1. **Wstęp:**
   Witam wszystkich bardzo serdecznie, temat mojej pracy to “Zastosowanie algorytmów sztucznej inteligencji w wykrywaniu i zapobieganiu cyberzagrożeniom w transakcjach finansowych”. Jestem tu razem z ekspertem w tej dziedzinie, Panem/Pani …. Witamy Pana/Panią i dziękujemy za przybycie na nasze dzisiejsze warsztaty.

2. Prezentacja i omówienie tematu:

- **Slajd 1: Rodzaje cyberzagrożeń w finansach**
  - Omówienie najczęstszych cyberzagrożeń, takich jak phishing, malware, ataki ransomware, oszustwa związane z kartami kredytowymi, itp.
- **Slajd 2: Rola algorytmów AI w wykrywaniu zagrożeń**
  - **Wykrywanie anomalii:** Wyjaśnienie, jak AI analizuje transakcje i identyfikuje nietypowe zachowania (np. nieoczekiwane lokalizacje, duże sumy transakcji)
  - **Uczenie maszynowe (ML):** Omówienie, w jaki sposób AI uczy się na historii transakcji, rozpoznając wzorce i przyspieszając identyfikację zagrożeń
  - **Analiza predykcyjna:** Wykorzystanie AI do przewidywania potencjalnych zagrożeń na podstawie danych historycznych
- **Slajd 3: Rodzaje algorytmów AI wykorzystywanych w cyberbezpieczeństwie finansowym**
  - **Algorytmy nadzorowane (Supervised Learning):** Uczenie maszynowe na oznaczonych danych (np. transakcje legalne/podejrzane). Przykład: klasyfikacja transakcji jako "oszustwo" lub "legalna"
  - **Algorytmy nienadzorowane (Unsupervised Learning):** Wykrywanie anomalii w danych bez wcześniejszych oznaczeń. Przykład: wykrywanie nowych, nieznanych metod oszustw
- **Slajd 4: Przykłady zastosowania AI w transakcjach finansowych**
  - **Monitorowanie transakcji w czasie rzeczywistym:** Analiza każdej transakcji pod kątem ryzyka i natychmiastowe informowanie o podejrzanych działaniach
  - **Zastosowanie biometriki:** Wsparcie w weryfikacji tożsamości użytkowników poprzez analizę odcisków palców, rozpoznawanie twarzy, głosu
  - **Analiza wzorców zachowań:** Identyfikacja transakcji odbiegających od normy poprzez uczenie się typowych wzorców zachowań użytkowników
- **Slajd 5: Korzyści z zastosowania AI w wykrywaniu cyberzagrożeń**
  - **Szybkie wykrywanie zagrożeń:** Natychmiastowa identyfikacja podejrzanych transakcji dzięki analizie w czasie rzeczywistym
  - **Zmniejszenie liczby fałszywych alarmów:** Zaawansowane algorytmy zmniejszają liczbę błędnych detekcji
  - **Ochrona danych użytkowników:** Lepsza ochrona prywatnych danych i zapobieganie wyciekom informacji
- **Slajd 6: Przyszłość AI w cyberbezpieczeństwie finansowym**
  - **Rozwój algorytmów:** Zwiększona precyzja w wykrywaniu oszustw dzięki coraz bardziej zaawansowanym modelom AI
  - **Integracja z blockchainem:** Zastosowanie AI do analizy transakcji na blockchainie w celu wykrywania nielegalnych działań
  - **Zwiększona automatyzacja:** Automatyzacja reakcji na zagrożenia
- **Slajd 7: Podsumowanie**
  - Podkreślenie roli sztucznej inteligencji jako niezastąpionego narzędzia w walce z cyberzagrożeniami[2].
  - Wymienienie korzyści: zwiększenie bezpieczeństwa, szybkie wykrywanie oszustw i ochrona danych użytkowników
  - Wyzwania: Konieczność zbierania odpowiednich danych, zarządzanie fałszywymi alarmami, etyczne aspekty wykorzystania danych

3. Zakończenie:

- To już wszystko w temacie zastosowanie algorytmów sztucznej inteligencji w wykrywaniu i zapobieganiu cyberzagrożeniom w transakcjach finansowych. Mam nadzieje, że udało mi się wam przekazać trochę mojej wiedzy na ten temat. Jeżeli są jakies pytania do eksperta to śmiało proszę je zadawać.