

SCENARIUSZ ZAAWANSOWANEGO E-MATERIAŁU

1. Metryczka materiału

Tytuł materiału	Cyberwojna
Numer materiału	I.6
Autor scenariusza	Artur Derdziak
Weryfikacja WCAG	Zespół ekspertów ds. WCAG (Dominika Gaponiuk, Agnieszka Brodowska, Urszula Grygier, Łukasz Mroziński)
Weryfikacja założeń techniczno-informatycznych	Zespół informatyków ds. integrowania e-materiałów pod względem technologicznym (Paweł, Tomaszek, Katarzyna Gagan, Anna Magdziarz-Tomaszek, Grzegorz Kusztełak)
Weryfikacja językowa	Angelika Wiśniewska
Rodzaj multimedium	gra karciana z wykorzystaniem AI
Wykorzystanie AR lub VR <small>AR - rozszerzona rzeczywistość VR - wirtualna rzeczywistość</small>	standardowa 2D lub 3D <input type="checkbox"/> AR <input type="checkbox"/> VR
Etap(y) edukacyjny(e), dla których przeznaczony jest materiał	III etap: Liceum / technikum zakres podstawowy Liceum / technikum zakres rozszerzony
Przedmiot(y), do nauki których przeznaczony jest materiał	edukacja dla bezpieczeństwa edukacja obywatelska informatyka wiedza o społeczeństwie

2. Opis materiału

Skrócony opis materiału (abstrakt)
<p>Cyberwojna to interaktywna gra karciana, przeznaczona dla 2–6 graczy, umożliwiająca rozgrywkę multiplayer zarówno lokalnie, jak i online. Gra łączy elementy strategicznego planowania, taktycznych ataków i obrony oraz działań dyplomatycznych i szpiegowskich. Celem każdego gracza jest zbudowanie i ochrona własnego państwa, co wymaga umiejętnego wykorzystywania kart instytucji i skutecznej obrony przed cyberatakami i działaniami przeciwników.</p> <p>W grze dostępne są różnorodne karty, w tym:</p> <ul style="list-style-type: none"> • ataki hakerskie: umożliwiają cyberataki na przeciwników (np. DDoS, phishing, wycieki danych); • obrona cybernetyczna: zapewniają ochronę poprzez systemy, takie jak firewalle czy szyfrowanie; • rozwój technologiczny: pozwalają inwestować w nowe technologie, wzmacniając możliwości ataku i obrony;



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



<ul style="list-style-type: none"> • dyplomacja i szpiegostwo: umożliwiają nawiązywanie sojuszy, działania wywiadowcze oraz sabotowanie przeciwników. <p>Gra oferuje różne poziomy trudności, system odpowiedzi oraz osiągnięć, a także edukacyjną integrację z systemem EDUchat, co pozwala nauczycielom dostosować treści do potrzeb uczniów.</p>
<p>Cel ogólny materiału</p>
<p>Celem gry jest zgromadzenie maksymalnej liczby punktów zwycięstwa poprzez strategiczne wykorzystanie kart, osiągnięcie przewagi nad przeciwnikiem i uniknięcie cyberataków. Gra oferuje graczom możliwość doświadczenia cyberwojny w interaktywny i strategiczny sposób. Uczeń przy okazji zabawy w grę karcianą pozna różne rodzaje ataków hakerskich zaliczanych do cyberwojny oraz sposoby ich zwalczania.</p>
<p>Cele z podstawy programowej kształcenia ogólnego możliwe do realizacji za pomocą materiału</p>
<p>Wiedza o społeczeństwie Uczeń: wyjaśnia pojęcie cyberwojny i podaje przykłady takich konfliktów (ataki hakerskie: phishing, DoS, DNS Spoofing, Ransomware, atak man in the middle) oraz przykłady stosowanej obrony (segmentacja sieci, szyfrowanie danych, firewall, oprogramowanie antywirusowe).</p> <p>Edukacja obywatelska Uczeń: - identyfikuje najważniejsze problemy globalne; - wyjaśnia przyczyny wybranego konfliktu międzynarodowego (także w kontekście zasad prawa międzynarodowego), identyfikuje jego konsekwencje oraz ocenia próby jego rozwiązania.</p> <p>Edukacja dla bezpieczeństwa Uczeń: - wyjaśnia znaczenie cyberzagrożeń w wymiarze cywilnym i potrafi je rozpoznać. Zna zasady identyfikacji podstawowych zagrożeń cyberbezpieczeństwa. Potrafi odbierać ze zrozumieniem, tworzyć i przedstawiać złożone wypowiedzi dotyczące roli i miejsca cyberbezpieczeństwa militarnego w systemie cyberbezpieczeństwa państwa.</p> <p>Informatyka Uczeń: - opisuje szkody, jakie mogą spowodować działania pirackie w sieci, w odniesieniu do indywidualnych osób, wybranych instytucji i całego społeczeństwa.</p>

3. Charakterystyka materiału

<p>Opis zawartości merytorycznej materiału</p>
<p>Elementy gry:</p> <p>Plansza wprowadzająca do gry z tytułem: <i>Cyberwojna</i> ma posiadać rozwiązania graficzne i opis, czym jest cyberwojna.</p> <p><u>Rodzaje kart:</u></p>



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



- 1)Karty reprezentujące państwo: instytucje takie jak banki, sektor energetyczny, służba zdrowia, edukacja, rząd.
 - 2)Ataki hakerskie: karty, które pozwalają na przeprowadzenie cyberataku na przeciwnika, takiego jak DDoS, phishing lub wycieki danych.
 - 3)Obrona cybernetyczna: karty, które wzmacniają systemy obronne gracza, takie jak firewalle, systemy wykrywania intruzów i szyfrowanie danych.
 - 4)Sabotaż komputerowy: karty specjalne, zwiększające możliwości ataku i obrony.
- Instytucje mają posiadać opis, dlaczego są zagrożone atakami hakerskimi, pozostałe mają posiadać opis, na czym polega dany atak, obrona czy sabotaż.

Kluczowe wymagania merytoryczne i dydaktyczne dla Wykonawcy materiału, które muszą zostać uwzględnione

Kluczowym wymaganiem jest ukazanie różnych aspektów cyberwojny. Materiał ma prezentować ataki hakerskie: phishing, DoS, DNS Spoofing, Ransomware, atak Man in the Middle oraz przykłady stosowanej obrony cybernetycznej: segmentacja sieci, szyfrowanie danych, firewall, oprogramowanie antywirusowe.

Pod względem dydaktycznym materiał ma mieć charakter samokształceniowy połączoną z zasadą aktywności opartą nie tylko na poznawaniu i utrwalaniu informacji zawartych na kartach gr, ale także na podejmowaniu logicznych i samodzielnych działań w celu zabezpieczenia się przed zagrożeniami cybernetycznymi.

Opis struktury treści materiału

Gra karciana dla 2 do 6 graczy, w której należy zbudować własne państwo, jednocześnie broniąc je przed atakami hakerskimi, zniszczeniem lub sabotażem instytucji przez przeciwników. Graczami mogą być inne osoby lub AI. W przypadku braku AI, grę można rozegrać tylko w przypadku, kiedy będą grały co najmniej 2 osoby.

68 kart - w tym w pięciu kolorach + karty wielokolorowe: każda karta ma swoją nadrzędną nazwę i tytuł.

Rodzaje i liczba kart:

a) karty reprezentujące państwo:

- 5 kart koloru czerwonego: banki i instytucje finansowe (na karcie budynek reprezentujący tę instytucję i krótki opis dlaczego są zagrożone cyberprzestępczością);
- 5 kart koloru zielonego: sektor energetyczny (na karcie budynek reprezentujący tę instytucję i krótki opis, dlaczego jest zagrożony cyberprzestępczością);
- 5 kart koloru niebieskiego: edukacja i badania (na karcie budynek reprezentujący tę instytucję i krótki opis, dlaczego jest zagrożony cyberprzestępczością);
- 5 kart koloru żółtego: ochrona zdrowia (na karcie budynek reprezentujący tę instytucję i krótki opis, dlaczego jest zagrożony cyberprzestępczością);
- 1 karta wielokolorowa: administracja publiczna i rząd (na karcie budynek reprezentujący tę instytucję i krótki opis, dlaczego jest zagrożony cyberprzestępczością).

b) karty reprezentujące ataki hakerskie:

- 4 karty czerwonych: phishing (na karcie obrazek reprezentujący ten atak i jego krótki opis);



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



- 4 karty koloru zielonego: DoS (na karcie obrazek reprezentujący ten atak i jego krótki opis);
 - 4 karty koloru niebieskiego: DNS Spoofing (na karcie obrazek reprezentujący ten atak i jego krótki opis);
 - 4 karty koloru żółtego: Ransomware (na karcie obrazek reprezentujący ten atak i jego krótki opis);
 - 1 karta wielokolorowa: atak Man in the Middle (na karcie obrazek reprezentujący ten atak i jego krótki opis).
- c) karty reprezentujące obronę cybernetyczną:**
- 4 karty koloru czerwonego: segmentacja sieci - (na karcie obrazek reprezentujący obronę i jej krótki opis);
 - 4 karty koloru zielonego: szyfrowanie danych (haszowanie)-(na karcie obrazek reprezentujący obronę i jej krótki opis);
 - 4 karty koloru niebieskiego: firewall (zapora sieciowa), (na karcie obrazek reprezentujący obronę i jej krótki opis);
 - 4 karty koloru żółtego: oprogramowanie antywirusowe, (na karcie obrazek reprezentujący obronę i jej krótki opis);
 - 4 karty wielokolorowe: sieć VPN - (na karcie obrazek reprezentujący obronę i jej krótki opis).
- d) karty specjalne w kolorze fioletowym z ogólną nazwą *Sabotaż komputerowy*:** Karty sabotażu pomagają zwyciężyć poprzez modyfikacje rozgrywki. Można ich użyć dla własnej korzyści lub w celu powstrzymania przeciwników przed skompletowaniem ich państw, zanim gracz skompletuje swoje. Karty te mają natychmiastowy efekt, a po użyciu odkłada się je na stos kart odrzuconych:
- **2 karty** zatytułowane - ***Szpiegostwo przemysłowe*** (na karcie obrazek reprezentujący to działanie i jego krótki opis). Tą kartą można zamienić wybraną instytucję państwa pomiędzy dwoma graczami. Nie ma znaczenia, czy instytucje państwa są tego samego koloru, czy są zabezpieczone jedną kartą obrony cybernetycznej, czy są zaatakowane jedną kartą ataku hakerskiego, czy też nie są wobec nich podjęte żadne działania. Gracz zamienia wybraną instytucję z innym graczem. Nie wolno tylko innemu graczowi odebrać karty reprezentującej instytucję państwa zabezpieczonej dwoma kartami obrony cybernetycznej (taka instytucja jest już uodporniona) oraz doprowadzić do sytuacji, że przeciwnik będzie posiadał dwie karty tego samego koloru reprezentujące instytucje państwowe.
 - **3 karty** zatytułowane ***Wyciek danych*** (na karcie obrazek reprezentujący to działanie i jego krótki opis). Taką kartą można ukraść kartę instytucji państwowej z państwa innego gracza i umieścić ją w swoim państwie. Można skraść każdą instytucję niezabezpieczoną, zabezpieczoną lub zaatakowaną, nie można jedynie ukraść instytucji uodpornionej dwoma kartami obrony cybernetycznej. Nie można też ukraść instytucji o tym samym kolorze, którą mamy już w swoim państwie tego samego koloru.
 - **3 karty** zatytułowane ***Kontrola dostępu*** (na karcie obrazek reprezentujący obronę i jej krótki opis). Za pomocą tej karty można przenieść tyle ataków hakerskich, ile można ze swoich instytucji państwowych na instytucje innych graczy. Nie można użyć tej karty na zabezpieczone lub zaatakowane już instytucje. Atakować można tylko te instytucje, wobec których nie podjęto żadnych działań.
 - **2 karty** zatytułowane ***DDoS*** (na karcie obrazek reprezentujący atak i jego krótki opis) Wszyscy gracze, oprócz posiadacza tej karty, odrzucają karty z ręki na stos kart odrzuconych. W swojej turze gracze ci przechodzą od razu do fazy 2. gry, czyli dobierają 3 karty.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Mechanika materiału

Gracze zgodnie ze wskazówkami zegara wykładają po jednej posiadanej karcie w celu podjęcia działania wobec wybranego przeciwnika lub zabezpieczenia własnego państwa. Po wyłożeniu karty uzupełniają zestaw ze wspólnego stosu kart. Mogą podjąć decyzję o rezygnacji z wyłożenia karty w ich kolejce, ale wtedy muszą odrzucić od 1 do 3 kart, które posiadają.

Przygotowanie:

Komputer tasuje karty i rozdaje każdemu z graczy po 3 karty. Pozostała część talii leży na planszy rewersem do góry w zasięgu wszystkich graczy. Obok będzie się znajdował stos kart odrzuconych przez gracza. Gdy talia wyczerpie się, następuje odwrócenie stosu kart odrzuconych. Nie trzeba go tasować i on stanowi teraz talię.

Cel gry:

Należy skompletować państwo. Aby państwo było kompletne, należy zebrać 4 różne karty reprezentujące instytucje państwowe, każda w innym kolorze. W momencie, gdy gracz położy przed sobą 4 różne, pozbawione ataków hakerskich, instytucje państwowe wygrywa.

Rozgrywka:

Wszyscy gracze na początku każdej rundy muszą mieć po 3 karty na ręce. Wolno im wykonać tylko 1 akcję na rundę. Po każdej rundzie gracze dobierają karty z talii, aby uzupełnić rękę do 3 kart. Zagrywają karty każdego rodzaju przed sobą, aby budować swoje państwo lub zagrywają je na karty przeciwników, aby powstrzymać ich przed skompletowaniem własnego państwa przed graczem. Jeżeli gracz nie ma karty, którą mógłby zagrać musi odrzucić co najmniej jedną z kart, które posiada i dobrać kolejną ze stosu. Niektóre karty mogą spowodować, że gracz będzie musiał odrzucić lub wymienić swoje instytucje państwowe, obronę cybernetyczną lub nawet wszystkie karty z ręki.

W przypadku remisu decyduje np. liczba zebranych punktów lub czas ukończenia gry.

Fazy gry:

FAZA 1. Wybierz jedną z dwóch akcji: ZAGRAJ lub ODRZUĆ

W każdej turze zagraj tylko jedną kartę z ręki - lub- Odrzuć tyle kart, ile chcesz.

FAZA 2. DOBIERZ

Dobierz tyle kart, aby mieć na ręce 3.

FAZA 3. ZAKOŃCZ TURĘ

Następuje tura kolejnego gracza.

Szczegółowe zasady rozgrywki i zwycięstwa:

Aby zwyciężyć, należy zbierać 4 niezaatakowane żadnym atakiem hakerskim instytucje państwa, każdą w innym kolorze. W żadnym momencie gry państwo gracza nie może posiadać 2 takich samych instytucji (kolorów). **Uwaga:** Państwo może mieć 5 różnych instytucji, jeżeli jedna z nich, to wielokolorowa karta. Gracz wygrywa, jeżeli 4 z nich będą pozbawione ataków hakerskich.

Wygrywające karty mogą być puste, zabezpieczone jedną obroną cybernetyczną lub uodpornione dwoma obronami cybernetycznymi. Wszystkie karty państwa atakujemy i zabezpieczamy kartami tego samego koloru co karta państwa. Wyjątkiem jest karta wielokolorowa, reprezentująca administrację publiczną i rząd. Można ją zaatakować każdym dowolnym kolorem i obronić każdym kolorem karty obrony cybernetycznej. Podobnie każdym kolorem można zniszczyć leżącą na niej kartę obrony cybernetycznej. Zniszczyć tę kartę można dwoma dowolnymi kartami reprezentującymi ataki hakerskie i tak samo ją uodpornić dwoma dowolnymi kartami obrony cybernetycznej

Na przykład:

1. Karta wielokolorowa została zaatakowana czerwoną kartą hakerską, gracz na tę kartę wyklada żółtą obronę cybernetyczną. Karta państwa pozostaje na planszy, a karta ataku i obrony wraca do puli kart odrzuconych.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



2. Karta wielokolorowa została zaatakowana czerwoną kartą hakerską, kolejny gracz zaatakował tę kartę żółtą kartą hakerską. Karta państwa zostaje zniszczona, zdjęta z planszy wraz z dwiema kartami ataku i trzy karty wracają do puli kart odrzuconych.
3. Karta wielokolorowa została zabezpieczona czerwoną kartą obrony, inny gracz na tę kartę wyklada niebieski atak. Karta państwa pozostaje na planszy, a karty ataku i obrony wracają do puli kart odrzuconych.
4. Karta wielokolorowa została zabezpieczona czerwoną kartą obrony, nikt jej nie zaatakował i w kolejnej rundzie gracz na tę kartę wyklada niebieską kartę obrony. Karta państwa pozostaje na planszy jako karta uodporniona wraz z dwiema kartami obrony do końca gry. Nie można jej nic zrobić.

Karty kolorowe mogą być atakowane i broniące tylko tym samym kolorem:

np: karta czerwona reprezentująca instytucję państwa może być atakowana tylko czerwonym atakiem hakerskim i bronią czerwoną obroną. Aby ją uodpornić, trzeba na niej położyć dwie czerwone karty obrony cybernetycznej.

Odstępstwem od tej reguły jest wielokolorowa karta ataku hakerskiego, którą można zastosować wszędzie i w każdym momencie, zastępuje ona w tym momencie dany kolor, zniszczyć ją jednak można każdym kolorem karty obrony cybernetycznej lub kartą wielokolorową obrony cybernetycznej. W przypadku wielokolorowej karty obrony cybernetycznej jej zastosowanie jest analogiczne do wielokolorowej karty ataku hakerskiego.

Karta kolorowa państwa zabezpieczona dwoma tego samego koloru obronami cybernetycznymi lub jedną tego samego koloru, a drugą wielokolorową lub dwiema wielokolorowymi jest uodporniona. Karta kolorowa państwa, na którą zostaje położona druga karta ataku hakerskiego, zostaje zdjęta z planszy i wraz z dwiema kartami ataku wraca do puli kart odrzuconych.

Karty ataku hakerskiego:

1. Atakują pustą kartę reprezentującą kartę państwa (jedna karta).
2. Niszczą kartę reprezentującą państwa (położenie drugiej karty ataku hakerskiego skutkuje zdjęciem trzech kart z planszy i wszystkie karty trafiają do puli kart odrzuconych).
3. Niszczą obronę cybernetyczną (na karcie państwa leży jedna karta obrony cybernetycznej, położenie na niej jednej karty ataku powoduje zniszczenie obrony - karty obrony i ataku zostają zdjęte i trafiają do puli kart odrzuconych, a na planszy zostaje pusta karta reprezentująca instytucję państwa).

Karty obrony cybernetycznej:

1. Zabezpieczają pustą kartę reprezentującą kartę państwa (jedna karta).
2. Uodporniają kartę reprezentującą państwa (położenie drugiej karty obrony cybernetycznej skutkuje pozostaniem wszystkich kart na planszy do końca gry).
3. Niszczą atak hakerski (na karcie państwa leży jedna karta ataku, położenie na niej jednej karty obrony powoduje zniszczenie ataku - karta obrony i ataku zostają zdjęte i trafiają do puli kart odrzuconych, a na planszy zostaje pusta karta reprezentująca instytucję państwa).

Wykorzystanie sztucznej inteligencji (AI):

1. AI dynamicznie dostosowuje poziom trudności na podstawie stylu gry gracza.
2. AI może grać różnymi stylami (np. agresywny atakujący vs. defensywny).
3. AI może zmieniać strategię w zależności od decyzji gracza.
4. AI może mieć różne style gry:
 - *Agresywny cyberprzestępca* – AI, które koncentruje się na ataku.
 - *Obrońca państwa* – AI, które buduje silne mechanizmy obronne.
 - *Szpieg* – AI, które częściej stosuje karty sabotażu i szpiegostwa.
5. AI może sugerować możliwe ruchy i tłumaczyć konsekwencje podjętych decyzji (np. *Jeśli użyjesz tej karty, twoja obrona osłabnie*).
6. EDUchat generuje raporty podsumowujące strategię gracza.
7. AI informuje gracza o zmianach poziomu trudności.

System punktacji i nagród:



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



1. Gracz zdobywa punkty w zależności od swoich działań w grze. Każda akcja ofensywna, defensywna i strategiczna wpływa na wynik końcowy. W grze dostępne są również osiągnięcia, które nagradzają określone style gry, np.:
 - Cyberobronca – wygraj grę bez utraty żadnej instytucji.
 - Cyberatak doskonały – wyeliminuj wszystkich przeciwników atakami hakerskimi.
 - Mistrz dyplomacji – wygraj grę bez użycia kart ataku.
 - Szybka odpowiedź – pokonaj przeciwnika w mniej niż 10 tur.
2. Po zakończeniu gry gracz otrzymuje raport podsumowujący punkty oraz zdobyte osiągnięcia.

Grafika

Kolorystyka i grafika – dopasowane do docelowej grupy wiekowej, przyjazne, z wyraźnym kontrastem. Tło na ekranie startowym z elementami graficznymi nawiązującymi do cyberwojny i nowoczesnych technologii.

Postacie przy stole: Rysunkowe postacie symbolizujące różne państwa siedzące przy stole, przy którym odbywa się gra. Każda postać może mieć akcenty graficzne związane z jej krajem. Postacie siedzą naprzeciw siebie tworząc klimat interaktywnej rozgrywki przy stole.

Stół z kartami: Na stole widoczne są wyłożone karty każdego gracza, w tym karty instytucji oraz aktywne karty ataku i obrony. Karty będą dobrze widoczne, zróżnicowane kolorystycznie, z prostymi symbolami i rysunkowymi grafikami zależnie od rodzaju karty i ich funkcji, np. instytucje, ataki, obrony.

Pasek kart gracza: Na dolnej części ekranu znajduje się osobisty pasek kart dla każdego gracza. Każdy gracz może tam zobaczyć swoje karty na ręce. Karty w tym pasku są wyraźnie widoczne i łatwo rozpoznawalne, z ikonami, krótkimi nazwami i grafiką odpowiadającą ich funkcji (np. ikona zamku na karcie obrony lub ikona wirusa na karcie ataku hakerskiego).

Dodatkowe efekty graficzne:

1. Efekty wizualne na kartach –karty z aktywnymi efektami (jak atak lub obrona) będą mieć specjalne animacje lub symbole, np. zaatakowana instytucja może być pokryta czerwonym symbolem ostrzegawczym, a broniona instytucja może mieć małą tarczę.
2. Wizualizacja akcji specjalnych – w przypadku użycia karty specjalnej (sabotaż, szpiegostwo) pojawia się animacja lub efekt graficzny, np. dymek z informacją o wykonanej akcji lub rysunkowy efekt, taki jak złamany symbol tarczy przy sabotowanej instytucji.

Przykładowe inspiracje

Mechanika gry:

- *Hearthstone* – dynamiczna gra karciana z intuicyjnym interfejsem.
- *Exploding Kittens* – prosta mechanika kart w połączeniu z humorystycznym stylem.
- *Terraforming Mars* – strategia oparta na kartach z różnymi efektami.
- *Wirus* – gra karciana o prostej mechanice, z dynamicznymi interakcjami między graczami i szybkim tempem rozgrywki, idealna do adaptacji w kontekście edukacyjnym.

Styl graficzny i UX:

- *Cyberpunk 2077* (interface) – cybernetyczny, nowoczesny wygląd.
- *Clash Royale* – czytelny pasek kart i animacje wskazujące aktywne efekty.

Edukacyjne aspekty:



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



- *Papers, Please* – narracja edukacyjna oparta na dynamicznych decyzjach.
- *Plague Inc.* – przystępne wyjaśnienie złożonych procesów poprzez grywalizację.

Tryb multiplayer:

- *Among Us* – łatwy w obsłudze system dołączania do gry online.
- *Catan Universe* – gra planszowa zaadaptowana do trybu multiplayer z AI.

4. Wymagania WCAG

Opis dostosowania materiału celem spełnienia standardu WCAG

Zaawansowany e-materiał musi uwzględniać założenia uniwersalnego projektowania w edukacji (UDL) oraz być zgodny ze standardami dostępności cyfrowej WCAG obowiązującymi na dzień ogłoszenia naboru, standardem ATAG 2.0 oraz zapisami ustawy z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami (Dz. U. z 2019 r. poz. 1696) i ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz. U. z 2019 r. poz. 848). Powinien też uwzględniać dobre praktyki, stosowane w celu zapewnienia wysokiej jakości dostępnych cyfrowo materiałów edukacyjnych.

Użytkownik ze szczególnymi potrzebami, korzystający z przygotowanego zaawansowanego e-materiału, powinien korzystać z mechaniki materiału (menu nawigacyjnego) w taki sam sposób, jak wszyscy użytkownicy. Należy przygotować menu, w którym wybiera on dostosowania materiału do swoich potrzeb. W ramach wybranych dostosowań zaawansowanego e-materiału użytkownik powinien korzystać ze wszystkich zaprojektowanych funkcjonalności. Zaawansowany e-materiał powinien spełniać kryteria dostępu dla technologii dotykowych (np. ekranów dotykowych), dostępności z poziomu klawiatury czy za pomocą zewnętrznych urządzeń wejściowych (np. mysz powiększona), technologii asystujących (np. czytniki ekranu). Poszczególne ułatwienia dostępu oraz ich konfiguracja powinny być dostępne w menu przed uruchomieniem aplikacji. Powinna istnieć również możliwość zapamiętania wybranych przez użytkownika ustawień, tak aby mogła być stosowana przy kolejnych uruchomieniach aplikacji przez użytkownika.

Zaawansowany e-materiał powinien spełniać następujące kryteria:

1. umożliwiać użytkownikowi z różnymi potrzebami korzystać z ułatwień dostępu, na wszystkich poziomach i etapach e-materiału;
2. posiadać instrukcję dla użytkowników z różnymi potrzebami, zawierającą informacje o sposobie korzystania z ułatwień dostępu i mechanizmach poruszania się po menu, przygotowaną za pomocą tzw. prostego języka;
3. posiadać rozwiązania z zakresu dostępności, które pozwalają uniknąć QTE lub działań związanych z łączeniem przycisków (uwzględnia ustawienie pozwalające je uprościć lub pominąć/wyłączyć);
4. umożliwiać korzystanie z wirtualnej klawiatury ekranowej (jeśli materiał tego wymaga), którą można sterować za pomocą myszy lub technologii wspomagających, takich jak wzrok lub przełącznik;
5. umożliwiać skorzystanie z pomocy w sytuacjach potencjalnie trudnych, związanych z poruszaniem się po materiale;
6. użytkownik przed skorzystaniem z zaawansowanego e-materiału powinien mieć możliwość zapoznania się tutorialiem objaśniającym, jak korzystać z ułatwień dostępu;
7. mechanika zaawansowanego e-materiału powinna pozwalać na dostęp do wszystkich obszarów interfejsu użytkownika;
8. zaawansowany e-materiał powinien być dostępny za pomocą technologii asystujących,



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



m.in. czytników ekranu, oprogramowania asystującego w technologiach mobilnych.

Jeżeli w materiale będą występowały treści nieinterpretowalne przez technologie asystujące, wykonawca zobowiązany jest zapewnić alternatywę wchodzącą w e-materiał i stanowiącą integralną całość zaawansowanego e-materiału. Bez konsultacji z ekspertami ORE nie dopuszcza się tworzenia alternatywnego (równoległego rozwiązania) dedykowanego osobom z różnymi potrzebami.

Zaawansowany e-materiał musi uwzględniać między innymi potrzeby osób:

- z ograniczeniami wzroku,
- z ograniczeniami słuchu,
- z ograniczeniami ruchu rąk i mobilności,
- z ograniczeniami możliwości poznawczych (związanymi z np. pamięcią, przetwarzaniem informacji, dysleksją),
- zaburzeniami neurorozwojowymi i psychicznymi (np. spektrum autyzmu, ADHD, stanami lękowymi, epilepsją),
- z zaburzeniami mowy,
- korzystających z czytników ekranu.

Podczas projektowania e-materiału należy uwzględniać różne potrzeby i możliwości użytkowników ze względu na:

Ograniczenia wzroku:

- stosowanie dobrze kontrastujących kolorów, czytelnych rozmiarów i typów fontów, możliwość zmiany i indywidualnego dopasowania przez użytkownika tych elementów;
- stosowanie zawsze widocznego fokusa (przynajmniej częściowo);
- używanie kombinacji koloru, kształtów i tekstu, niestosowanie znaczenia tylko kolorem;
- umieszczanie przycisków i powiadomień w kontekście;
- stosowanie odpowiedniej wielkości, kolorów i rozmieszczenia elementów interfejsu;
- umożliwienie zmiany kolorów dla osób będących daltonistami;
- umożliwienie zmiany wielkości elementów interfejsu;
- używanie dźwięku przestrzennego i rozróżnialnych dźwięków, różnych w zależności od zdarzeń;
- umożliwienie wyboru wyglądu kursora/celownika, zmiany kształtu, wielkości, koloru, jeśli projektowana mapa interaktywna zakłada bardzo dużo obiektów;
- wyświetlanie istotnych informacji w centrum, na linii wzroku lub możliwość powiększania całości, poszczególnych elementów mapy interaktywnej;
- nawigacja i sterowanie za pomocą klawiatury;
- stosowanie tekstów alternatywnych lub audiodeskrypcji do grafik;
- elementy materiału powinny być duże i łatwe do odróżnienia oraz oddalone od siebie;
- dodanie opisów alternatywnych do obrazów i innych elementów wizualnych, które opisują treści lub funkcje;
- stosowanie dużego kontrastu między istotnymi elementami w materiale;
- użytkownicy niewidomi powinni móc skorzystać z każdej funkcjonalności materiału z poziomu klawiatury.

Ograniczenia słuchu:

- stosowanie prostego języka, niestosowanie figur stylistycznych i idiomów;
- zapewnienie alternatywy tekstowej każdej kluczowej informacji dźwiękowej;
- dodanie napisów i transkrypcji do treści audio i wideo;
- możliwość modyfikacji napisów, zmiana rozmiaru/koloru oraz ich włączania i wyłączania zanim pojawi się dźwięk;
- stosowanie napisów rozszerzonych informujących o dodatkowych dźwiękach i nastroju



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



- oraz postaci mówiących;
- stosowanie prostych logicznych i spójnych układów treści;
- zapewnienie możliwości osobnej regulacji dźwięku dla różnych elementów multimedialnych w mapie interaktywnej;
- zastosowanie przełącznika dźwięku mono/stereo w materiałach filmowych i audio (jeśli takie się pojawią w zaawansowanym materiale).

Ograniczenia ruchu rąk i mobilności:

- umożliwienie w menu materiału ustawienia dużych obszarów klikalnych;
- projektowanie obsługi za pomocą klawiatury i mowy;
- unikanie tworzenia dynamicznych treści, wymagających dużego ruchu myszy;
- nieograniczanie czasu otwarcia okien, wykonania zadań;
- zapewnienie alternatywy dla akcji, wymagających równoczesnych czynności (np. klik zamiast przeciągnij i upuść);
- zapewnienie sterowania przy użyciu prostych kontrolerów;
- unikanie stosowania bardzo precyzyjnych ruchów.

Ograniczenia poznawcze oraz zaburzenia neurorozwojowe i psychiczne:

- używanie prostych, stonowanych barw;
- używanie prostego języka, bez stosowania figur stylistycznych i idiomów;
- używanie krótkich zdań i punktowania;
- używanie wyjaśnienia skrótów;
- tworzenie opisowych przycisków;
- budowanie prostych i spójnych układów treści;
- wyrównanie tekstów do lewej i zachowanie spójnego układu;
- niestosowanie dużych bloków ciężkiego tekstu;
- niestosowanie podkreślania słów, niepochylenia tekstu i pisanie wielkimi literami;
- umożliwienie zmiany kontrastu pomiędzy tłem a tekstem;
- niestosowanie ograniczenia czasowego na wykonanie zadania;
- niestosowanie presji czasowej lub związanej z możliwością wykonania tylko jednej próby wykonania zadania.

Ograniczenia związane z korzystaniem z czynników ekranów:

- opisywanie obrazów, stosownie transkrypcji, audiodeskrypcji;
- nieumieszczanie informacji tylko na obrazie lub wideo;
- nadawanie struktury treści i nieoznaczanie jej tylko rozmiarem i rozmieszczeniem tekstu;
- stosowanie liniowego logicznego układu;
- umożliwienie sterowania za pomocą klawiatury;
- tworzenie opisowych łączy.

Powyższe wytyczne są jedynie przykładami potrzeb, jakie powinny zostać spełnione przy projektowaniu zaawansowanego e-materiału. Beneficjent konkursowy powinien zapewnić możliwie największą dostępność dla osób z różnymi potrzebami. Rozwiązania związane z zapewnieniem dostępności osobom z różnymi potrzebami Beneficjent konkursowy powinien konsultować z ekspertami ORE na poszczególnych etapach realizacji projektu konkursowego.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



5. Wymagania funkcjonalne i techniczne

Kluczowe warunki funkcjonalne dla Wykonawców

Aplikacja musi spełniać wymagania określone w dokumencie „Ogólne wymagania funkcjonalne i techniczne dla e-materiałów”.

Ekran startowy

- **Opcje gry:**
 - Tryb gry: Singleplayer (gra z AI) lub multiplayer (lokalnie i online) z możliwością tworzenia pokoi lub losowego dobierania graczy..
 - Liczba graczy: od 2 do 6, z możliwością dodania AI jako przeciwników lub sojuszników.
 - Można wyłączyć lub ustawić limit czasu na turę (np. 30-60 sekund)
 - Poziom trudności: dostosowanie gry do umiejętności graczy. AI może mieć różne poziomy trudności.

Interakcja i system podpowiedzi

- **System podpowiedzi:**
 - Podpowiedzi kontekstowe wyświetlane na bieżąco w trakcie gry, dostosowane do poziomu zaawansowania gracza.
 - Wsparcie dla graczy początkujących, np. oznaczanie możliwych ruchów na planszy.
 - EDUchat generuje wskazówki dotyczące strategii, takich jak najlepszy ruch na podstawie aktualnej sytuacji w grze.
- **Interakcje:**
 - Aktywne informacje zwrotne: Komunikaty o skuteczności działań gracza (np. *Instytucja została skutecznie obroniona*).
 - Reakcje wizualne na ruchy gracza i efekty kart (np. animacje ataków lub obrony).

System punktacji i nagród

- Gra powinna zawierać system nagród i osiągnięć, który motywuje graczy do stosowania różnych strategii.
- Punkty są przyznawane za skuteczne akcje ofensywne, defensywne i dyplomatyczne.
- Po zakończeniu gry gracz otrzymuje podsumowanie wyników oraz odznaki za wyjątkowe osiągnięcia.
- System nagród jest zintegrowany z EDUchat, który analizuje wyniki i sugeruje sposoby poprawy strategii.

Nawigacja i eksploracja świata gry

- **Interaktywna mapa gry:**
 - W grach z większym światem wirtualnym dostępna minimapa z oznaczeniem kluczowych punktów.
 - Przejrzysty podział planszy na obszary dla każdego gracza.
- **Nawigacja:**
 - Intuicyjny interfejs z oznaczeniami pól, kart i działań dostępnych dla gracza.
 - Możliwość przewijania instrukcji i podglądu zasad gry w dowolnym momencie.

Śledzenie postępów



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



- **Zapisywanie i wznowienie gry:**
 - Możliwość zapisania stanu gry i kontynuacji w dowolnym momencie.
- **Statystyki:**
 - Szczegółowy raport po zakończeniu gry, obejmujący:
 - liczbę użytych kart,
 - liczbę skutecznych ataków i obron,
 - liczbę kart specjalnych i ich efektywność.
- **Profil gracza:**
 - System zapisujący postępy gracza oraz jego wyniki w różnych scenariuszach.

Integracja edukacyjnych celów gry

- **Cele edukacyjne:**
 - Gra uczy zasad cyberbezpieczeństwa, strategii i zarządzania ryzykiem.
 - Gracz rozwija umiejętności planowania i podejmowania decyzji w trudnych sytuacjach.
- **Feedback edukacyjny:**
 - Konstruktywna informacja zwrotna po każdym zadaniu lub turze, wskazująca błędy i sugerująca poprawę.
 - Komunikaty podsumowujące efekty działań gracza (np. *Skutecznie obroniłeś dwie instytucje*).

Personalizacja przez nauczyciela

- **Konfiguracja gry:**
 - Możliwość ustawienia poziomu trudności, liczby graczy oraz długości rozgrywki.
 - Opcja wyboru scenariuszy i zasobów dostępnych w grze (np. typów kart, rodzajów wyzwań).
 - Wykluczanie określonych kart (np. tylko defensywne lub ofensywne).
 - Tworzenie własnego zestawu kart i scenariuszy.
- **Dostosowanie zadań:**
 - Możliwość zmiany treści edukacyjnych lub dodawania własnych zasobów przez nauczyciela.
 - Ukrywanie lub odkrywanie wybranych opcji w zależności od potrzeb edukacyjnych grupy.

Integracja z EDUchat (szczegóły w scenariuszu I.1)

- **Pełna integracja:**
 - Wykorzystanie API EDUchat do generowania dynamicznych podpowiedzi oraz analizy decyzji gracza.
 - Automatyczne dostosowanie poziomu trudności w czasie rzeczywistym na podstawie działań gracza.
- **Wsparcie edukacyjne:**
 - EDUchat umożliwia tworzenie dodatkowych ćwiczeń na podstawie wyników z gry.
 - System analizy treści i wyników wspiera nauczyciela w monitorowaniu postępów uczniów.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Kluczowe warunki techniczne dla Wykonawców

Aplikacja musi spełniać wymagania określone w dokumencie „Ogólne wymagania funkcjonalne i techniczne dla e-materiałów”.

Mechanizmy pomiaru i raportowania postępów

- **Monitorowanie przez nauczyciela:** Aplikacja powinna oferować nauczycielom możliwość monitorowania wyników uczniów, takich jak czas spędzony w grze, liczba ukończonych zadań oraz osiągnięte cele.
- **Automatyczne raporty:** System generowania raportów, zawierających szczegółowe informacje o postępach uczniów, w tym ich wyniki, błędy i mocne strony.
- **Eksport danych:** Raporty powinny być eksportowalne w formatach takich jak PDF lub CSV, aby umożliwić dalszą analizę.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską

