Politechnika Koszalińska

Wydział Elektroniki i Informatyki

Kierunek: Informatyka

Rok akademicki: 2015/2016

Temat:

Space Invader – aplikacja na platormę Android

Wykonawcy:

Patryk Rygas

Artur Jaświłek

Dawid Dąbrowski

Michał Wójcik

Karolina Kaczmarek

Justyna Jarkiewicz

1. Protokół założycielski

Dnia 01.03.2016 została utworzona grupa projektowa w celem wykonania zadania programistycznego „Gra zręcznościowa na platformie Android – Space Invader”

Przewidywana data zakończenia projektu: 31.05.2016r. Jeśli projekt nie zostanie zakończony w pierwszym terminie to przewidywany jest drugi termin zakończenia projektu: 07.06.2016r. Zespół zostanie rozwiązany po zakończeniu projektu w odpowiednim terminie.

W skład grupy wchodzą:

- Patryk Rygas – Kierownik projektu, programista, analityk
- Dawid Dąbrowski – Programista, projektant
- Karolina Kaczmarek – Programista, dokumentalista
- Michał Wójcik – Programista, grafik
- Artur Jaświłek – Programista, tester
- Justyna Jarkiewicz – Dokumentalistka, grafik

Tytuł projektu: Space Invaders

Kierownik projektu: Patryk Rygas (programista, analityk) – jednogłośnie wybrany w sposób demokratyczny.

Zasady współpracy w grupie:

- Wszystkie przydzielone nam zadania zobowiązujemy wykonywać terminowo.
- Wszyscy angażujemy się w pracę i jesteśmy odpowiedzialni za wyniki.

• Szanujemy oraz wspomagamy się nawzajem.

• Doceniamy pracę i zaangażowanie innych.

• Uwagi zgłaszamy do kierownika projektu.

• Podnosimy motywacje i zaangażowanie w zespole.

• Nie używamy wulgarnych wyrażeń przeciwko drugiej osobie.

• Ważne, aby każdy członek zespołu otrzymał określoną funkcję lub mógł sam ją wybrać.

Cel projektu:

Celem projektu jest stworzenie prostej gry zręcznościowej nawiązującej klimatem do kultowych gier typu „Galaxian", „Space Invader" znanych z konsoli Pegasus, Atari, Commodore oraz telefonów komórkowych starszej generacji.

7.Rola i odpowiedzialności:

• Patryk Rygas – pełni rolę jako kierownik projektu oraz programista. Odpowiada za nadzór nad wykonaniem projektu zgodnie z harmonogramem prac. Odpowiada za

• Dawid Dąbrowski – pełni rolę jako programista oraz projektant. Odpowiada za zaprojektowanie oraz stworzenie szkieletu aplikacji, optymalizację wydajności i jakości istniejącej aplikacji, projektowanie klas, metod i obiektów.

• Karolina Kaczmarek –Programista odpowiadający zarówno za kod jak i za dokumentacje .

- Michał Wójcik – Odpowiada za stworzenie prostego i przejrzystego, a zarazem estetycznego interfejsu użytkownika.
- Artur Jaświłek – Wszechstronny.
- Justyna Jarkiewicz-Dokumentalistka.

Nagrody i kary:

- Nagrody: Za pracę zgodnie z harmonogramem uczestnicy projektu pozytywną ocenę z wpisem do indeksu.
- Kary: W przypadku niewywiązania się z obowiązków w procesie realizacji projektu, osoby należące do grupy mogą wykluczyć daną osobę z projektu.
- Rozwiązanie grupy: Rozwiązanie grupy następuje po zakończeniu prac projektowych.
- Postanowienie końcowe: Do projektu dopuszcza się wprowadzenie najwyżej trzech zmian, które nie będą miały wielkiego wpływu na funkcjonalność niniejszego projektu.
- Zostaną sporządzone trzy kopie umowy, po jednym egzemplarzu dla każdej ze stron.
- Umowa zaczyna obowiązywać w dniu, w którym zostanie podpisana i obowiązuje do 08.06.2016.

Patryk Rygas …….

Dawid Dąbrowski…….

Karolina Kaczmarek …….

Michał Wójcik …….

Artur Jaświłek …….

Justyna Jarkiewicz …….

2. Instrumentarium

Zostało stworzone repozytorium projektu o nazwie „SpaceInvader” na serwerze GitHub Do repozytorium dodawane będą kolejne wersje dokumentacji, z możliwością przeglądania przez wszystkich członków zespołu projektowego.

Narzędzia wykorzystywane podczas pracy projektowej:

- Oracle Eclipse - producent Eclipse Foundation, licencja Eclipse Public License (http://www.eclipse.org/),
- Diagram Designer - producent MeeSoft, licencja freeware (http://logicnet.dk/DiagramDesigner/),
- ArgoUML – producent Tigris.org
- Photoshop - producent Adobe Systems, licencja komercyjna (http://www.adobe.com/Photoshop/),
- Mozilla Firefox - producent Mozilla Corporation, licencja Mozilla Licensing (http://www.mozilla.org/pl/firefox/new/)
- Microsoft Word - producent Microsoft, licencja komercyjna (http://office.microsoft.com/pl- pl/word/)

3. Opis wymagań klienta

3.1. Model biznesowy klienta

Klientem jest każdy użytkownik telefonu z systemem Android. Gra nie posiada ograniczeń wiekowych.

3.2. Wymagania niefunkcjonalne:

- Brak weryfikacji użytkownika.
- Działanie nie wymaga dostępu do Internetu.

4.Wstępny harmonogram prac

Luty:

1. Założenie grupy projektowej

Marzec:

2. Uzgodnienie wstępnych założeń projektu z klientem
3. Określenie wymagań funkcjonalnych projektu
4. Tworzenie dokumentacji (diagram klas, diagram przypadków użycia, funkcjonalności)

Kwiecień:

5. Zaprojektowanie graficznego interfejsu użytkownika
6. Programowanie kolejnych etapów projektu
7. Konsultacje z klientem
8. Programowanie wykończeniowe

Maj:

9. Testowanie i naprawa ewentualnych błędów
10. Finalizacja projektu

5.Specyfikacja funkcji:

Generowanie planszy – Ustalenie na którym trybie gramy: Modern lub retro. Wyczyszczenie menu oraz wypełnienie okna tłem z pliku w odpowiednim formacie, zależnie od trybu w którym gramy.

Generowanie bohatera – Ustalenie pozycji startowej. Wczytanie grafiki statku z pliku zależnie od trybu w którym gramy.

Generowanie przeciwników - Ustawienie przeciwnika wczytując tym samym jego grafikę z pliku odpowiadającemu planszy na której gramy. Przesuniecie x o (n) i ustawienie kolejnego przeciwnika i tak do końca linii po czym zwiększenie y o (n) i ustawienie kolejnych przeciwników. Przeciwnicy mogą zajmować maksymalnie jedną trzecia ekranu patrząc od góry.

Funkcja poruszania statkiem w prawo i w lewo – Nasłuchiwanie klawiatury w oczekiwaniu na wciśniecie przycisku: strzałka w lewo lub strzałka w prawo. Po przechwyceniu kliknięcia funkcja oblicza nowe współrzędne dla wartości x w przypadku strzałki w lewo odejmuje 25 w przypadku strzałki w prawo dodanie

25. Po tym następuje sprawdzenie czy nowa wartość nie wychodzi za obszar planszy jeśli nie wychodzi statek jest usuwany i rysowany na nowych współrzędnych. W przypadku przekroczenia zakresu nie jest wykonywane przesuniecie i współrzędne wracają do starych wartości.

Funkcja strzelania gracza– funkcja czeka na wciśniecie przycisku „spacja" po czym tworzy nowy obiekt który jest pociskiem. Jego współrzędne startowe są identyczne co współrzędne gracza. Co 0,1 Y pocisku jest zmniejszane o 10 dzięki czemu pocisk się przemieszcza w stronę przeciwników. Jeśli współrzędne x i y pokryją się z współrzędnymi przeciwnika jest on niszczony. Przy wystrzeleniu pocisku z magazynka jest zabierany jeden strzał.

6. Wymagania sprzętowe 3.1Telefon/SmartPhone

1. System minimalny – Android 2.3 Gingerbread.
2. Gra zostanie zaprojektowana, aby SmartPhony posiadające pamięć 8GB lub 16GB nie odczuwały w żaden sposób obciążenia. Urządzenia o mniejszej pamięci wbudowanej również poradzą sobie z wymaganiami programu.

3. Minimalne wymagania podzespołów
   Samsung Exynos 4210
   Zegar procesora: 1,20 GHz Liczba rdzeni: 2
   GPU:ARM Mali-400 MP4 @266 MHz
   Pamięć RAM: 1 GB
   3.5 Wyświetlacz
   Kolorowy / 16M kolorów
   480 x 800 px (4.27")
   218 ppi.

4. Aplikacja nie będzie działała na podzespołach o mniejszej wartości niż podane. Docelowo gra zostanie zaprojektowana dla modelu Samsung Galaxy S2 i wszystkich jego danych sprzętowcyh oraz przypisanego mu danego systemu Android. Program będzie aktualizowany, aby mógł również pracować na innych modelach telefonów z systemem Android, począwszy od Androida 2.3 Gingerbread aż do Android Lollipop 5.0.

7.Słowniczek

- Gracz – użytkownik telefonu
- Komputer – przeciwnik gracza, wspierany przez algorytm AI.
- Statek – pojazd kierowany przez gracza

8.Identyfikacja aktorów

Gracz – Główny użytkownik aplikacji.

- Wyświetlenie rankingu najlepszych graczy
- Sterowanie ruchem statku
- Strzelanie
- Zamknięcie aplikacji

Komputer – Ruchomy przeciwnik wygenerowany na rzecz projektu.

9.Przypadki użycia

Nr przypadku: 1

1. Nazwa przypadku: Rozpoczęcie rozgrywki

   Krótki opis: Przypadek użycia pozwala na rozpoczęcie rozgrywki przez użytkownika.

   Aktor główny: Gracz

   Wyzwalacz: Przypadek użycia rozpoczyna sie w momencie kliknięcia ikony aplikacji przez użytkownika, w katalogu aplikacji urządzenia na którym zainstalowana jest aplikacja.

   Przebieg zdarzeń:

Przebieg podstawowy

Gracz włącza aplikację poprzez naciśnięcie jej ikony w katalogu aplikacji.

Gracz naciska przycisk START w menu głównym.

Zostaje wyświetlona aktywność Nowa Gra.

Przebieg alternatywny

1. Gracz naciska przycisk powrót.

2. Zamknięcie aplikacji.

Nr przypadku: 2

1. Nazwa przypadku : Granie w grę

   Krótki opis: Przypadek określa postępowanie w przypadku kiedy gracz prowadzi rozgrywkę.

   - Aktor główny Gracz
   - Wyzwalacz: Naciśnięcie przycisku START w menu głównym

Przebieg zdarzeń

1. przebieg podstawowy
2. Gracz naciska przycisk START w menu głównym.
3. System wyświetla grafikę gracza.
4. System wyświetla grafikę przeciwnika w określonej lokalizacji.
5. Gracz przesuwa swój statek na pozycję w której może strzelić do przeciwnika.
6. Gracz strzela statkiem.
7. Pocisk wystrzelony ze statku trafia w przeciwnika.
8. Przeciwnik zostaje zniszczony.
9. Gracz wygrywa.

Przebieg alternatywny

1. Pocisk wystrzenony ze statku nie trafia w przeciwnika.
2. Przeciwnik nie zostaje zniszczony.
3. Gracz przegrywa.
4. Koniec gry

Nr przypadku: 3

1. Nazwa przypadku: Zmiana ustawień gry
2. Krótki opis: Przypadek użycia zachodzi kiedy gracz czhe zmienić ustawienia gry.
3. Aktor główny: Gracz
4. Wyzwalacz: Naciśnięcie przycisku SETTINGS w menu głównym

Przebieg zdarzeń

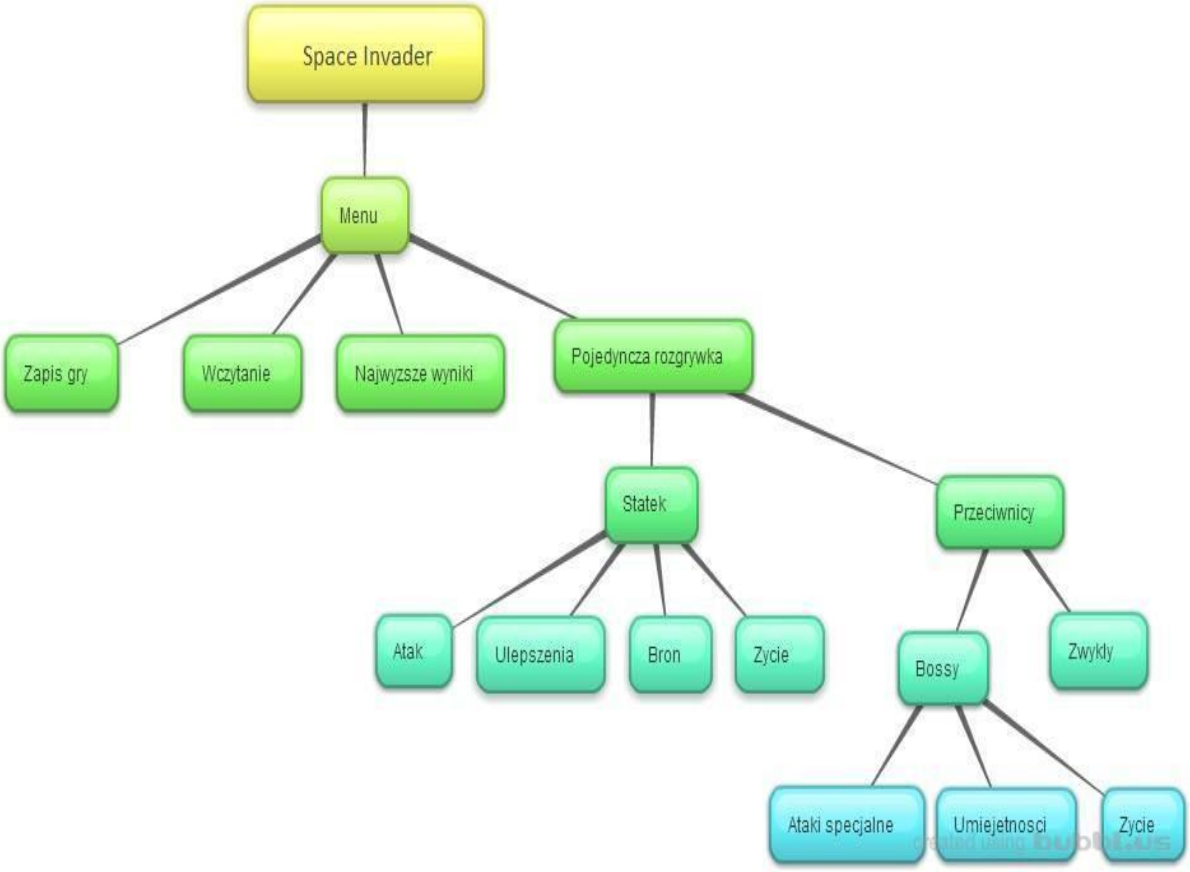
1. przebieg podstawowy

1. Gracz przyciska przycisk SETTINGS w menu głównym gry.
2. Wyświetlana jest aktywność ustawienia.
3. Aktualizowane są ustawienia gry.
4. Gracz zmienia checkbox dzwięki na przeciwne.
5. Gracz zmienia checkbox muzyka na przeciwny.
6. Gracz naciska przycisk Powrót.
7. Ekran ustawień zostaje zamknięty.

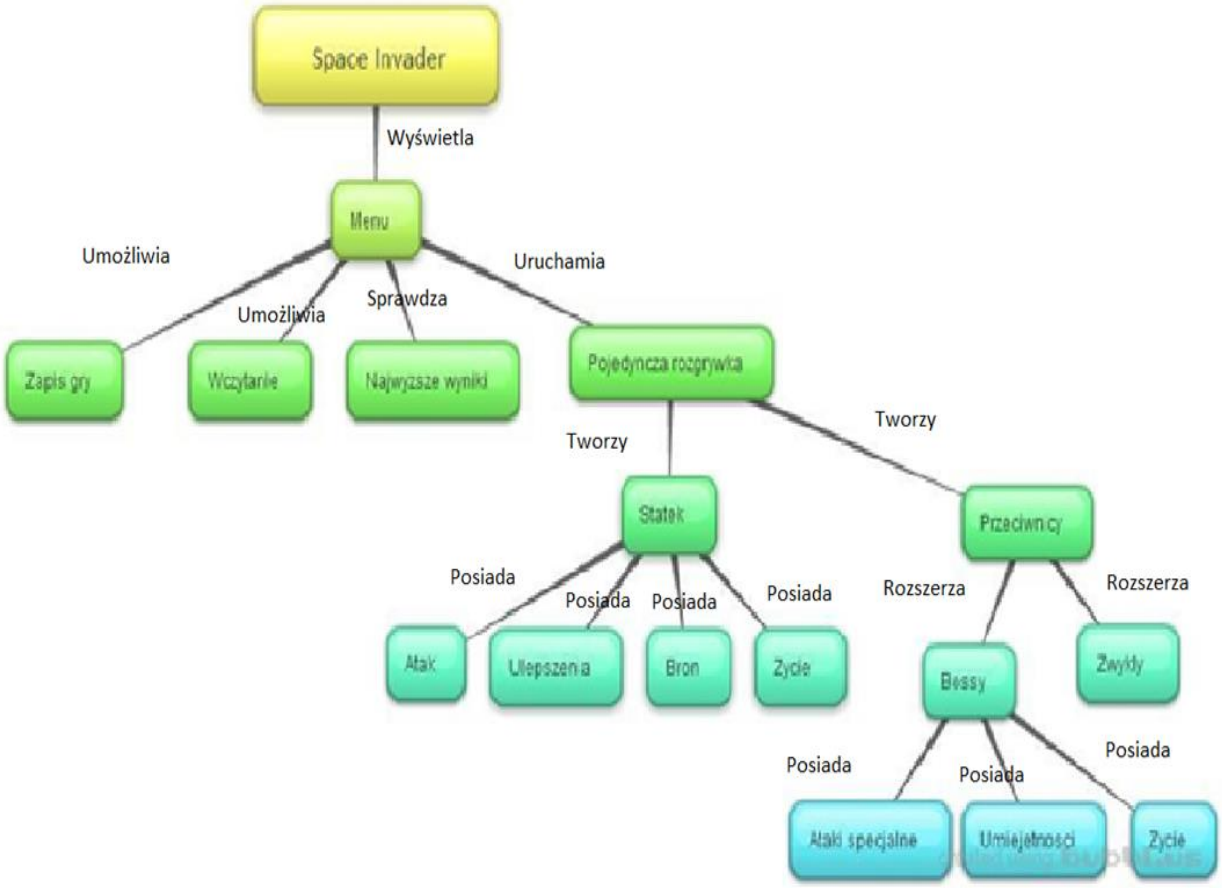
Przebieg alternatywny:

1. Gracz przyciska przycisk Powrót.
2. Ekran ustawień zostaje zamknięty.

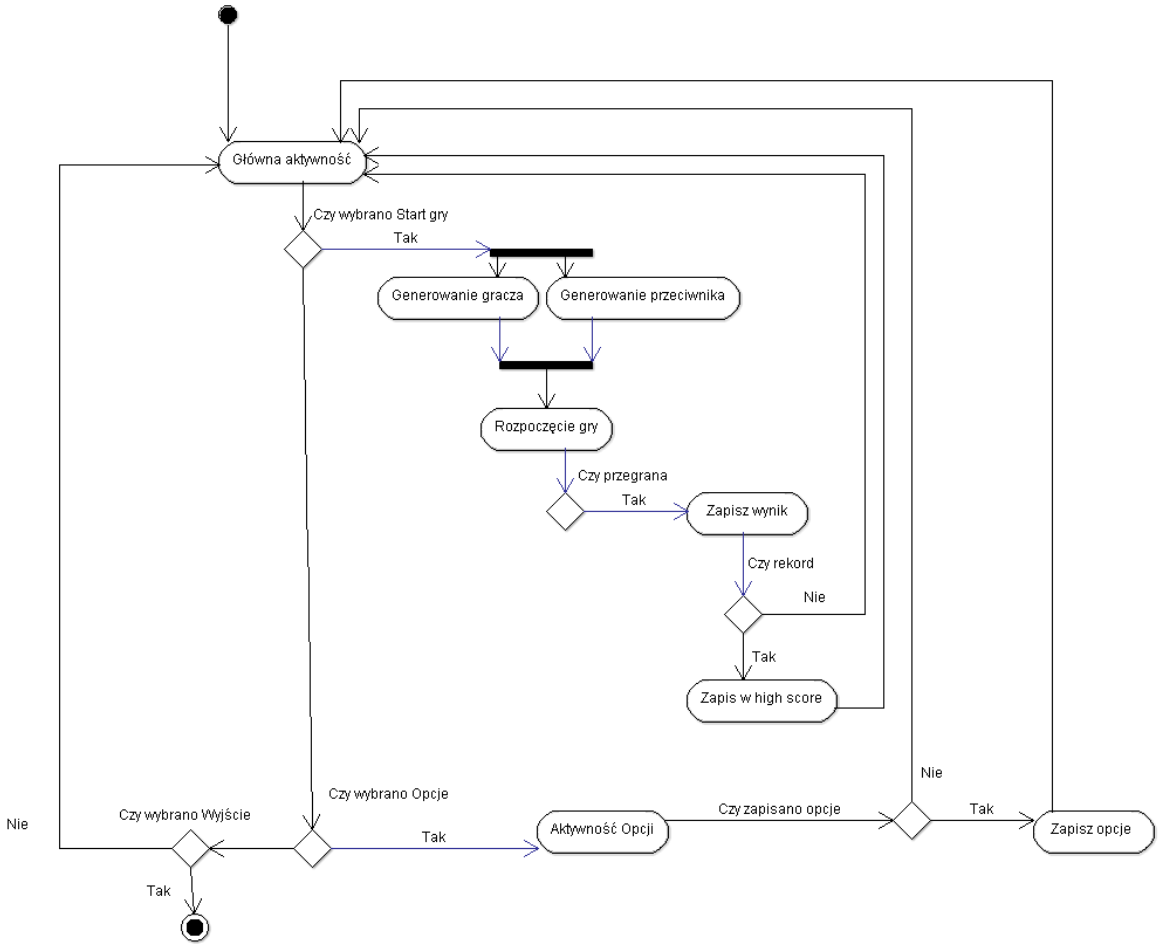
10.Mapa Myśli



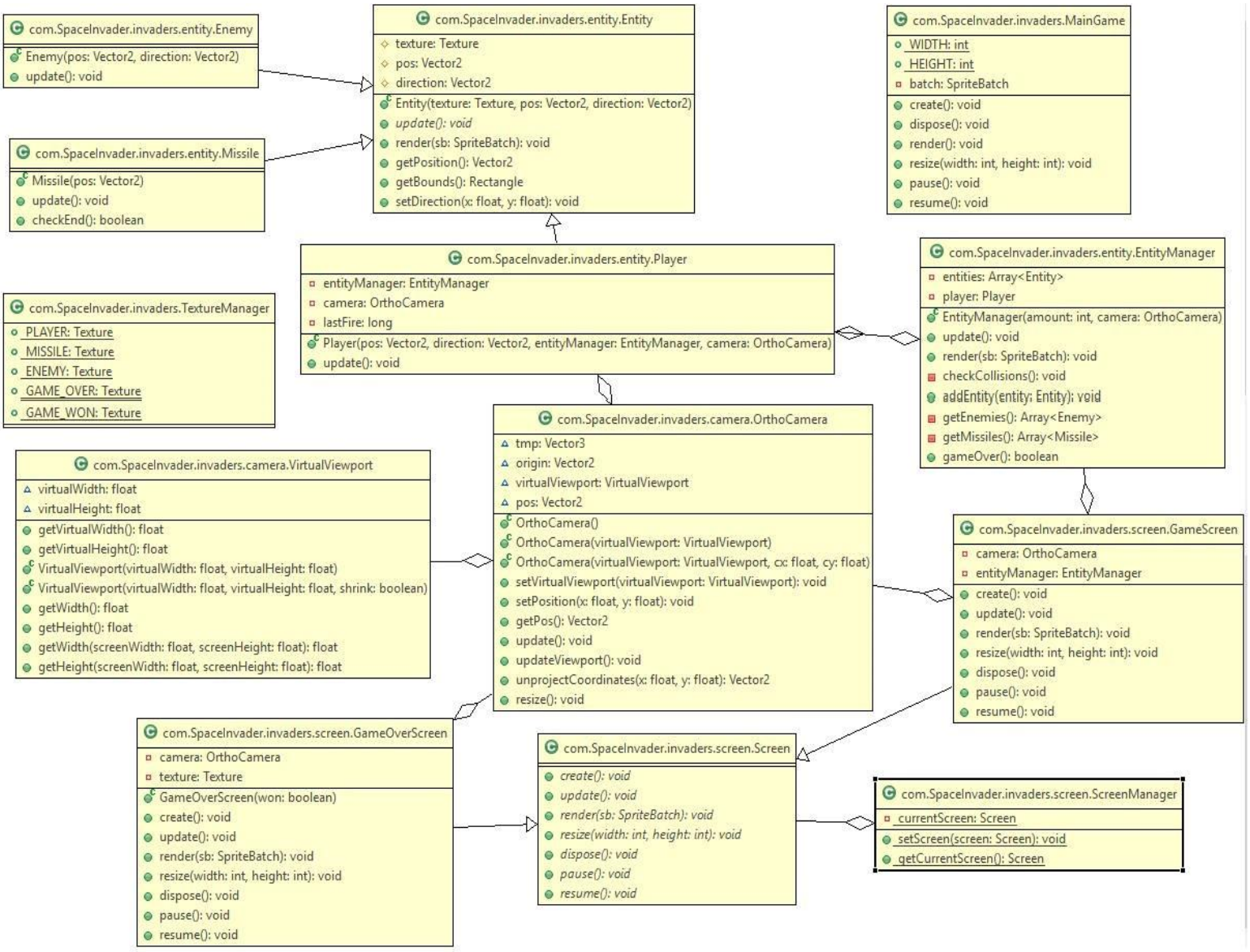
11.Mapa konceptualna .



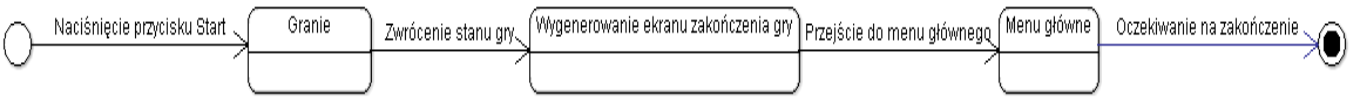
12.Diagram aktywności UML



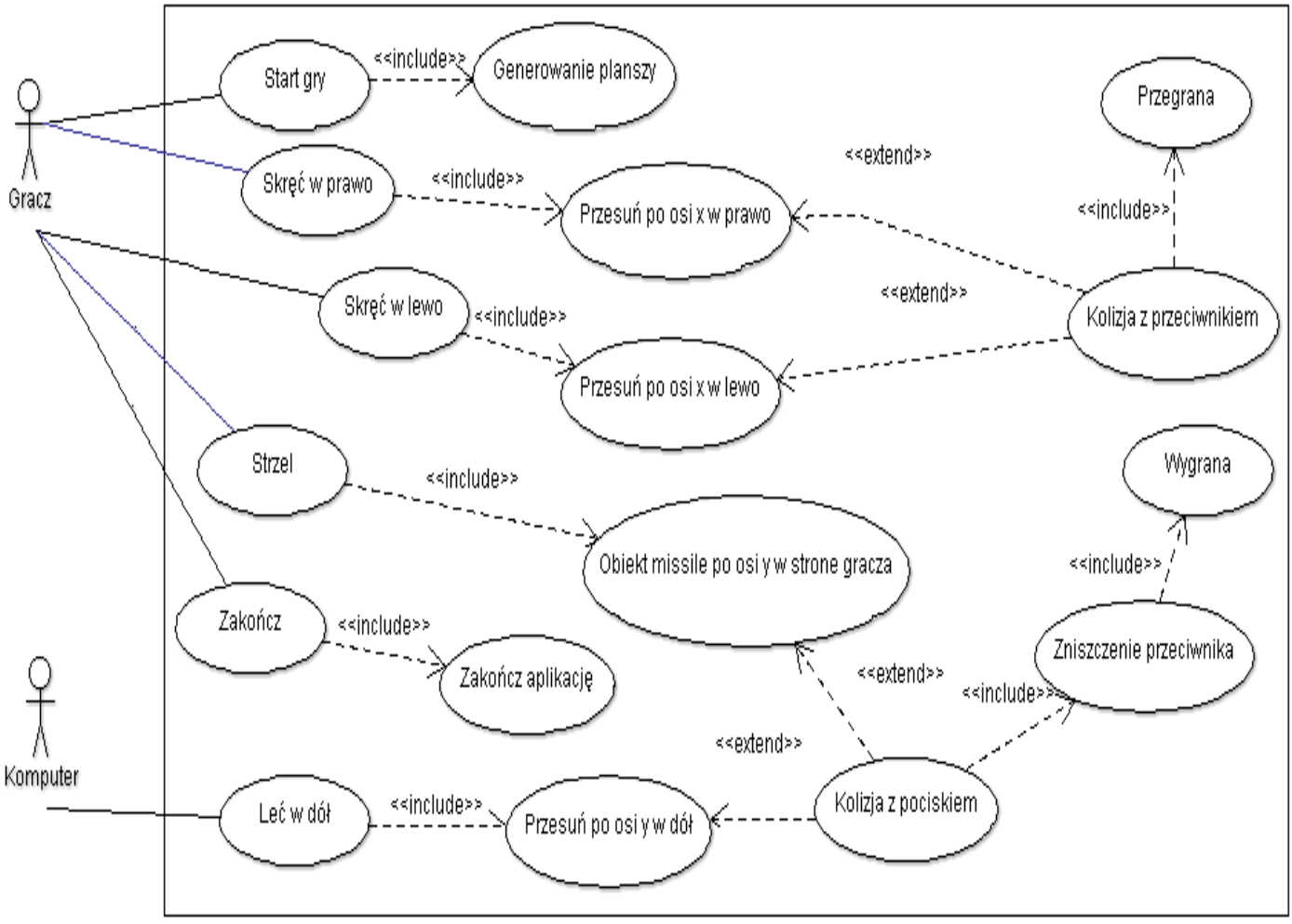
13.Diagram klas UML



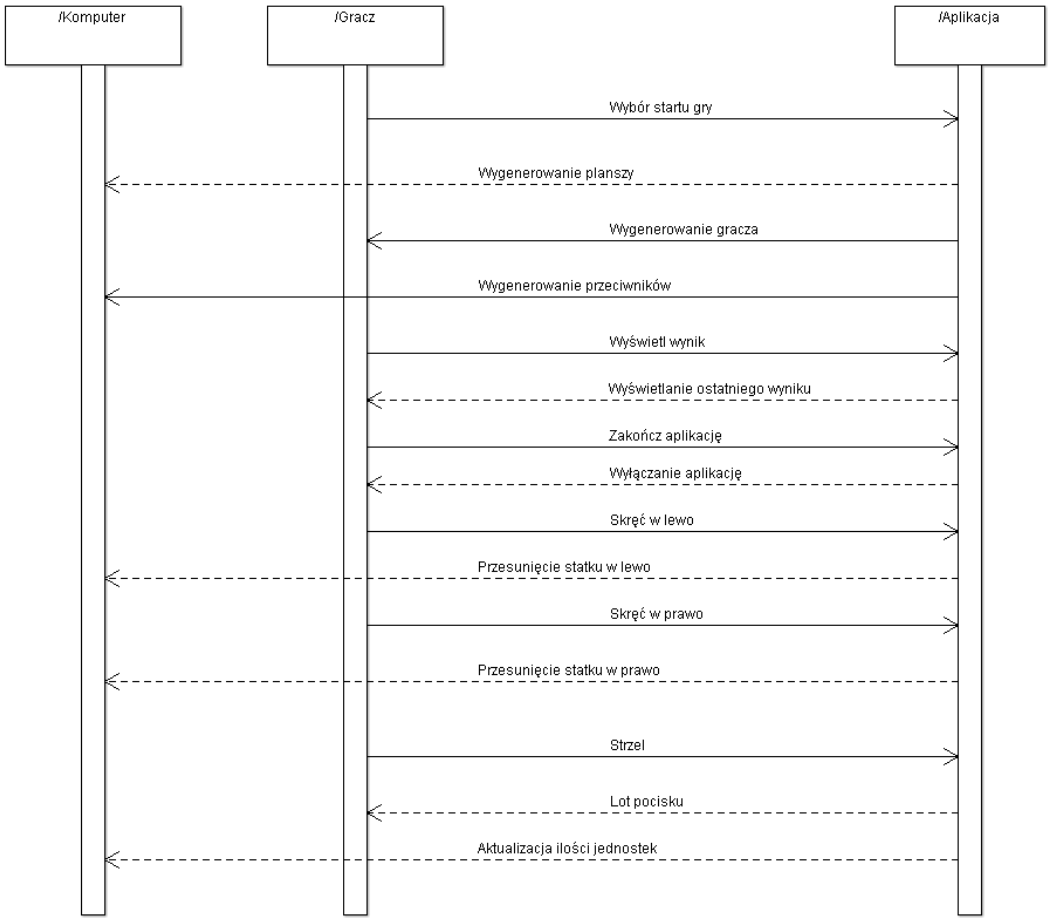
14.Diagram przepływu danych



15.Diagram przypadków użycia



16.Diagram sekwencji



17.Polityka jakości, bezpieczeństwa i niezawodności

Firma „Analizuj z nami” wykonuję analizy niezawodności oprogramowania w składy których wchodzą:

- Okresowe szkolenia pracowników
- Ocena niezawodności oprogramowania
- Ocena bezpieczeństwa oprogramowania

Okresowe szkolenia pracowników – polegają na jak najlepszy przygotowaniu użytkowników do użytkowania oprogramowania. Pozwalają one szkolić pracowników w kategoriach użytkowania oprogramowania, bezpieczeństwa i wsparcia.

Ocena niezawodności oprogramowani – to proces oceny oprogramowania biorący pod uwagę prawdopodobieństwo awarii różnych modułów oprogramowania i sposób ich połączenia wpływający na całkowitą niezawodność oprogramowania

Ocena bezpieczeństwa oprogramowania – to proces pozwalający na dokładne testy bezpieczeństwa od luk w programie po użytkownika końcowego. Dzięki temu procesowi mogą być państwo pewni że ryzyko wycieku danych czy awarii jest zminimalizowane.

Polityką Jakości firmy „Analizuj z nami" jest

- Inicjowanie i prowadzenie działań służących zapewnieniu bezpieczeństwa oprogramowania
- Ukierunkowanie świadczonych usług w zakresie:
  - Zarządzania
  - Szkoleń na spełnianie potrzeb i oczekiwań Klientów
  - Certyfikacji osób
  - Oceny zgodności
  - Popularyzowania zagadnień związanych z bezpieczeństwem danych
- Dbałość o właściwy wizerunek „Nazwa firmy" i świadczenie usług w sposób etyczny i kompetentny.

- Dostosowanie form działalności do wymagań rynku

Zadowolenie Klientów stanowi miarę jakości naszych usług.

Podejmowanie działań na rzecz poprawy jakości ma dla nas znaczenie priorytetowe i wszyscy jesteśmy w nie zaangażowani. Osiąganie planowanych wyników jakości realizujemy przez wdrożenie i ciągłe doskonalenie skuteczności systemu zarządzania jakością.

„Nazwa firmy" inicjuje i prowadzi działania służące zapewnieniu bezpieczeństwa danych, kompetencji pracowników poprzez stałą poprawę i ciągłe doskonalenie naszych usług.

Dążymy do:

- Zapewnienia zasobów i środków do wdrażania polityki.
- Podnoszenia kwalifikacji oraz uwzględnienia roli pracowników i ich angażowania do działań na rzecz poprawy jakości naszych usług
- Rozwoju naszej firmy na rynek globalny, a nie tylko lokalny.

Polityka bezpieczeństwa

17.1.Definicja bezpieczeństwa.

Przez bezpieczeństwo informacji w systemach IT rozumie się zapewnienie:

- Poufności informacji (uniemożliwienie dostępu do danych osobom trzecim).
- Integralności informacji (uniknięcie nieautoryzowanych zmian w danych).
- Dostępności informacji (zapewnienie dostępu do danych, w każdym momencie żądanym przez użytkownika)
- Rozliczalności operacji wykonywanych na informacjach (zapewnie przechowywania pełnej historii dostępu do danych, wraz z informacją kto

taki dostęp uzyskał).

Zarząd Firmy stosuje adekwatne do sytuacji środki aby zapewnić bezpieczeństwo informacji w Firmie.

17.2.Oznaczanie danych

Jako dane podlegające szczególnej ochronie (informacje poufne) rozumie się:

- informacje o realizowanych kontraktach (zarówno planowane, bieżące jak i historyczne),
- informacje finansowe Firmy,
- informacje organizacyjne,
- dane dostępowe do systemów IT,
- dane osobowe,
- informacje stanowiące o przewadze konkurencyjnej Firmy,
- inne informacje oznaczone jako „informacji poufne” lub „dane poufne”.

17.3.Zasada minimalnych uprawnień

W ramach nadawania uprawnień do danych przetwarzanych w systemach IT Firmy należy stosować zasadę „minimalnych uprawnień”, to znaczy przydzielać minimalne uprawnienia, które są konieczne do wykonywania pracy na danym stanowisku.

Przykładowo: pracując na komputerze PC każdy pracownik powinien posiadać tylko takie uprawnienia jakie są wymagane do realizacji swoich obowiązków (a nie na przykład uprawnienia administracyjne).

17.4.Zasada wielowarstwowych zabezpieczeń

System IT Firmy powinien być chroniony równolegle na wielu poziomach. Zapewnia to pełniejszą oraz skuteczniejszą ochronę danych.

Przykładowo: w celu ochrony przed wirusami stosuje się równolegle wiele technik: oprogramowanie antywirusowe, systemy typu firewall, odpowiednią konfigurację systemu aktualizacji Windows.

17.5.Zasada ograniczania dostępu

Domyślnymi uprawnieniami w systemach IT powinno być zabronienie dostępu. Dopiero w przypadku zaistnienia odpowiedniej potrzeby, administrator IT przyznaje stosowne uprawnienia.

Przykładowo: domyślnie dostęp do bazy przechowującej dane klientów jest zabroniony. Stosowny dostęp zostaje przyznany osobie, której zajmowane stanowisko wiąże się z koniecznością pracy w tego typu systemie.

17.6.Dostęp do danych poufnych na stacjach PC.

- Dostęp do danych poufnych w LAN realizowany jest na przeznaczonych do tego serwerach.
- Dostęp do danych poufnych (udany lub nieudany) na serwerach jest odnotowywany. Lista systemów objętych tego typu działaniami dostępna jest w osobnym dokumencie.
- Jeśli stacja PC jest komputerem przenośnym (laptopem) to musi ona być dodatkowo zabezpieczona (np. z wykorzystaniem szyfrowania dysku twardego - FDE).
- Dostęp do danych poufnych z zewnątrz firmy powinien odbywać się z wykorzystaniem kanału szyfrowanego (np. VPN, dostęp do e-mail poprzez protokół szyfrowany).
- Dostęp do danych poufnych poprzez firmową sieć WiFi powinien odbywać się z wykorzystaniem kanału szyfrowanego (np. VPN).

17.7.Zabezpieczenie stacji roboczych

- Stacje robocze powinny być zabezpieczone przed nieautoryzowanych dostępem osób trzecich.
- Minimalne środki ochrony to:
- zainstalowane na stacjach systemy typu: firewall oraz antywirus,
- wdrożony system aktualizacji systemu operacyjnego oraz jego składników,
- wymaganie podania hasła przed uzyskaniem dostępu do stacji,
- niepozostawianie niezablokowanych stacji PC bez nadzoru,
- bieżąca praca z wykorzystaniem konta nieposiadającego uprawnień administracyjnych.
- Szczegółowe informacje dotyczące korzystania ze stacji roboczych można znaleźć w stosownym dokumencie.

8. Wykorzystanie haseł

- Hasła powinny być okresowo zmieniane.
- Hasła nie mogą być przechowywane w formie otwartej (nie zaszyfrowanej).
- Hasła nie powinny być łatwe do odgadnięcia, to znaczy:
- powinny składać się z minimum 9 znaków, w tym jeden znak specjalny
- nie mogą przybierać prostych form, np. 123456789, stanislaw, dom99, hasło, Magda8, itp.
- Hasła mogą być tworzone według łączenia "losowych" (tj nie istniejących w popularnych słownikach) sylab/słów, np,: mal-tra-laza-#topa. W ten sposób można uzyskać długie hasło stosunkowo proste do zapamiętania.

17.8.Odpowiedzialność pracowników za dane poufne

Każdy pracownik odpowiada za utrzymanie w tajemnicy danych poufnych, do których dostęp został mu powierzony.

17.9.Monitoring bezpieczeństwa

W celu zapewnienia ochrony informacji Zarząd może stosować monitoring wykorzystania firmowej infrastruktury informatycznej, w szczególności obejmujący następujące elementy:

- analiza oprogramowania wykorzystanego na stacjach roboczych,
- analiza stacji roboczych pod względem wykorzystania nielegalnego oprogramowania / plików multimedialnych oraz innych elementów naruszających Prawo Autorskie,
- analiza odwiedzanych stron WWW,
- analiza godzin pracy na stanowiskach komputerowych,
- analiza wszelakich dostępów (autoryzowanych oraz nieautoryzowanych) do systemów IT będących w posiadaniu Firmy,
- Analiza ruchu sieciowego pod względem komunikacji, szkodliwej dla bezpieczeństwa danych Firmy.

Monitoring bezpieczeństwa musi odbywać się z zachowaniem obowiązującego prawa.

17.10.Edukacja pracowników w zakresie bezpieczeństwa

Firma dba o cykliczną edukację pracowników w zakresie bezpieczeństwa informacji. Pracownicy w zależności od zajmowanego stanowiska mogą uczestniczyć w szkoleniach z zakresu:

- ochrony Danych Osobowych,
- świadomości istnienia problemów bezpieczeństwa,
- szczegółowych aspektów bezpieczeństwa.

17.11.Odpowiedzialność pracowników za dane dostępowe do systemów

Każdy pracownik zobowiązany jest do ochrony swoich danych dostępowych do systemów informatycznych. Dane dostępowe obejmują między innymi takie elementy jak:

- hasła dostępowe,

- klucze softwareowe (pliki umożliwiające dostęp – np. certyfikaty do VPN) oraz sprzętowe,
- inne mechanizmy umożliwiające dostęp do systemów IT.

Przykłady ochrony danych dostępowych:

- nieprzekazywanie dostępów do systemów IT innym osobom (np. przekazywanie swojego hasła dostępowego osobom trzecim),
- nieprzechowywanie danych w miejscach publicznych (np. zapisywanie haseł dostępowych w łatwo dostępnych miejscach),
- Ochrona danych dostępowych przed kradzieżą przez osoby trzecie.

17.12.Transport danych poufnych przez pracowników

Zabrania się przenoszenia niezabezpieczonych danych poufnych poza teren Firmy. W szczególności zabrania się przenoszenia danych poufnych na nośnikach elektronicznych (np.: pendrive, nośniki CD) poza teren Firmy.

17.13.Korzystanie z firmowej infrastruktury IT w celach prywatnych

Zabrania się korzystania firmowej infrastruktury IT w celach prywatnych.

17.14.Sieć lokalna (LAN).

Sieć lokalna musi być odpowiednio chroniona przed nieuprawnionym dostępem, przykładowo:

- istotne serwery muszą być odseparowywane od sieci klienckich,
- gniazdka sieciowe dostępne publiczne muszą być nieaktywne,
- goście nie mogą uzyskiwać dostępu do sieci LAN.

Szczegółowe informacje dotyczące przyjętych metod ochrony zostały zawarte w osobnej procedurze.

17.15.Systemy IT / serwery

- Systemy IT przechowujące dane poufne (np. dane osobowe) muszą być odpowiednio zabezpieczone.
- W szczególności należy dbać o poufność, integralność i rozliczalność danych przetwarzanych w systemach.

- Szczegółowe informacje dotyczące przyjętych metod ochrony zostały zawarte w osobnej procedurze.

17.16.Dokumentowanie bezpieczeństwa

Firma prowadzi dokumentacje w zakresie:

- obecnie wykorzystywanych metod zabezpieczeń systemów IT,
- budowy sieci IT,
- ewentualnych naruszeń bezpieczeństwa systemów IT,
- dostępów do zbiorów danych / systemów udzielonych pracownikom.

Wszelkie zmiany w obszarach objętych dokumentacją, uwzględniane są w tejże dokumentacji.

17.17.Dane osobowe

Szczegółowe wytyczne dotyczące przetwarzania danych osobowych zawarte są w osobnym dokumencie.

17.18.Publiczne udostępnianie infrastruktury IT

Infrastruktura udostępniona publicznie musi być szczególnie zabezpieczona. Przykładowe środki bezpieczeństwa:

- Separacja od sieci LAN (np. z wykorzystaniem strefy DMZ)
- Wykonanie hardeningu systemu (zwiększenia bezpieczeństwa oferowanego domyślne przez system)
- Wewnętrzna lub zewnętrzna weryfikacja bezpieczeństwa systemu (np. poprzez realizację testów penetracyjnych)

17.19.Kopie zapasowe.

- Każde istotne dane (w tym dane poufne) powinny być archiwizowane na wypadek awarii w firmowej infrastrukturze IT.
- Nośniki z kopiami zapasowymi powinny być przechowywane w miejscu uniemożliwiającym dostęp osobom nieupoważnionym.
- Okresowo kopie zapasowe muszą być testowane pod względem rzeczywistej możliwości odtworzenia danych.

17.20.Dostęp do systemów IT po rozwiązaniu umowy o pracę

W przypadku rozwiązania umowy o pracę z pracownikiem, dezaktywowane są wszelakie jego dostępy w systemach IT.

17.21.Naruszenie bezpieczeństwa

Wszelakie podejrzenia naruszenia bezpieczeństwa danych w Firmie należy zgłaszać w formie ustnej lub za pośrednictwem poczty elektronicznej do Zarządu Spółki.

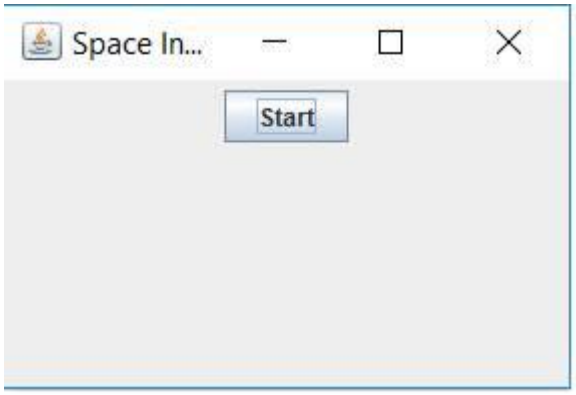
Każdy incydent jest odnotowywany w stosownej bazie danych, a Zarząd Firmy podejmuje stosowne kroki zaradcze.

17.22.Weryfikacja przestrzegania polityki bezpieczeństwa.

Zarząd okresowo wykonuje wewnętrzny lub zewnętrzny audyt bezpieczeństwa mający na celu wykrycie ewentualnych uchybień w realizacji założeń polityki bezpieczeństwa.

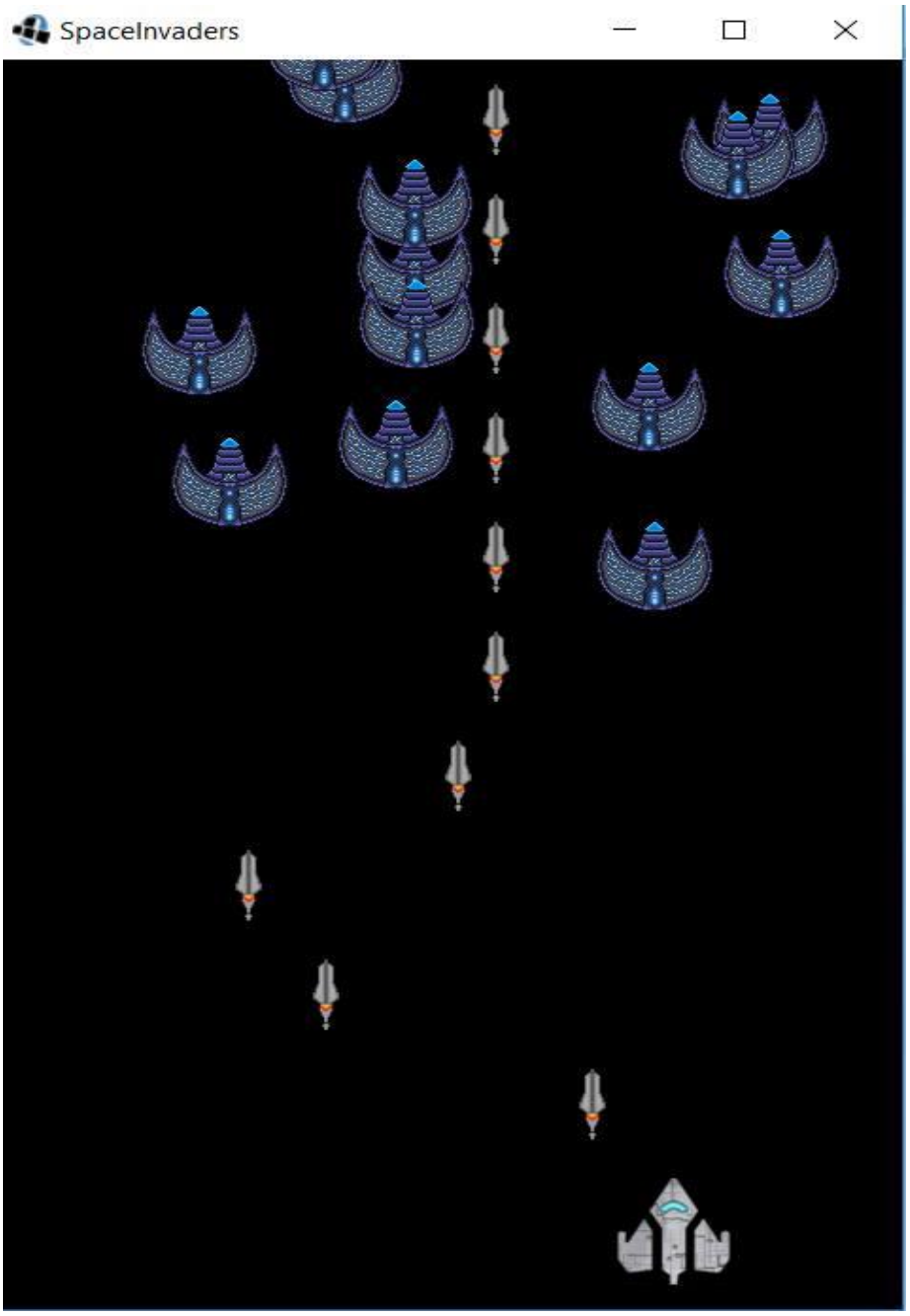
18. Instrukcja Obsługi

18.1 Główne okno programu



W głównym oknie programu należy nacisnąć przycisk „Start”, który wywoła uruchomienie gry.

18.2 Okno Gry



Poruszanie się w grze umożliwiają klawisze „A – w lewo” „D – w prawo” bądź myszką.