Wstępny konspekt prezentacji – Karol Lubelski, Szymon Kowalczyk

Temat: Zabezpieczenia anti-cheat w grach komputerowych

**1. Wstęp**

**1.1. Wprowadzenie do tematu**

* Omówienie istoty bezpieczeństwa w grach komputerowych.
* Znaczenie systemów anti-cheat dla zachowania uczciwości rozgrywki.
* Przedstawienie kontekstu problemu: rosnąca liczba incydentów związanych z oszustwami w grach i ich wpływ na społeczność graczy.

**1.2. Cel badania**

* Zbadanie metod wykrywania oszustów w grach, od prostych skryptów po zaawansowane systemy oparte na sztucznej inteligencji.
* Analiza wyzwań stojących przed twórcami systemów anti-cheat oraz omówienie przykładów skutecznych i nieskutecznych rozwiązań.

**1.3. Zakres badania**

* Analiza różnych typów zabezpieczeń anti-cheat stosowanych w branży gier komputerowych.
* Przegląd przypadków z różnych popularnych gier (FPS, MOBA, Battle Royale) i ocena ich skuteczności.

**2. Przegląd źródeł i przykładów**

**2.1. Artykuły z Internetu**

* Wykorzystanie artykułów branżowych dotyczących najnowszych technologii wykorzystywanych w zabezpieczeniach anti-cheat.
* Przykłady publikacji na temat roli sztucznej inteligencji w wykrywaniu oszustw.

**2.2. Raporty i statystyki**

* Raporty i dane statystyczne dotyczące problemu oszustw w grach, liczby banów, fałszywych pozytywów oraz incydentów naruszeń.
* Wykorzystanie raportów firm zajmujących się zabezpieczeniami, takich jak Valve, BattleEye, Easy Anti-Cheat.

**3. Metodologia badania**

**3.1. Opis systemów anti-cheat**

* Przedstawienie różnych typów systemów anti-cheat: skrypty detekcyjne, systemy oparte na sztucznej inteligencji, monitorowanie serwerów w czasie rzeczywistym.
* Analiza, jak różne podejścia wykrywają cheaterów i jakie są ich mocne oraz słabe strony.

**3.2. Dobór przypadków do analizy**

* Wybór konkretnych gier do analizy: FPS (np. "Counter-Strike: Global Offensive"), Battle Royale (np. "Fortnite"), MOBA (np. "League of Legends").
* Kryteria doboru: popularność gry, rodzaj systemu anti-cheat oraz liczba wykrywanych incydentów oszustw.

**3.3. Procedura analizy danych**

* Opis analizy systemów zabezpieczeń na podstawie publicznie dostępnych informacji, statystyk oraz przypadków wykrytych oszustw.
* Omówienie metod badawczych: analiza dostępnych raportów, artykułów branżowych oraz danych statystycznych.

**4. Analiza wyników**

**4.1. Przykłady i wyniki z wybranych gier**

* Prezentacja danych dotyczących skuteczności systemów anti-cheat w różnych grach.
* Porównanie ilości banów, szybkości reakcji systemów oraz liczby fałszywych pozytywów.

**4.2. Wnioski z analizy**

* Identyfikacja głównych problemów związanych z wykrywaniem cheaterów (np. fałszywe pozytywy, opóźnienia w detekcji).
* Jakie czynniki wpływają na skuteczność systemów anti-cheat? Jakie są najczęstsze problemy związane z ich wdrożeniem?

**5. Dyskusja**

**5.1. Odniesienie wyników do artykułów i raportów**

* Porównanie wyników analizy z materiałami, które można znaleźć w raportach branżowych i artykułach dotyczących bezpieczeństwa w grach.
* Czy systemy są wystarczająco skuteczne w walce z cheaterami? Jakie są różnice między popularnymi rozwiązaniami?

**5.2. Interpretacja zjawisk związanych z cheatowaniem**

* Omówienie behawioralnych aspektów cheatowania: dlaczego gracze oszukują? Jakie są motywacje cheaterów?
* Wpływ technologii (np. rozwój AI) na zmiany w sposobie cheatowania.

**5.3. Rekomendacje praktyczne**

* Sugestie dotyczące ulepszania systemów anti-cheat, zwiększania skuteczności detekcji oraz minimalizowania fałszywych pozytywów.
* Rekomendacje dla twórców gier dotyczące przyszłych działań i wdrażania nowych technologii.

**6. Podsumowanie**

**6.1. Wnioski końcowe**

* Najważniejsze wnioski na temat skuteczności systemów anti-cheat i wyzwań związanych z ich rozwojem.
* Znaczenie ciągłego monitorowania i aktualizacji systemów w walce z rosnącą liczbą oszustów.

**6.2. Perspektywy na przyszłość**

* Możliwe kierunki dalszego rozwoju technologii anti-cheat.
* Wykorzystanie sztucznej inteligencji, blockchain i innych technologii przyszłości w walce z oszustwami w grach.

**7. Bibliografia**

* Spis źródeł: artykuły branżowe, raporty firm zajmujących się zabezpieczeniami, dane statystyczne dotyczące incydentów cheatowania w grach.