**Sztuczna inteligencja w walce z cyberzagrożeniami finansowymi**

30.01.2026 uczniowie klasy 8 Zespołu Szkół nr 2 w Sosnowcu uczestniczyli w warsztatach w ramach ogólnopolskiego programu VI edycji „Złote Szkoły NBP".

W dzisiejszych czasach cyberprzestępczość stanowi poważne zagrożenie dla sektora finansowego. Wraz z postępem technologicznym, oszuści stają się coraz bardziej wyrafinowani, a tradycyjne metody zabezpieczeń często okazują się niewystarczające. Na szczęście, z pomocą przychodzi sztuczna inteligencja (AI), która oferuje nowe możliwości w wykrywaniu i zapobieganiu cyberzagrożeniom.

**Rodzaje cyberzagrożeń w finansach**

Cyberprzestępcy wykorzystują różnorodne metody, aby atakować systemy finansowe. Do najczęstszych zagrożeń należą:

- Phishing: Wyłudzanie poufnych informacji poprzez fałszywe wiadomości e-mail lub SMS.
- Malware: Złośliwe oprogramowanie, które infekuje systemy i kradnie dane.
- Ransomware: Blokowanie dostępu do danych i żądanie okupu za ich odzyskanie.
- Oszustwa związane z kartami kredytowymi: Nieautoryzowane transakcje dokonywane przy użyciu skradzionych danych kart.

**Rola algorytmów AI w wykrywaniu zagrożeń**

Algorytmy AI mogą analizować ogromne ilości danych o transakcjach i wykrywać nietypowe wzorce, które mogą wskazywać na oszustwo. Przykłady zastosowań AI w wykrywaniu zagrożeń:

- Wykrywanie anomalii: AI analizuje transakcje i identyfikuje nietypowe zachowania, takie jak nieoczekiwane lokalizacje lub duże sumy transakcji.
- Uczenie maszynowe (ML): AI uczy się na historii transakcji, rozpoznając wzorce i przyspieszając identyfikację zagrożeń.
- Analiza predykcyjna: AI przewiduje potencjalne zagrożenia na podstawie danych historycznych.

**Rodzaje algorytmów AI**

W cyberbezpieczeństwie finansowym wykorzystuje się różne rodzaje algorytmów AI, w tym:

- Algorytmy nadzorowane (Supervised Learning): Uczenie maszynowe na oznaczonych danych, np. transakcje legalne/podejrzane.

- Algorytmy nienadzorowane (Unsupervised Learning): Wykrywanie anomalii w danych bez wcześniejszych oznaczeń.

**Przykłady zastosowania AI w transakcjach finansowych**

AI znajduje zastosowanie w wielu obszarach transakcji finansowych:

- Monitorowanie transakcji w czasie rzeczywistym: AI analizuje każdą transakcję pod kątem ryzyka i natychmiastowo informuje o podejrzanych działaniach.
- Zastosowanie biometriki: AI wspiera weryfikację tożsamości użytkowników poprzez analizę odcisków palców, rozpoznawanie twarzy, głosu.
- Analiza wzorców zachowań: Algorytmy AI uczą się typowych wzorców zachowań użytkowników, identyfikując transakcje odbiegające od normy.

**Korzyści z zastosowania AI w wykrywaniu cyberzagrożeń**

Zastosowanie AI w cyberbezpieczeństwie finansowym przynosi wiele korzyści:

- 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.

**Przyszłość AI w cyberbezpieczeństwie finansowym**

Przyszłość AI w cyberbezpieczeństwie finansowym rysuje się obiecująco:

- 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: W przyszłości AI będzie coraz bardziej zautomatyzowana, co poprawi szybkość reakcji na zagrożenia.

**Podsumowanie**

Sztuczna inteligencja jest niezastąpionym narzędziem w walce z cyberzagrożeniami w sektorze finansowym. Zapewnia zwiększenie bezpieczeństwa, szybkie wykrywanie oszustw i ochronę danych użytkowników. Wyzwaniem jest konieczność zbierania odpowiednich danych, zarządzanie fałszywymi alarmami oraz etyczne aspekty wykorzystania danych.

Jakub Bartela 8C