Zgłoszenie tematu pracy dyplomowej **:: STUDIA II STOPNIA ::**

na rok akademicki 2024/25

Promotor:	**dr inż Grzegorz Sokal**
Temat pracy magisterskiej (j. polski oraz j. angielski):	Analiza możliwości wykorzystania AI w projektowaniu zabezpieczeń sieci komputerowych *Analysis of the possibilities of using AI in the design of computer network security*
Zakres i oczekiwane rezultaty pracy:	1. Przegląd literatury i aktualnych badań Omówienie istniejących badań i literatury dotyczących wykorzystania sztucznej inteligencji (AI) w obszarze bezpieczeństwa sieci komputerowych. Przegląd popularnych technologii AI stosowanych w ochronie sieci, takich jak uczenie maszynowe, sieci neuronowe i algorytmy oparte na analizie behawioralnej. 2. Charakterystyka zagrożeń w sieciach komputerowych Analiza typowych zagrożeń i ataków na sieci komputerowe, takich jak ataki DDoS, phishing, malware, ransomware, czy ataki typu man-in-the-middle (MITM). Przegląd tradycyjnych metod zabezpieczeń i ich ograniczeń. 3. Przegląd technologii AI stosowanych w zabezpieczeniach sieci Opis technologii i narzędzi AI, które można wykorzystać do projektowania systemów zabezpieczeń, takich jak: - Systemy wykrywania intruzów (IDS), - Systemy zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM), - Algorytmy detekcji anomalii, - Sieci neuronowe i metody głębokiego uczenia. 4. Studium przypadku – implementacja systemu opartego na AI Opis przykładowego projektu, w którym AI jest stosowane do wykrywania zagrożeń w środowisku sieciowym. Analiza wyników, zalet i ograniczeń tej technologii na przykładzie wybranych narzędzi. 5. Ocena efektywności AI w zabezpieczeniach sieci komputerowych Analiza skuteczności AI w wykrywaniu i reagowaniu na zagrożenia w porównaniu do tradycyjnych metod zabezpieczeń. Ocena wydajności, skalowalności, łatwości wdrożenia oraz kosztów związanych z implementacją rozwiązań AI. 6. Analiza przyszłych trendów i wyzwań Przedstawienie kierunków rozwoju sztucznej inteligencji w zabezpieczeniach sieciowych, wyzwań związanych z implementacją AI w tym obszarze, a także potencjalnych zagrożeń związanych z automatyzacją procesów bezpieczeństwa. Oczekiwane rezultaty 1. Kompleksowa analiza możliwości wykorzystania AI Szczegółowe zrozumienie, jak i gdzie AI może wspomóc projektowanie i implementację zabezpieczeń sieci komputerowych, a także analiza jej skuteczności. 2. Identyfikacja i ocena technologii AI Identyfikacja kluczowych narzędzi i technologii AI dostępnych na rynku oraz ocena ich przydatności i skuteczności w kontekście różnych zagrożeń. 3. Wskazanie korzyści i ograniczeń stosowania AI

	Wypracowanie wniosków na temat korzyści (np. automatyzacja, szybsze wykrywanie zagrożeń) oraz ograniczeń (np. wymagania dotyczące danych, zasoby obliczeniowe) wynikających ze stosowania AI w zabezpieczeniach sieciowych. 4. Rekomendacje dotyczące implementacji AI Praktyczne wskazówki i rekomendacje dotyczące wdrażania systemów AI w zabezpieczeniach sieci komputerowych, uwzględniające najlepsze praktyki oraz potencjalne wyzwania. 5. Ocena przyszłych możliwości rozwoju Wskazanie obszarów, w których AI może mieć największy wpływ w przyszłości, oraz analiza ryzyka i korzyści związanych z dalszą automatyzacją zabezpieczeń sieci komputerowych.
*Aspekt naukowy, problemowy pracy:	**Aspekt naukowy** Praca opiera się na analizie interdyscyplinarnej, łącząc obszary związane z bezpieczeństwem sieci komputerowych, informatyką, oraz sztuczną inteligencją. Z perspektywy naukowej dotyczy ona badań nad skutecznością zastosowania algorytmów AI (głównie uczenia maszynowego i głębokiego) do identyfikacji, zapobiegania i reagowania na zagrożenia sieciowe. Praca uwzględnia również analizę danych, w tym zagadnienia związane z przetwarzaniem dużych zbiorów danych, które stanowią podstawę do skutecznego uczenia systemów AI. Kluczowym aspektem naukowym jest tutaj ocena, na ile efektywne i skalowalne mogą być metody sztucznej inteligencji w porównaniu do klasycznych metod zabezpieczeń sieciowych oraz jakie wymagania techniczne i organizacyjne są niezbędne, aby w pełni wykorzystać ich potencjał. **Aspekt problemowy** Złożoność i dynamika współczesnych zagrożeń sieciowych – takich jak zaawansowane ataki DDoS, oprogramowanie typu ransomware, phishing, czy ataki zero-day – powodują, że tradycyjne metody zabezpieczeń stają się często niewystarczające. Problemem, na który odpowiada praca, jest potrzeba wdrażania nowoczesnych systemów, które umożliwiają szybszą i bardziej precyzyjną identyfikację oraz reagowanie na zagrożenia w czasie rzeczywistym. W związku z tym, zasadniczy problem badawczy to odpowiedź na pytanie: **Czy oraz w jakim stopniu sztuczna inteligencja może efektywnie wspierać projektowanie zabezpieczeń sieciowych oraz jakimi metodami należy implementować AI, aby skutecznie wykrywać, analizować i neutralizować zagrożenia sieciowe?** Praca ma na celu przedstawienie wyników analizy w oparciu o przegląd aktualnych rozwiązań oraz eksperymenty mające na celu zweryfikowanie skuteczności wybranych algorytmów i narzędzi AI w zakresie zabezpieczeń sieci.
Literatura	**Książki i podręczniki** 1. Bishop, C. M. (2006). *Pattern Recognition and Machine Learning*. Springer. Klasyczna pozycja omawiająca teoretyczne i praktyczne aspekty uczenia maszynowego, w tym algorytmy przydatne w

	rozpoznawaniu wzorców w danych sieciowych. 2. Goodfellow, I., Bengio, Y., Courville, A. (2016). *Deep Learning*. MIT Press. Przewodnik po głębokim uczeniu, z omówieniem najnowszych technik, które są szczególnie przydatne w tworzeniu systemów wykrywania zagrożeń bazujących na analizie behawioralnej. 3. Kott, A., Wang, C., Erbacher, R. F. (2014). *Cyber Defense and Situational Awareness*. Springer. Zbiór artykułów omawiający zagadnienia cyberobrony i metod zwiększających świadomość sytuacyjną, w tym techniki AI. 4. Sarker, I. H. (2020). *Machine Learning for Cybersecurity*. Springer. Książka skupiająca się na zastosowaniu uczenia maszynowego w bezpieczeństwie sieciowym, z przykładami wykorzystania algorytmów AI do detekcji i zapobiegania zagrożeniom. **Artykuły naukowe** 1. Buczak, A. L., Guven, E. (2016). "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection". *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176. Przegląd metod uczenia maszynowego stosowanych w systemach detekcji intruzów (IDS), omówienie zalet i ograniczeń. 2. Ahmed, M., Mahmood, A. N., Hu, J. (2016). "A Survey of Network Anomaly Detection Techniques". *Journal of Network and Computer Applications*, 60, 19–31. Artykuł przedstawiający różne techniki wykrywania anomalii w ruchu sieciowym, które mogą być przydatne przy implementacji AI. 3. Sommer, R., Paxson, V. (2010). "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection". *IEEE Symposium on Security and Privacy*, 305–316. Krytyczna analiza zastosowania uczenia maszynowego w systemach wykrywania intruzów, wraz z omówieniem wyzwań związanych z tą technologią. 4. Kim, G., Lee, S., Kim, S. (2014). "A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection with Misuse Detection". *Expert Systems with Applications*, 41(4), 1690–1700. Propozycja hybrydowej metody wykrywania intruzów łączącej wykrywanie anomalii i wykrywanie nadużyć, która ilustruje efektywność systemów AI w tym obszarze. **Raporty i dokumenty branżowe** 1. Gartner, Inc. (2021). *Top Security and Risk Management Trends*. Raport omawiający najnowsze trendy w zarządzaniu bezpieczeństwem, z uwzględnieniem wykorzystania AI i automatyzacji w cyberobronie. 2. Cisco (2020). *Annual Cybersecurity Report*. Raport analizujący aktualne zagrożenia sieciowe i technologie obronne, w tym wykorzystanie uczenia maszynowego w wykrywaniu zagrożeń. 3. IBM Security (2021). *Cost of a Data Breach Report*. Analiza kosztów naruszeń danych i ocena, jak zastosowanie AI może pomóc w zmniejszeniu tych kosztów poprzez szybsze wykrywanie

	incydentów. **Publikacje online i blogi techniczne** 1. OpenAI. "Using AI for Cybersecurity: Challenges and Solutions". Dostępne na: openai.com/blog Blog omawiający zastosowanie AI w bezpieczeństwie sieciowym, wyzwania związane z implementacją i przyszłe możliwości rozwoju tej technologii. 2. Google Cloud. "Machine Learning for Network Security". Dostępne na: cloud.google.com/blog Artykuł omawiający przykłady wykorzystania AI w zabezpieczeniach sieciowych na platformie Google Cloud. 3. Microsoft Security. "The Future of Cybersecurity: AI-Driven Approaches". Dostępne na: microsoft.com/security/blog Blog omawiający nowoczesne podejścia do cyberbezpieczeństwa, w tym narzędzia AI stosowane w ochronie infrastruktury sieciowej.
Oprogramowanie, język programowania, środowisko systemowe:	Docker, Kubernetes, Python/Golang do analizy danych i skryptów automatyzacyjnych, Linux jako główne środowisko systemowe
Środowisko uruchomieniowe:	Oprogramowanie Do realizacji celów pracy magisterskiej zostaną wykorzystane narzędzia oraz biblioteki wspierające rozwój sztucznej inteligencji i analizy danych. W szczególności zastosowane będą: 1. Python - główny język programowania, który zapewnia szeroką dostępność bibliotek do AI i analizy danych. - Scikit-Learn – do implementacji klasycznych algorytmów uczenia maszynowego, takich jak drzewa decyzyjne, SVM, kNN i inne. - TensorFlow i Keras – do budowy i trenowania sieci neuronowych, głębokiego uczenia oraz tworzenia modeli wykrywania anomalii. - Pandas i NumPy – do analizy danych i ich przetwarzania. - Matplotlib i Seaborn – do wizualizacji wyników i analizy efektywności algorytmów. 2. Wireshark lub tcpdump – narzędzia do monitorowania ruchu sieciowego, które pomogą w tworzeniu zestawów danych do testowania i trenowania modeli AI. 3. Snort lub Suricata – narzędzia IDS/IPS (Intrusion Detection/Prevention Systems), które pozwalają na integrację AI z klasycznymi metodami zabezpieczeń i analizę ich skuteczności w wykrywaniu zagrożeń. 4. Jupyter Notebook – interaktywne środowisko do implementacji i testowania kodu oraz dokumentowania przebiegu analiz. Język programowania - Python – ze względu na swoje bogate zasoby bibliotek AI oraz popularność w dziedzinie przetwarzania danych i sztucznej inteligencji. - Dodatkowo, możliwe jest użycie SQL do zarządzania i przetwarzania dużych zbiorów danych.

	Środowisko systemowe - System operacyjny: Linux (np. Ubuntu lub CentOS) – z uwagi na optymalizację pod kątem narzędzi sieciowych, bezpieczeństwa i zgodności z oprogramowaniem open-source do analizy ruchu sieciowego. - Chmura obliczeniowa (np. Google Cloud Platform, AWS) – w przypadku potrzeby skalowania obliczeń dla bardziej złożonych modeli głębokiego uczenia lub pracy z dużymi zbiorami danych. Praca nad projektem będzie realizowana w środowisku pozwalającym na łatwą integrację narzędzi AI z monitorowaniem ruchu sieciowego, co umożliwi testowanie systemu w realistycznych warunkach sieciowych.
Dodatkowe wymagania i uwagi:	

UWAGA:
W polu literatura należy wskazać minimum 1 publikację z listy czasopism punktowanych wg wykazu MNiSW z dnia 5 stycznia 2024 r. związaną z proponowanym tematem pracy dyplomowej.

* Regulamin studiów § 36 2. Praca dyplomowa na profilu praktycznym, podobnie jak praca inżynierska, powinna mieć charakter aplikacyjny, badawczy, projektowy lub oceniający praktykę w świetle teorii.
pola opcjonalne