów** 16](#_Toc124202889)

[**5.6 Dokumenty przygotowywane przez kontrolera jakości** 16](#_Toc124202890)

[**5.7 Informacje przekazywane zespołowi wytwórczemu** 17](#_Toc124202891)

[Wzorzec konstrukcyjny 18](#_Toc124202892)

[Identyfikacja ograniczeń 22](#_Toc124202893)

[Dokumenty robocze i wzorce 23](#_Toc124202894)

Wstęp

Niniejszy dokument stanowi opis zespołu projektowego realizującego przedsięwzięcie projektu modernizacji systemu bezpieczeństwa informacji. Każdy zespół i rola ma ściśle przydzielone zadania w ramach projektu. Dokumenty powstałe w ramach projektu będą wytwarzane w oparciu o spójny szablon (papier firmowy), którego wzór znajduje się w załączniku do dokumentu.

Dokument zawiera również informacje o repozytorium projektowym – w jakiej technologii został przygotowany, jaki zestaw uprawnień został przydzielony każdej z osób / ról występujących w projekcie, a także w jaki sposób można uzyskać do niego dostęp. W kolejnej części dokumentu przedstawiony został diagram Gantta zawierający daty realizacji kolejnych kamieni milowych projektu.

Na podstawie ustaleń z Klientem, sporządzono również dokument PQP (ang. Project Quality Plan), który jest częścią składową niniejszego dokumentu. Wskazano również wybrany wzorzec konstrukcyjny, a także wzorce dokumentów roboczych oraz protokołów.

Rozdział I

Skład zespołu projektowego

Zespół projektowy składa się ze studentów wojskowych oraz cywilnych z grup szkoleniowych WCY21IH1S4 oraz WCY21IM1S4

Tabela Zestawienie członków zespołu projektowego

|  |  |
| --- | --- |
| Rola | Imię i nazwisko |
| Kierownik projektu | Piotr STĘPIEŃ |
| Tester | Piotr SZMIGIEL |
| Bibliotekarz | Krystian PALCZAK |
| Zabezpieczenia informatyczne | Damian FEDOROWICZ  Dawid GRĘDZIŃSKI  **Rafał KĘPCZYŃSKI (szef zespołu)** |
| Zabezpieczenia fizyczne i techniczne | Wiktoria SIUDA  Przemysław STADEJEK  **Hubert WOJTAS (szef zespołu)** |
| Wsparcie rozwiązań (zabezpieczeń) organizacyjnych | Krzysztof MAGDOŃ  **Szymon WOŹNICA (szef zespołu)** |

Role w zespole zostały dobrane na podstawie umiejętności, kwalifikacji oraz doświadczenia poszczególnych członków zespołu w realizacji podobnych przedsięwzięć projektowych.

Kierownik projektu jako przedstawiciel całego przedsięwzięcia nadzoruje pracę pozostałych członków zespołu oraz jako osoba komunikatywna utrzymuje stały kontakt z klientem, ustala harmonogram Gantta oraz pilnuje dotrzymania terminów.

Tester nadzoruje jakość wytworzonej dokumentacji przez podzespoły od zabezpieczeń i wsparcia rozwiązań oraz trzymania się wcześniej ustalonych standardów.

Bibliotekarz ma za zadanie nadzorować repozytorium projektowe, ustalać dostęp do dokumentów odpowiednim podzespołom projektowym oraz zachowanie w archiwum wcześniejszych wersji dokumentów.

Zespół od zabezpieczeń informatycznych odpowiedzialny jest za modernizacje infrastruktury sieci wraz z wymianą przestarzałego sprzętu na nowszy oraz instalację lub aktualizację systemów informatycznych z długim okresem wsparcia technicznego.

Zespół przydzielony do zabezpieczeń fizycznych i technicznych ma na celu stworzenie sieci monitoringu budynku wraz z czujnikami ruchu i ochronę przed nieupoważnionym dostępem fizycznym osób trzecich oraz opracowanie procedur w razie naruszenia własności banku.

Zespół odpowiedzialny za wsparcie rozwiązań organizacyjnych ma na celu analizę obecnych rozwiązań organizacyjnych w firmie, a po porównaniu jej z wzorcem konstrukcyjnym przedstawia propozycję nowych zabezpieczeń

**Rozdział II**

Szablon dokumentacyjny

Szablon dokumentacyjny zawiera schemat układu poszczególnych elementów dla każdego z utworzonych dokumentów. Schemat szablonu znajduje się w repozytorium pod nazwą „Szablon dokumentacyjny.docx”, dodatkowa kopia znajduje się poniżej.



Rozdział III

Organizacja repozytorium projektowego

Niniejszy dokument zawiera przedstawienie organizacji repozytorium projektowego. Zawarte również są w nim podstawowe informacje na temat podziału zespołów, przydziału uprawnień, a także podstawowe informacje na temat bezpieczeństwa repozytorium.

## **Realizacja**

W celu realizacji zadania, utworzono repozytorium w serwisie GitHub o nazwie **PSBI,** znajduje się ono pod adresem ([*https://github.com/PSBI/PSBI*](https://github.com/PSBI/PSBI)*).*



Rysunek 1 Utworzone w repozytorium zespoły.

Powyższy rysunek przedstawia zespoły stworzone w serwisie GitHub zgodnie z podziałem zespołu projektowego na poszczególne zespoły zgodnie z tab. 1. Do stworzenia zespołów konieczne było stworzenie Organizacji, która pozwala na tworzenie grup według własnych potrzeb.

## **Podział i uprawnienia**

W ramach repozytorium stworzono zespoły, odpowiadające nazwami zespołom zadeklarowanych w trakcie początkowej fazy organizacji projektu. Do każdego z zespołów przypisani zostali odpowiedni członkowie, a następnie dla każdego zespołu została określona grupa wskazująca na uprawnienia. Żaden z członków projektu zgodnie z założeniami nie ma możliwości na usuwanie zawartości repozytorium. *Kierownik projektu* oraz *bibliotekarz* mają dostęp do wszystkich plików projektu. Członkowie zespołów mają możliwość edycji jedynie plików znajdujących się w konkretnym repozytorium, do którego mają prawa. Każdy z członków każdego zespołu może przeglądać zawartość pozostałych repozytoriów oraz plików utworzonych przez innych. Prawa dla poszczególnych członków przydzielać może *bibliotekarz.* Role w repozytorium zostały przypisane na podstawie Tab.1 określającej przynależność do konkretnych zespołów projektowych.

Tabela 2 Role oraz uprawnienia zespołów projektowych

|  |  |
| --- | --- |
| Rola | Uprawnienia |
| Bibliotekarz | * Modyfikacja wszystkich plików, * Czytanie zawartości wszystkich repozytoriów, * Klonowanie repozytorium. |
| Kierownik | * Modyfikacja wszystkich plików, * Czytanie zawartości wszystkich repozytoriów, * Klonowanie repozytorium. |
| Tester | * Modyfikacja wszystkich plików, * Czytanie zawartości wszystkich repozytoriów, * Klonowanie repozytorium. |
| Wsparcie rozwiązań | * Modyfikacja plików w repozytorium utworzonym w ramach zespołu, * Czytanie zawartości wszystkich repozytoriów, * Klonowanie repozytorium. |
| Zabezpieczenie fizyczne i techniczne | * Modyfikacja plików w repozytorium utworzonym w ramach zespołu, * Czytanie zawartości wszystkich repozytorium, * Klonowanie repozytorium. |
| Zabezpieczenie informatyczne | * Modyfikacja plików w repozytorium utworzonym w ramach zespołu, * Czytanie zawartości wszystkich repozytoriów, * Klonowanie repozytorium. |

## **Bezpieczeństwo**

Bezpieczeństwo przeprowadzanych projektów jest istotnym elementem działania. Zastosowanie technologii kontrolera wersji, pozwala na odtwarzanie wersji projektów, które w ramach czynników ludzkich czy też błędów systemowych mogły zostać utracone.

## **Wersjonowanie**

W celu kontroli wersji projektu, przyjęte zostaje wersjonowanie zgodnie ze specyfikacją [https://semver.org]. Odpowiednie wartości wskaźników wersji, w przypadku aktualizacji inkrementowane będą o 1 w górę. Wersjonowanie wykorzystane w przypadku projektu przedstawione będzie w formie:

* MAJOR – zmiana liczby na większą następuje w przypadku wprowadzania znacznych zmian, odbiegających znacznie od koncepcji wersji poprzedniej;
* MINOR – dodanie elementów zgodnych z aktualną wersją projektu;
* RELEASE – zmieniana w przypadku wprowadzania wyłącznie drobnych poprawek do aktualnej wersji.

Wersja przedstawiana będzie w formacie MAJOR.MINOR.RELEASE, np.: **1.4.2**.

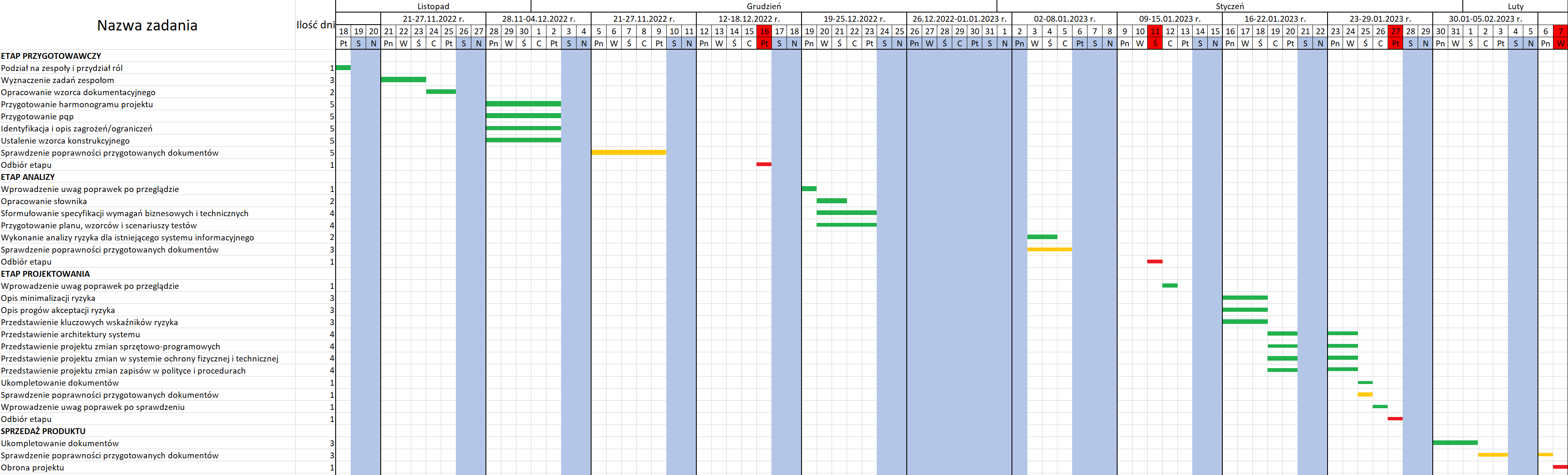
Każdy z członków zespołu projektowego, wykorzystując możliwość *GitHub,* może stworzyć *„branch”* umożliwiający stworzenie kopii, którą następnie może dowolnie modyfikować w obrębie uprawnień które zostały mu nadane.

## **Kopie bezpieczeństwa**

W celu zminimalizowania ryzyka utraty danych wykorzystane jest środowisko chmurowe, internetowe. Pozwala to na przechowywanie wszelkich danych zdalnie, jednocześnie umożliwiając dostęp z każdego miejsca na świecie członkom projektu. Repozytorium jest prywatne, więc tylko osoby dodane do projektu przez bibliotekarza mogą mieć do niego dostęp, jednocześnie eliminując wpływ osób postronnych niemal do 0. Poza przechowywaniem danych on-line, wykonywana będzie co tygodniowa kopia całego repozytorium na dysku sieciowym dostępnym dla każdego członka zespołu (serwis OneDrive dostępny dla studentów WAT). Umożliwi todostęp do danych w przypadku braku dostępu do witryny *GitHub.* Zalecane jest również, by wyznaczony członek zespołu (bibliotekarz) w wyznaczonych okresach czasu wykonywał dodatkową kopię bezpieczeństwa na prywatnym komputerze.

Rozdział IV

Harmonogram prac projektowych



Rysunek Diagram Gantta

**Tabelaryczny harmonogram prac projektowych: (na czerwono „kamienie milowe”)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ETAP | ZADANIE | ROZPOCZĘCIE | ILOŚĆ DNI | ZAKOŃCZENIE |
| PRZYGOTOWAWCZY | Podział na zespoły i podział ról | 18.11.2022 | 1 | 18.11.2022 |
| Wyznaczenie zadań zespołom | 21.11.2022 | 3 | 23.11.2022 |
| Opracowanie wzorca dokumentacyjnego | 24.11.2022 | 2 | 25.11.2022 |
| Przygotowanie harmonogramu projektu | 28.11.2022 | 5 | 02.12.2022 |
| Przygotowanie PQP | 28.11.2022 | 5 | 02.12.2022 |
| Identyfikacja i opis zagrożeń/ograniczeń | 28.11.2022 | 5 | 02.12.2022 |
| Ustalenie wzorca konstrukcyjnego | 28.11.2022 | 5 | 02.12.2022 |
| Sprawdzenie poprawności przygotowanych dokumentów | 05.12.2022 | 5 | 09.12.2022 |
| Odbiór etapu | 16.12.2022 | 1 | 16.12.2022 |
| ANALIZY | Wprowadzenie uwag poprawek po przeglądzie | 19.12.2022 | 1 | 19.12.2022 |
| Opracowanie słownika | 20.12.2022 | 2 | 21.12.2022 |
| Sformułowanie specyfikacji wymagań biznesowych i technicznych | 20.12.2022 | 4 | 23.12.2022 |
| Przygotowanie planu, wzorców i scenariuszy testów | 20.12.2022 | 4 | 23.12.2022 |
| Wykonanie analizy ryzyka dla istniejącego systemu informacyjnego | 03.01.2023 | 2 | 04.01.2023 |
| Sprawdzenie poprawności przygotowanych dokumentów | 03.01.2023 | 3 | 05.01.2023 |
| Odbiór etapu | 11.01.2023 | 1 | 11.01.2023 |
| PROJEKTOWANIA | Wprowadzenie uwag poprawek po przeglądzie | 12.01.2023 | 1 | 12.01.2023 |
| Opis minimalizacji ryzyka | 16.01.2023 | 3 | 18.01.2023 |
| Opis progów akceptacji ryzyka | 16.01.2023 | 3 | 18.01.2023 |
| Przedstawienie kluczowych wskaźników ryzyka | 16.01.2023 | 3 | 18.01.2023 |
| Przedstawienie architektury systemu | 18.01.2023 | 4 | 24.01.2023 |
| Przedstawienie projektu zmian sprzętowo-programowych | 18.01.2023 | 4 | 24.01.2023 |
| Przedstawienie projektu zmian w systemie ochrony fizycznej i technicznej | 18.01.2023 | 4 | 24.01.2023 |
| Przedstawienie projektu zmian zapisów w polityce i procedurach | 18.01.2023 | 4 | 24.01.2023 |
| Ukompletowanie dokumentów | 25.01.2023 | 1 | 25.01.2023 |
| Sprawdzenie poprawności przygotowanych dokumentów | 25.01.2023 | 1 | 25.01.2023 |
| Wprowadzenie uwag poprawek po przeglądzie | 26.01.2023 | 1 | 26.01.2023 |
| Odbiór etapu | 27.01.2023 | 1 | 27.01.2023 |
| SPRZEDAŻ PRODUKTU | Ukompletowanie dokumentów | 30.01.2023 | 3 | 01.02.2023 |
| Sprawdzenie poprawności przygotowanych dokumentów | 02.02.2023 | 3 | 06.02.2023 |
| Obrona projektu | 07.02.2023 | 1 | 07.02.2023 |

Rozdział V

Project Quality Plan

## **5.1 Sposoby oceniania jakości**

1. Doświadczenie zebrane podczas wieloletniej pracy członków zespołu.
2. Ocena zamawiającego
3. Wzorcem do oceny jakości będą normy ISO 27002:2014-12 oraz NIST 800-160
4. Przed złożeniem wersji produktu do repozytorium jest zbierana opinia o tym produkcie od wszystkich członków zespołu wykonawczego.
5. Dobra komunikacja z interesariuszami.
6. Realizacja wymagań interesariuszy
7. Dobór właściwych metod projektowania
8. Kompletność dokumentacji projektowej
9. Jednoznaczność dokumentacji projektowej

## **5.2 Rodzaje prowadzonych kontroli i przeglądów realizacji przedsięwzięcia**

1. Kontrola realizacji przedsięwzięcia w dniu 16.12.2022
   1. Spotkanie stacjonarne w budynku 65, sala nr 106
   2. Rozpoczęcie spotkania: 17:35
   3. Przewidywany czas spotkania 3 godziny
   4. Uczestnicy:
      1. Strona zamawiająca:
         1. Krzysztof Liderman, Adam Patkowski
      2. Strona wykonawcy:
         1. Piotr Stępień, Hubert Wojtas.
2. Odbiór etapu I przedsięwzięcia w dniu 11.01.2022
   1. Spotkanie stacjonarne w budynku 65, sala 106
   2. Rozpoczęcie spotkania: 17:35
   3. Przewidywany czas spotkania 3 godziny.
   4. Uczestnicy:
      1. Strona zamawiająca:
         1. Krzysztof Liderman, Adam Patkowski
      2. Strona wykonawcy:
         1. Piotr Stępień, Hubert Wojtas.
3. Odbiór etapu II przedsięwzięcia w dniu 27.01.2022
   1. Spotkanie stacjonarne w budynku 65, sala 106
   2. Rozpoczęcie spotkania: 09:50
   3. Przewidywany czas spotkania 3 godziny.
   4. Uczestnicy:
      1. Strona zamawiająca:
         1. Krzysztof Liderman, Adam Patkowski
      2. Strona wykonawcy:
         1. Piotr Stępień, Hubert Wojtas.
4. Odbiór projektu w dniu 07.02.2022
   1. Spotkanie stacjonarne w budynku 65, sala 203
   2. Rozpoczęcie spotkania: 09:50
   3. Przewidywany czas spotkania 1,5 godziny.
   4. Uczestnicy:
      1. Strona zamawiająca:
         1. Krzysztof Liderman, Adam Patkowski
      2. Strona wykonawcy:
         1. Piotr Stępień, Hubert Wojtas.

## **5.3 Normy stosowane podczas realizacji przedsięwzięcia**

1. Norma Międzynarodowa ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements - ma status Polskiej Normy
2. Norma Międzynarodowa ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls - ma status Polskiej Normy

## **5.4 Sposoby rozstrzygania sporów zleceniodawca-wykonawca**

1. Zleceniodawca musi otrzymać dokumentacje od wykonawcy na nie później niż dwie doby przed odbyciem się zaplanowanej kontroli realizacji przedsięwzięcia.
2. Czas na usunięcie wskazanych przez zleceniodawcę niedociągnięć i uwag wynosi 7 dni.
3. Korekty będą wprowadzane poprzez organizacje dodatkowego spotkania w przypadku wystąpienia wielu modyfikacji.
4. Małe korekty dotyczące niewielkich modyfikacji będą realizowane poprzez spotkanie się kierownika projektu i zleceniodawcy.
5. Jeżeli zespoły biorące udział w przekazaniu produktu nie dochodzą do porozumienia, decyzje podejmuje komitet sterujący projektu.
6. Inne niewymienione przypadki rozstrzyga się według kodeksu postępowania cywilnego.

## **5.5 Procedury wyszukiwania i zgłaszania błędów**

1. Procedury wyszukiwania błędów opracowanie przez kierownictwo projektu
   1. Wynik rzeczywisty różni się od wyniku oczekiwanego.
   2. Zaproponowane rozwiązanie nie spełnia wymagań nałożonych na projektu
2. Procedury zgłaszania błędów
   1. Przekazywać informację o błędach ustnie lub pisemnie do kierownika projektu (zastosować zasadę, że komunikacja ustna jest uzupełnieniem komunikacji pisemnej).
   2. Raport o błędach powinien zawierać: temat, datę, autora, krótki opis błędu.

## **5.6 Dokumenty przygotowywane przez kontrolera jakości**

1. Plan testów (plan testów wymagań)
2. Scenariusze testowe
3. Notatki z przeprowadzonych spotkań
4. Raporty z testów ad hoc
5. Raport ze spotkania z zamawiającym

## **5.7 Informacje przekazywane zespołowi wytwórczemu**

1. Okoliczności wystąpienia błędów
2. Wpływ zgłoszonych błędów na jakość wykonania projekt

**Rozdział VI**

Wzorzec konstrukcyjny

**Konstruowanie systemu zabezpieczeń według zaleceń norm ISO/IEC 27002:2013 i ISO/IEC 27001:2013**

Dziewięćdziesięcio stronicowa norma ISO/IEC 27002:2013 zawiera specyfikację 14 obszarów bezpieczeństwa (w normie nazwanych clauseses, odpowiadających tytułom rozdziałów głównych 5-18 – patrz Rysunek 2) zawierających łącznie 35 głównych kategorii bezpieczeństwa (odpowiadających tytułom podrozdziałów rozdziałów 5-18) i 114 zabezpieczeń. Podanej w normie kolejności obszarów (wyrażonej ich numeracją) nie należy traktować jak listy priorytetowej – znaczenie poszczególnych obszarów będzie się zwykle różniło w zależności od stosującej normę organizacji.

Każda główna kategoria bezpieczeństwa (ang. main security control category) zawiera:

* cele zabezpieczeń, wskazujące co należy osiągnąć,
* jedno lub więcej zabezpieczeń które powinny zostać zastosowane dla osiągnięcia celów.

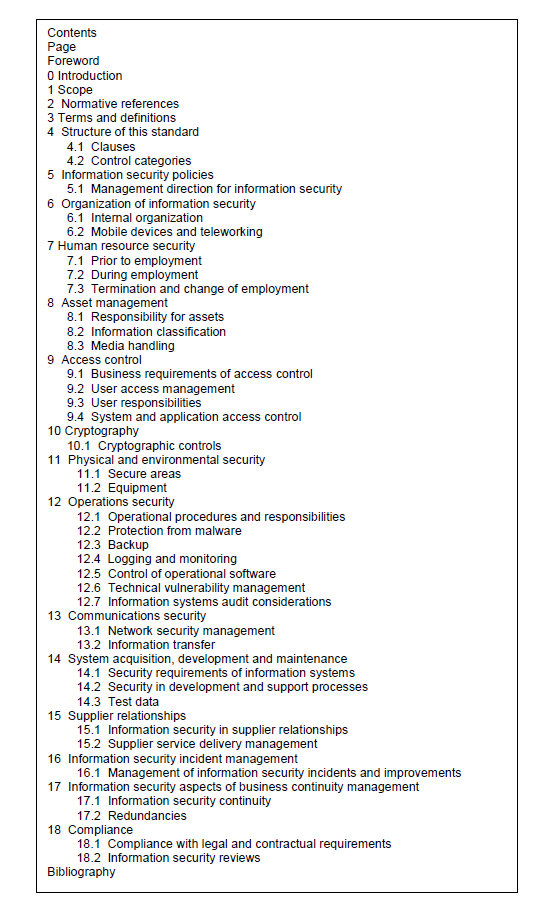
Każde z zawartych w normie 114 zabezpieczeń jest opisanych w następującej formie:

* nazwa zabezpieczenia i krótki opis,
* wskazówki do implementacji zabezpieczenia (ang. implementation guidance),
* informacje dodatkowe (ang. other information).

Norma ISO/IEC 27001:2013 znajduje zastosowanie we wszystkich rodzajach organizacji niezależnie od typu, rozmiaru i natury prowadzonej działalności biznesowej. Określono w niej wymagania dotyczące ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymywania i doskonalenia udokumentowanego SZBI. Obligatoryjną podstawą tych działań jest zidentyfikowane ryzyko biznesowe. Zaleca się, aby wprowadzenie SZBI było dla organizacji decyzją strategiczną. Norma ISO/IEC 27001 może być wykorzystywana do szacowania zgodności przez zainteresowane strony wewnętrzne i zewnętrzne.

Przedstawiony w normie model SZBI został zaprojektowany tak, aby zapewnić adekwatne i proporcjonalne zabezpieczenia, które odpowiednio chronią aktywa informacyjne co w efekcie ma pozwolić uzyskać zaufanie zainteresowanych stron co do deklarowanej skuteczności ochrony zasobów informacyjnych.

Aktualne wydanie normy, tj. ISO/IEC 27001:2013, to 30 stron o zawartości przedstawionej na Rysunek 3 Norma „jako taka” zajmuje 9 stron. Pozostałe strony to normatywny załącznik A, stanowiący podstawę konstrukcji deklaracji stosowania, który zawiera przedstawione w zwartej formie zalecenia z obszarów 5-18 normy ISO/IEC 27002:2013. Tytuły rozdziałów 4-10 normy to w zasadzie nazwy czynności (dokładniej – zbiorów czynności) które należy wykonać w celu zbudowania SZBI.



Rysunek Struktura normy ISO/IEC 27002:2013

Obraz zawierający tekst

Opis wygenerowany automatycznie

Rysunek Struktura normy ISO/IEC 27001:2013

Rozdział VII

Identyfikacja ograniczeń

Identyfikacja ograniczeń wraz ze specyfikacją wymagań znajdują się w repozytorium pod nazwą „Specyfikacja wymagań. Projekt PSBI 2022-2023.docx”.

Rozdział VIII

Dokumenty robocze i wzorce

< dołączane w trakcie realizacji projektu, np. protokoły z odbiorów etapów >

Wykaz rysunków

[Rysunek 1 Utworzone w repozytorium zespoły. 7](#_Toc124202966)

[Rysunek 2 Diagram Gantta 12](#_Toc124202967)

[Rysunek 3 Struktura normy ISO/IEC 27002:2013 20](#_Toc124202968)

[Rysunek 4 Struktura normy ISO/IEC 27001:2013 21](#_Toc124202969)

Wykaz tabel

[Tabela 1 Zestawienie członków zespołu projektowego 4](#_Toc124202960)