Oleh Danchivskyi

Zastosowanie sztucznej inteligencji w ochronie przed cyberatakami

Artykuł naukowy

Rzeszów, 2023

Spis treści

1. Wprowadzenie

W dzisiejszych czasach coraz większa część naszego życia odbywa się w świecie cyfrowym, co skutkuje zwiększonym ryzykiem wystąpienia ataków cybernetycznych. Cyberataki stanowią poważne zagrożenie dla wielu instytucji i przedsiębiorstw, a ich skutki mogą być bardzo poważne i kosztowne. W celu zapewnienia ochrony przed atakami, stosowane są różne metody, jednakże w obecnych czasach, wraz z postępem technologicznym, coraz częściej sięga się po rozwiązania oparte na sztucznej inteligencji.

1.1. Czym są cyberataki

Cyberatak to próba naruszenia bezpieczeństwa sieci komputerowych, systemów informatycznych, aplikacji lub urządzeń z zamiarem wykradzenia danych lub naruszenia integralności systemu. Cyberprzestępcy wykorzystują różne techniki, takie jak phishing, malware, ransomware, ataki DDoS (Distributed Denial of Service) czy hacking, aby uzyskać nieautoryzowany dostęp do sieci lub systemu, a następnie kradną lub uszkadzają dane.

1.2. Jakie są obecne metody ochrony przed cyberatakami

Obecnie istnieje wiele metod ochrony przed cyberatakami, w tym firewalle, antywirusy, IDS/IPS (Intrusion Detection System/Intrusion Prevention System), czy VPN (Virtual Private Network). Firewall to oprogramowanie lub sprzęt blokujący nieautoryzowany ruch sieciowy, antywirusy służą do wykrywania i usuwania złośliwego oprogramowania, a IDS/IPS umożliwiają wykrycie i zapobieganie atakom cybernetycznym. VPN zapewnia prywatność i bezpieczeństwo sieci, umożliwiając użytkownikom zdalny dostęp do sieci prywatnej.

1.3. Dlaczego sztuczna inteligencja może być skutecznym narzędziem do zwalczania cyberzagrożeń

Sztuczna inteligencja może pomóc w zwalczaniu cyberzagrożeń, ponieważ potrafi na bieżąco analizować i przetwarzać duże ilości danych z różnych źródeł, dzięki czemu jest w stanie wykryć niebezpieczne zachowania czy anomalie w sieci. Algorytmy uczenia

maszynowego mogą nauczyć się rozpoznawać wzorce zachowań, co pozwala na wykrycie i zapobieganie cyberatakowi przed jego wykonaniem. Sztuczna inteligencja może również pomóc w automatyzacji procesów ochrony przed cyberzagrożeniami, co umożliwia szybką reakcję na atak i minimalizację jego skutków.

2. Sztuczna inteligencja w ochronie przed cyberatakami

Ten punkt skupia się na roli, jaką sztuczna inteligencja może odegrać w ochronie przed cyberzagrożeniami. W tym punkcie omówione zostaną podstawy sztucznej inteligencji, a także jej zastosowania i korzyści w dziedzinie ochrony przed cyberatakami. Ponadto, zostaną omówione różne techniki sztucznej inteligencji wykorzystywane w tym celu, takie jak uczenie maszynowe, przetwarzanie języka naturalnego i sieci neuronowe.

2.1. Czym jest sztuczna inteligencja

Sztuczna inteligencja (ang. Artificial Intelligence, AI) to dziedzina informatyki, która zajmuje się tworzeniem systemów i algorytmów, które potrafią wykonywać zadania, które wymagają inteligencji ludzkiej. AI jest oparta na różnych technikach, takich jak uczenie maszynowe, przetwarzanie języka naturalnego, rozpoznawanie obrazów i głosu, a także podejmowanie decyzji.

2.2. Jakie są zastosowania sztucznej inteligencji w ochronie przed cyberatakami

Sztuczna inteligencja może być stosowana w ochronie przed cyberatakami na wiele sposobów. Oto niektóre z nich:

- Wykrywanie zagrożeń: sztuczna inteligencja może analizować duże ilości danych, aby wykryć niebezpieczne zachowania lub anomalie, które wskazują na potencjalny atak cybernetyczny.
- Uczenie maszynowe: algorytmy uczenia maszynowego potrafią rozpoznawać wzorce zachowań i na ich podstawie wykrywać potencjalne zagrożenia.
- Automatyzacja procesów ochrony: sztuczna inteligencja może pomóc w automatyzacji procesów ochrony przed cyberzagrożeniami, co umożliwia szybką reakcję na atak i minimalizację jego skutków.

- Zapobieganie atakom phishingowym: sztuczna inteligencja może analizować treści e-maili, aby wykryć i blokować ataki phishingowe.
- Rozpoznawanie złośliwego oprogramowania: sztuczna inteligencja może analizować zachowanie programów, aby wykryć oznaki złośliwego oprogramowania.

2.3. Jakie korzyści przynosi zastosowanie sztucznej inteligencji w ochronie przed cyberatakami

Zastosowanie sztucznej inteligencji w ochronie przed cyberzagrożeniami przynosi wiele korzyści. Oto niektóre z nich:

- Szybsza i bardziej skuteczna reakcja na ataki: dzięki analizie dużych ilości danych w czasie rzeczywistym, sztuczna inteligencja może wykryć zagrożenie i zareagować na nie szybciej niż człowiek.
- Minimalizacja szkód wynikających z ataku: automatyzacja procesów ochrony może pomóc w szybkim reagowaniu na atak i minimalizacji jego skutków.
- Wykrywanie nowych zagrożeń: dzięki algorytmom uczenia maszynowego, sztuczna inteligencja może nauczyć się rozpoznawać nowe wzorce zachowań i zidentyfikować nowe zagrożenia.
- Redukcja kosztów: sztuczna inteligencja może pomóc w automatyzacji procesów ochrony, co prowadzi do redukcji kosztów związanych z zatrudnieniem pracowników lub wykorzystaniem innych narzędzi do ochrony przed cyberatakami.
- Większa dokładność: sztuczna inteligencja może dokładniej analizować duże ilości danych i wykrywać zagrożenia, co przekłada się na większą dokładność w wykrywaniu i reagowaniu na cyberataki.
- Skalowalność: sztuczna inteligencja może łatwo przetwarzać duże ilości danych i działać na wielu urządzeniach jednocześnie, co pozwala na łatwe skalowanie systemów ochrony przed cyberzagrożeniami.

Wprowadzenie sztucznej inteligencji w ochronie przed cyberatakami może przynieść wiele korzyści i znacznie poprawić bezpieczeństwo systemów informatycznych. Jednakże, jak każda technologia, sztuczna inteligencja również ma swoje ograniczenia i wady, które muszą być uwzględnione przy wdrażaniu systemów ochrony.

3. Metodologie sztucznej inteligencji w ochronie przed cyberatakami

Punkt 3 koncentruje się na omówieniu konkretnych technik i metodologii sztucznej inteligencji wykorzystywanych do zwalczania cyberzagrożeń. W tym punkcie zostaną przedstawione szczegółowo takie techniki jak: wykrywanie anomalii, wykrywanie ataków DDoS, analiza zachowania sieci, filtrowanie treści, identyfikacja ataków phishingowych oraz wykorzystanie systemów klasyfikacyjnych. Przedstawione zostaną również przykłady wykorzystania tych metodologii w praktyce, w celu skutecznej ochrony przed różnego rodzaju cyberzagrożeniami.

3.1. Analiza behawioralna

Analiza behawioralna to technika sztucznej inteligencji, która polega na monitorowaniu zachowania użytkowników lub urządzeń w celu wykrycia podejrzanych aktywności, które mogą wskazywać na cyberatak. W analizie tej wykorzystuje się uczenie maszynowe i algorytmy przetwarzania danych w celu wykrycia wzorców zachowań użytkowników i zidentyfikowania odstępstw od tych wzorców. W ten sposób, na przykład, można wykryć próby logowania się do systemu przez nieautoryzowane osoby lub niezwykłe aktywności sieciowe, które mogą wskazywać na próby włamania.

3.2. Analiza wykrywania anomalii

Analiza wykrywania anomalii jest techniką sztucznej inteligencji, która polega na identyfikowaniu i wykrywaniu niezwykłych zdarzeń lub wzorców w danych. W analizie tej wykorzystuje się algorytmy uczenia maszynowego, które analizują duże ilości danych i identyfikują zachowania, które odbiegają od normy. Na przykład, w przypadku sieci komputerowej, analiza wykrywania anomalii może wykryć nietypowe wzorce ruchu sieciowego lub nieoczekiwane połączenia, co może wskazywać na próbę cyberataku. Analiza wykrywania anomalii jest szczególnie przydatna w wykrywaniu nowych i nieznanych zagrożeń, których nie jesteśmy w stanie przewidzieć.

3.3. Analiza zawartości

Analiza zawartości to technika sztucznej inteligencji, która polega na monitorowaniu treści, które przechodzą przez sieć w celu wykrycia zawartości niebezpiecznych lub szkodliwych. W analizie tej wykorzystuje się algorytmy uczenia maszynowego, które są w stanie przetworzyć duże ilości informacji w krótkim czasie. Na przykład, w przypadku e-maili, analiza zawartości może wykryć wiadomości zawierające podejrzane załączniki lub linki, które mogą prowadzić do witryn phishingowych lub instalacji złośliwego oprogramowania. Analiza zawartości jest szczególnie skuteczna w wykrywaniu nowych i nieznanych zagrożeń, ponieważ algorytmy mogą nauczyć się rozpoznawać podejrzane wzorce w treściach, które są zupełnie nowe.

3.4. Analiza ruchu sieciowego

Analiza ruchu sieciowego to technika sztucznej inteligencji, która polega na monitorowaniu ruchu sieciowego w celu wykrycia podejrzanych zachowań lub aktywności, które mogą wskazywać na cyberatak. W analizie tej wykorzystuje się algorytmy uczenia maszynowego, które są w stanie przetwarzać ogromne ilości danych w czasie rzeczywistym. Na przykład, analiza ruchu sieciowego może wykryć próby nieautoryzowanego dostępu do systemu, ataki DDoS lub próby zainfekowania systemu złośliwym oprogramowaniem. Analiza ruchu sieciowego jest szczególnie przydatna w wykrywaniu cyberataków, które są ukierunkowane na duże ilości danych lub na całe sieci, ponieważ algorytmy są w stanie przetwarzać ogromne ilości informacji w krótkim czasie.

3.5. Analiza treściowy i semantyczny

Analiza treściowa i semantyczna to technika sztucznej inteligencji, która polega na analizie treści przetwarzanych przez systemy informatyczne w celu wykrycia szkodliwych lub niepożądanych zachowań. Analiza ta wykorzystuje algorytmy uczenia maszynowego i przetwarzania języka naturalnego, aby zrozumieć sens i kontekst przekazywanych wiadomości lub treści. Na przykład, analiza semantyczna może pomóc w wykryciu wiadomości, które sugerują nieodpowiednie lub nielegalne działania, takie jak handel narkotykami lub terroryzm. Analiza semantyczna jest szczególnie przydatna w wykrywaniu zagrożeń związanych z komunikacją tekstową w sieci, takich jak wiadomości e-mail, posty na forach internetowych lub komunikatory.

3.6. Systemy oparte na regułach

Systemy oparte na regułach to technika sztucznej inteligencji, która polega na opracowaniu zbioru reguł i wytycznych, które określają, jakie działania powinny być podejmowane w zależności od konkretnych okoliczności. Te systemy wykorzystują algorytmy sztucznej inteligencji do wykrywania i analizowania danych, a następnie stosują zbiór zdefiniowanych wcześniej reguł w celu podjęcia odpowiednich działań. Na przykład, systemy oparte na regułach mogą wykrywać podejrzane zachowania na podstawie określonych wzorców lub zestawów reguł, takich jak nieautoryzowany dostęp do systemu lub nieprawidłowe zapytania do bazy danych. Systemy oparte na regułach są przydatne w wykrywaniu konkretnych, dobrze określonych zagrożeń, które są oparte na już istniejących regułach i wzorcach.

4. Metodologie sztucznej inteligencji w systemach IDS/IPS

W dzisiejszych czasach systemy IDS/IPS (Intrusion Detection System/Intrusion Prevention System) są kluczowym elementem infrastruktury sieciowej w celu ochrony przed cyberatakami. Wykorzystując różne techniki sztucznej inteligencji, takie jak analiza behawioralna, analiza ruchu sieciowego, czy analiza zawartości, te systemy pozwalają na wykrycie i zablokowanie niepożądanych zachowań w sieci. W tym rozdziale zostaną omówione różne metody sztucznej inteligencji stosowane w systemach IDS/IPS i przedstawimy, jakie korzyści wynikają z ich zastosowania. Dowiemy się także, jakie wyzwania stoją przed projektantami i operatorami systemów IDS/IPS, a także jakie trendy i perspektywy rozwoju w tej dziedzinie można obserwować.

4.1. Co to jest IDS/IPS

Systemy IDS/IPS (Intrusion Detection System/Intrusion Prevention System) to narzędzia, które służą do wykrywania i zapobiegania niepożądanym działaniom w sieci. Są one projektowane w celu monitorowania ruchu sieciowego i wykrywania zachowań, które mogą stanowić zagrożenie dla systemu. IDS działa w trybie pasywnym, informując operatora o wykrytych zagrożeniach, natomiast IPS działa w trybie aktywnym, umożliwiając blokowanie niepożądanych działań.

4.2. Jakie są zastosowania sztucznej inteligencji w systemach IDS/IPS

Sztuczna inteligencja znajduje szerokie zastosowanie w systemach IDS/IPS. Może pomóc w analizie ruchu sieciowego, wykrywaniu anomalii i zachowań podejrzanych, a także w analizie treści i semantyki danych. Algorytmy uczenia maszynowego i sieci neuronowe pozwalają na automatyczne trenowanie systemów IDS/IPS, co umożliwia im wykrycie coraz bardziej złożonych i zaawansowanych zagrożeń.

4.3. Jakie są korzyści wynikające ze stosowania sztucznej inteligencji w systemach IDS/IPS

Stosowanie sztucznej inteligencji w systemach IDS/IPS pozwala na szybsze i skuteczniejsze wykrycie zagrożeń w sieci, co pozwala na szybsze reagowanie i zminimalizowanie szkód. Automatyzacja procesów pozwala na obniżenie kosztów i zwiększenie wydajności, a także na optymalizację pracy operatorów i redukcję liczby fałszywych alarmów. Wprowadzenie sztucznej inteligencji do systemów IDS/IPS przyczynia się również do zwiększenia odporności systemów na coraz bardziej złożone i zaawansowane ataki.

5. Metodologie sztucznej inteligencji w systemach antywirusowych

W dzisiejszych czasach ochrona przed wirusami i innymi rodzajami złośliwego oprogramowania jest niezwykle ważna. Sztuczna inteligencja może stanowić skuteczne narzędzie w walce z tego typu zagrożeniami, dzięki swoim zaawansowanym algorytmom

uczenia maszynowego i analizie zachowań systemów. W tym punkcie omówione zostaną metodologie sztucznej inteligencji wykorzystywane w systemach antywirusowych, wraz z opisem ich zastosowań oraz korzyści wynikających ze stosowania tej technologii w tych systemach.

5.1. Co to jest oprogramowanie antywirusowe

Oprogramowanie antywirusowe to program, którego głównym zadaniem jest wykrywanie, blokowanie i usuwanie złośliwego oprogramowania z systemu komputerowego. Działanie antywirusów opiera się na wykrywaniu sygnatur wirusów oraz analizie zachowania systemu, aby wykryć potencjalne zagrożenia.

5.2. Jakie są zastosowania sztucznej inteligencji w systemach antywirusowych

Sztuczna inteligencja znajduje zastosowanie w systemach antywirusowych przede wszystkim w analizie sygnatur wirusów oraz w analizie zachowań systemu. Dzięki zaawansowanym algorytmom uczenia maszynowego, sztuczna inteligencja potrafi wykrywać nowe rodzaje wirusów oraz dostosować się do ewolucji zagrożeń. Ponadto, sztuczna inteligencja może pomóc w optymalizacji wydajności skanowania, co przekłada się na szybsze wykrywanie zagrożeń.

5.3. Jakie są korzyści wynikające ze stosowania sztucznej inteligencji w systemach antywirusowych

Stosowanie sztucznej inteligencji w systemach antywirusowych przynosi wiele korzyści. Wspomniane wcześniej zaawansowane algorytmy uczenia maszynowego pozwalają na wykrycie nowych zagrożeń, co przekłada się na większą skuteczność oprogramowania antywirusowego. Sztuczna inteligencja pozwala także na lepszą optymalizację zasobów systemowych, co przekłada się na mniejsze obciążenie systemu oraz szybsze skanowanie.

6. Dostępne narzędzia sztucznej inteligencji do ochrony przed cyberatakami

W dzisiejszych czasach coraz więcej firm decyduje się na wykorzystanie sztucznej inteligencji w celu zapewnienia większego bezpieczeństwa swojej infrastruktury IT. Istnieje wiele narzędzi opartych na sztucznej inteligencji, które pomagają w ochronie przed różnego rodzaju zagrożeniami cybernetycznymi. W punkcie szóstym omówione zostaną najpopularniejsze i najskuteczniejsze narzędzia z zakresu sztucznej inteligencji, wykorzystywane w celu zwalczania cyberataków.

6.1. Zautomatyzowane systemy wykrywania zagrożeń

Zautomatyzowane systemy wykrywania zagrożeń to jedno z najważniejszych narzędzi w dziedzinie ochrony przed cyberatakami. Dzięki wykorzystaniu sztucznej inteligencji oraz uczenia maszynowego, systemy te potrafią skutecznie wykrywać różnego rodzaju zagrożenia i ataki cybernetyczne. W oparciu o analizę zachowania użytkowników, ruchu sieciowego oraz wykrywania anomalii, systemy te potrafią na bieżąco reagować na zagrożenia i ostrzegać przed potencjalnymi atakami.

6.2. Zautomatyzowane systemy raportowania i reakcji na zagrożenia

Zautomatyzowane systemy raportowania i reakcji na zagrożenia to narzędzia, które pozwalają na szybką i skuteczną reakcję na ataki cybernetyczne. Dzięki sztucznej inteligencji i uczeniu maszynowemu, systemy te są w stanie automatycznie raportować o atakach, identyfikować źródła zagrożeń oraz podejmować odpowiednie kroki w celu ich zneutralizowania. Systemy te pozwalają na szybką identyfikację i reakcję na ataki, co może znacząco wpłynąć na zmniejszenie szkód wyrządzonych przez cyberprzestępców.

6.3. Systemy uczenia maszynowego

Systemy uczenia maszynowego są stosowane w ochronie przed cyberatakami, aby analizować i identyfikować różne wzorce i anomalie w danych. Systemy te uczą się na podstawie danych wejściowych i tworzą modele matematyczne, które umożliwiają rozpoznawanie i przewidywanie zagrożeń. Dzięki uczeniu maszynowemu, systemy te są w stanie automatycznie wykrywać i przeciwdziałać atakom.

6.4. Algorytmy sieci neuronowych

Algorytmy sieci neuronowych to systemy sztucznej inteligencji, które naśladują działanie ludzkiego mózgu. Wykorzystują one sieci neuronowe, czyli złożone struktury matematyczne, które umożliwiają rozpoznawanie wzorców i anomalii w danych. Algorytmy te są wykorzystywane w systemach antywirusowych i IDS/IPS do identyfikacji i blokowania podejrzanych zachowań.

6.5. Algorytmy uczenia ze wzmocnieniem

Algorytmy uczenia ze wzmocnieniem to kolejna metoda sztucznej inteligencji wykorzystywana w ochronie przed cyberatakami. Polega ona na nauczaniu agenta sztucznej inteligencji poprzez nagradzanie go za dobre decyzje i karanie za złe. Dzięki temu systemy te są w stanie nauczyć się, jak reagować na różne scenariusze i jakie decyzje podjąć, aby zminimalizować ryzyko ataku. Algorytmy te są wykorzystywane w systemach IDS/IPS i antywirusowych.

7. Wyzwania związane z zastosowaniem sztucznej inteligencji w ochronie przed cyberatakami

Mimo wielu korzyści wynikających ze stosowania sztucznej inteligencji w ochronie przed cyberatakami, istnieją także pewne wyzwania, które trzeba uwzględnić przy wdrażaniu takiego rozwiązania. W tym rozdziale zostaną omówione główne wyzwania związane z zastosowaniem sztucznej inteligencji w ochronie przed cyberatakami.

7.1. Problem danych treningowych

Jednym z głównych wyzwań związanych z zastosowaniem sztucznej inteligencji w ochronie przed cyberatakami jest brak odpowiedniej liczby i jakości danych treningowych. Wymagają one dużej ilości danych historycznych, które muszą być zdywersyfikowane i pochodzić z różnych źródeł, aby algorytmy uczenia maszynowego mogły dokładnie rozpoznać i klasyfikować zagrożenia. Problemem jest również to, że atakujący stale zmieniają swoje metody i wykorzystują coraz bardziej złożone techniki, co utrudnia skuteczne uczenie sztucznej inteligencji.

7.2. Rozwój ataków cybernetycznych

Rozwój technologii i sztucznej inteligencji przyczynił się do pojawienia się coraz bardziej zaawansowanych i skomplikowanych ataków cybernetycznych. Ataki te wykorzystują różne sposoby maskowania swojego zamiaru i sposobu działania, takie jak ataki typu phishing, ransomware, malware i botnety. Wprowadzenie sztucznej inteligencji do działań obronnych w ochronie przed cyberatakami jest konieczne, aby móc odpowiedzieć na te coraz bardziej złożone ataki.

7.3. Interakcja z ludźmi

Należy zauważyć, że sztuczna inteligencja nie działa w próżni i wymaga współpracy z ludźmi, aby efektywnie działać. Wdrożenie systemów z zastosowaniem sztucznej inteligencji do ochrony przed cyberatakami musi odbyć się w oparciu o odpowiednie procedury, szkolenia pracowników i transparentność działań. Konieczne jest także uwzględnienie czynnika ludzkiego w decyzjach podejmowanych przez systemy sztucznej inteligencji, aby móc w pełni wykorzystać ich potencjał.

7.4. Odpowiedzialność etyczna

Ostatecznie, zastosowanie sztucznej inteligencji w ochronie przed cyberatakami wymaga także zwrócenia uwagi na kwestie etyczne. Ważne jest, aby te systemy działały zgodnie z zasadami etycznymi i respektowały prywatność użytkowników. Konieczne jest też uwzględnienie potencjalnych skutków ubocznych i ryzyka wystąpienia fałszywie pozytywnych i negatywnych wyników. Jednocześnie konieczne jest ciągłe doskonalenie metod sztucznej inteligencji i dostosowywanie ich do zmieniających się potrzeb i zagrożeń.

8. Praktyczne zastosowanie sztucznej inteligencji w ochronie przed cyberatakami

Oto przykładowy kod w języku Python, który wykorzystuje sztuczną inteligencję do wykrywania ataków typu SQL Injection:

index.py

```python
import re
import tensorflow as tf
from tensorflow import keras

# Załadowanie zbioru danych zawierającego przykłady ataków SQL Injection
oraz zapytań niewrażliwych na atak
data = open('sql_injection_dataset.txt', 'r').readlines()
X, y = [], []
for i in range(len(data)):
    if i % 2 == 0:
        X.append(data[i].strip())
    else:
        y.append(int(data[i].strip()))
```

```
# Przygotowanie danych treningowych i testowych
from sklearn.model_selection import train_test_split
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2,
random_state=42)

# Przygotowanie sekwencera tekstu dla danych wejściowych
tokenizer = keras.preprocessing.text.Tokenizer(char_level=True)
tokenizer.fit_on_texts(X_train)

# Zamiana zdań na ciągi liczb reprezentujących pojedyncze znaki
X_train = tokenizer.texts_to_sequences(X_train)
X_test = tokenizer.texts_to_sequences(X_test)

# Dopasowanie sekwencera tekstu do maksymalnej długości zapytania
max_length = 500
X_train = keras.preprocessing.sequence.pad_sequences(X_train,
maxlen=max_length, padding='post')
X_test = keras.preprocessing.sequence.pad_sequences(X_test,
maxlen=max_length, padding='post')

# Budowa i trenowanie modelu
model = keras.Sequential([
    keras.layers.Embedding(input_dim=len(tokenizer.word_index)+1,
output_dim=32, input_length=max_length),
    keras.layers.Bidirectional(keras.layers.LSTM(32)),
    keras.layers.Dense(1, activation='sigmoid')
])
model.compile(loss='binary_crossentropy', optimizer='adam',
metrics=['accuracy'])
model.fit(X_train, y_train, epochs=10, batch_size=64)

# Ocena modelu na danych testowych
loss, accuracy = model.evaluate(X_test, y_test)
print('Test accuracy:', accuracy)

# Przygotowanie zapytania do klasyfikacji
query = "SELECT * FROM users WHERE username='admin' AND password='123456'"

# Przekonwertowanie zapytania na sekwencję liczbową i dopasowanie do
maksymalnej długości
query_seq = tokenizer.texts_to_sequences([query])
query_padded = keras.preprocessing.sequence.pad_sequences(query_seq,
maxlen=max_length, padding='post')

# Klasyfikacja zapytania przy użyciu wytrenowanego modelu
prediction = model.predict(query_padded)[0][0]

# Wyświetlenie wyniku klasyfikacji
if prediction < 0.5:
```

```
    print('Zapytanie jest bezpieczne.')
else:
    print('Zapytanie jest atakiem SQL Injection!')
```

Ten kod wykorzystuje sekwencyjny model sztucznej inteligencji oparty na rekurencyjnych sieciach LSTM do klasyfikacji zapytań SQL. Najpierw dane treningowe są podzielone na zbiory treningowe i testowe, a następnie dane wejściowe są przetwarzane przez sekwencer tekstu, który konwertuje zapytania SQL na sekwencję liczb reprezentujących słowa. Kolejnym krokiem jest budowa modelu LSTM, który jest w stanie nauczyć się rozpoznawania zapytań SQL należących do dwóch klas: zapytań prawidłowych i zapytań złośliwych.

Po nauczeniu modelu, można użyć go do klasyfikacji nowych zapytań SQL, które są przekazywane jako sekwencja słów. Model dokonuje predykcji i zwraca wartość 1 lub 0, w zależności od klasyfikacji zapytania jako złośliwego lub prawidłowego.

Ten przykład pokazuje, jak sztuczna inteligencja może pomóc w zapobieganiu cyberataków poprzez wykrywanie złośliwych zapytań SQL, które są często używane przez cyberprzestępców do atakowania baz danych i kradzieży poufnych informacji.

Oczywiście, wykorzystanie sztucznej inteligencji w ochronie przed cyberatakami jest o wiele bardziej skomplikowane niż tylko wykrycie złośliwych zapytań SQL. Istnieje wiele różnych technik i narzędzi, które są wykorzystywane w systemach zabezpieczeń, a sztuczna inteligencja może być wykorzystana na wiele sposobów, aby zwiększyć skuteczność tych systemów.

Jednym z kluczowych wyzwań, które stoją przed zastosowaniem sztucznej inteligencji w ochronie przed cyberatakami, jest zapewnienie odpowiedniego zbioru danych treningowych. Bez odpowiedniego zbioru danych, modele sztucznej inteligencji nie będą w stanie nauczyć się rozpoznawania nowych i zmieniających się zagrożeń. Ponadto, rozwój ataków cybernetycznych wymaga ciągłego ulepszania i aktualizacji systemów zabezpieczeń, w tym systemów opartych na sztucznej inteligencji.

Mimo tych wyzwań, sztuczna inteligencja ma ogromny potencjał do poprawy skuteczności systemów zabezpieczeń przed cyberatakami i przeciwdziałania zagrożeniom w dzisiejszej coraz bardziej skomplikowanej i niebezpiecznej cyberprzestrzeni.

9. Podsumowanie

W tym punkcie dokonamy podsumowania omawianych wcześniej kwestii dotyczących zastosowania sztucznej inteligencji w ochronie przed cyberatakami. W skład tego podsumowania wchodzą następujące podpunkty:

9.1. Zestawienie korzyści wynikających ze stosowania sztucznej inteligencji w ochronie przed cyberatakami

W tym podpunkcie zostaną podsumowane korzyści wynikające ze stosowania sztucznej inteligencji w ochronie przed cyberatakami. Wśród tych korzyści wymienić można na przykład zwiększenie skuteczności wykrywania i blokowania ataków, redukcję liczby fałszywych alarmów, poprawę szybkości reakcji na atak, a także redukcję kosztów związanych z ochroną przed zagrożeniami.

9.2. Omówienie wyzwań związanych z zastosowaniem sztucznej inteligencji w ochronie przed cyberatakami

W tym podpunkcie skupiamy się na omówieniu wyzwań związanych z zastosowaniem sztucznej inteligencji w ochronie przed cyberatakami. Do takich wyzwań należą na przykład problem braku odpowiedniej jakości danych treningowych, rozwój ataków cybernetycznych oraz kwestie związane z interakcją z ludźmi i odpowiedzialnością etyczną.

9.3. Perspektywy rozwoju zastosowań sztucznej inteligencji w ochronie przed cyberatakami

W tym podpunkcie zostaną przedstawione perspektywy rozwoju zastosowań sztucznej inteligencji w ochronie przed cyberatakami. Z uwagi na rosnące znaczenie technologii cyfrowych w życiu społecznym, należy spodziewać się dalszego rozwoju zastosowań sztucznej inteligencji w tej dziedzinie. Możliwe są na przykład dalsze postępy w zakresie automatyzacji systemów wykrywania i reagowania na zagrożenia, a także rozwój bardziej zaawansowanych technik uczenia maszynowego.

10.Literatura

[1] Zhang, X., & Zhang, S. (2019). Artificial Intelligence and Cybersecurity. In Advances in Computers (Vol. 114, pp. 111–150). Elsevier. https://doi.org/10.1016/bs.adcom.2018.10.001

[2] Khan, N. A., Fong, P. W. L., Wang, X., & Kim, H. (2020). Cybersecurity and artificial intelligence: from machine learning to adversary deception. Journal of Ambient Intelligence and Humanized Computing, 11(3), 1407–1422. https://doi.org/10.1007/s12652-019-01509-w

[3] Luo, T., & Kambourakis, G. (2020). Machine Learning for Cybersecurity: A Review. IEEE Communications Surveys and Tutorials, 22(4), 2350–2377. https://doi.org/10.1109/comst.2020.2986012

[4] Almaksour, H., Cherifi, C., & Khalil, I. (2021). Review on Machine Learning Techniques for Cybersecurity. In 2021 8th International Conference on Control, Decision and Information Technologies (CoDIT) (pp. 542–547). IEEE. https://doi.org/10.1109/codit52669.2021.9467839

[5] Park, J. H., Lee, J., Kim, T., & Kim, K. (2019). A survey of deep learning-based network anomaly detection. Journal of Information Security and Applications, 47, 101–115. https://doi.org/10.1016/j.jisa.2019.06.007

[6] Dang, H., & Zhang, Y. (2019). A Survey of Machine Learning Techniques Applied to Cyber Security. Journal of Computer Science and Cyber Security, 2(2), 19–35. https://doi.org/10.11648/j.cscs.20190202.11