ul. Jagiellońska 57/59
03-301 Warszawa

tel. 22 519 21 00
akademia@kozminski.edu.pl

kozminski.edu.pl

AKADEMIA
LEONA KOŹMIŃSKIEGO

dr hab. Bogdan Księżopolski
Katedra Cyberbezpieczeństwa
Akademia Leona Koźmińskiego

Warszawa, 31.05.2025 r.

Recenzja osiągnięć naukowych oraz istotnej aktywności naukowej w postępowaniu habilitacyjnym dr. inż. Marka Pawlickiego w dziedzinie nauk technicznych, w dyscyplinie informatyka techniczna i telekomunikacja

1. Wprowadznie

Niniejsza recenzja została przygotowana na zlecenie Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja Politechniki Bydgoskiej (Uchwała nr 9/2025 z dnia 20 marca 2025 r.) oraz na podstawie zawiadomienia o wyznaczeniu na recenzenta w komisji habilitacyjnej w postępowaniu w sprawie nadania stopnia doktora habilitowanego podpisanego przez Przewodniczącego Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja Politechniki Bydgoskiej dr hab. inż. Tomasza Talaśka (z dnia 21 marca 2025 r.).

Recenzja została przygotowana w oparciu o materiały prezentujące (1) osiągnięcie naukowe doktora inżyniera Marka Pawlickiego wraz z autoreferatem oraz (2) dorobek naukowy, w szczególności wykaz opublikowanych prac naukowych, a także informacje o działalności naukowej. Na początku wyrażę opinię na temat osiągnięcia doktora inżyniera Marka Pawlickiego, a następnie odniosę się do dorobku naukowego oraz dydaktycznego.

2. Ocena osiągnięcia naukowego

Przedmiotem oceny jest osiągnięcie naukowe w formie cyklu publikacji powiązanych ze sobą tematycznie, obejmujących 9 pozycji opublikowanych w latach 2020-2024. Prace te są opublikowane: w czasopismach z IF (4 pozycje) oraz w materiałach konferencyjnych (5 pozycji). Osiągnięcie jest zatytułowane: **„Zaawansowane metody uczenia maszynowego oraz wyjaśnialnej sztucznej inteligencji (xAI) dla wykrywania ataków sieciowych.”**. Są to wyszczególnione poniżej publikacje (w porządku chronologicznym):

1. Choraś, M., and Pawlicki, M. (2021) - **Intrusion detection approach based on optimised artificial neural network**. In Neurocomputing, 452, (pp. 705–715), IF 5.719.
2. Pawlicki, M., Kozik, R. and Choraś, M. (2022) - **A survey on neural networks for (cyber-) security and (cyber-) security of neural networks.** In Neurocomputing, 500, (pp.1075–1087), IF 5.779.

3. Pawlicki, M., Pawlicka, A., Kozik, R., and Choraś, M. (2023) - **How to Boost Machine Learning Network Intrusion Detection Performance with Encoding Schemes.** In International Conference on Computer Information Systems and Industrial Management (pp. 283-297). Cham: Springer Nature Switzerland, CORE C.
4. Pawlicki, M., Kozik, R., and Choraś, M. (2022) - **Towards Deployment Shift Inhibition Through Transfer Learning in Network Intrusion Detection**. In Proceedings of the 17th International Conference on Availability, Reliability and Security (pp. 1-6), CORE B.
5. Pawlicki, M., Kozik, R., and Choraś, M. (2023) - **Improving Siamese Neural Networks with Border Extraction Sampling for the use in Real-Time Network Intrusion Detection**. In International Joint Conference on Neural Networks (IJCNN), Gold Coast, Australia, (pp. 1-8), CORE B.
6. Pawlicki, M., (2023) - **Towards Quality Measures for xAI algorithms: Explanation Stability**. in IEEE 10th International Conference on Data Science and Advanced Analytics (DSAA), (pp. 1–10), CORE B.
7. Pawlicki, M., Pawlicka, A., Kozik, R. and Choraś, M., (2024) - **Explainability versus Security: The Unintended Consequences of xAI in Cybersecurity**, in Proceedings of the 2nd ACM Workshop on Secure and Trustworthy Deep Learning Systems, (pp. 1–7), CORE A.
8. Pawlicki, M., (2024) ARIA, HaRIA, and GeRIA: **Novel Metrics for Pre-Model Interpretability**, in IEEE Access, vol. 12, (pp.123561-123580), IF 3.4.
9. Pawlicki, M., Pawlicka, A., Kozik, R., and Choraś, M., (2024) - **The survey on the dual nature of xAI challenges in intrusion detection and their potential for AI innovation**. In Artificial Intelligence Review 57, (art. no. 330), IF 10.7.

Przedstawiony cykl prac opublikowany został w renomowanych czasopismach z wysokim wskaźnikiem IF (Artificial Intelligence Review, Neurocomputing, IEEE Access) i znaczących materiałach konferencyjnych. Prace dotyczą siedmiu zagadnień badawczych:

1. Optymalizacja metod AI i ML w NIDS.
2. Rozwiązywanie problemu przesunięcia wdrożeniowego za pomocą uczenia transferowego.
3. Zwiększenie zdolności wykrywania nieznanych ataków za pomocą sieci neuronowych Siamese.
4. Ocena technik xAI poprzez analizę stabilności.
5. Ujawnianie ryzyka wykorzystania xAI w atakach typu adversarial.
6. Wprowadzenie interpretowalności przedmodelowej (PMI) i nowych metryk.
7. Identyfikacja przyszłych kierunków badań w xAI.

ul. Jagiellońska 57/59
03-301 Warszawa

tel. 22 519 21 00
akademia@kozminski.edu.pl

kozminski.edu.pl

AKADEMIA
LEONA KOŹMIŃSKIEGO

Pierwsze zagadnienie dotyczy problemu arbitralnych konfiguracji modeli AI i ML w systemach wykrywania intruzów (NIDS), co przekłada się na obniżenie ich skuteczności w rzeczywistych implementacjach [1, 2, 3]. Problem ten nie jest nowy – istnieje wiele badań, które pomijają wpływ doboru topologii i hiperparametrów na dokładność wykrywania. Habilitant przeprowadził systematyczną analizę oraz optymalizację topologii i parametrów sieci neuronowych (ANN), wykorzystywanych w NIDS, co pozwoliło na redukcję przypadkowości w konfiguracji modeli. Moim zdaniem dużą wartością tej pracy jest jej aspekt metodologiczny – dostarcza on solidnych podstaw do dalszych badań i praktycznego wdrażania systemów NIDS. W moim odczuciu praca [1] jest to najlepsza praca w całym cyklu, która została znacząco zauważona na Świecie (Cytowanie WoS:54, Sco:73, Gsc:112).

Kolejne zagadnienie dotyczy praktycznego wdrażania systemów NIDS, czyli spadku skuteczności modeli ML w nowych środowiskach sieciowych [4]. Habilitant zaproponował zastosowanie metod uczenia transferowego, które pozwalają na adaptację modeli przy minimalnej ilości danych z sieci docelowej. Przedstawione podejście wyróżnia się niskimi wymaganiami co do danych i brakiem konieczności pełnego ponownego szkolenia modelu. Z perspektywy praktycznej jest to bardzo istotne, ponieważ umożliwia wdrażanie skutecznych systemów detekcji w zróżnicowanych środowiskach bez dużych nakładów zasobów.

Trzecie zagadnienie dotyczy wykrywania nieznanych ataków w systemach NIDS, co stanowi jedno z kluczowych wyzwań dla skutecznego i proaktywnego cyberbezpieczeństwa [5]. Habilitant zaproponował nową metodę uczenia sieci neuronowych typu Siamese, wykorzystującą ekstrakcję granic klas za pomocą algorytmu k-NN. Dzięki temu podejściu możliwe jest skuteczniejsze rozpoznawanie ataków typu zero-day, które wcześniej nie występowały w danych treningowych. Zastosowana technika może być cenna w przyszłych implementacjach systemów NIDS.

Kolejne zagadnienie dotyczy oceny technik wyjaśnialnej sztucznej inteligencji (xAI), co ma kluczowe znaczenie dla budowania zaufania do systemów AI w kontekście cyberbezpieczeństwa. W pracy [6] Habilitant zaproponował nową metodę oceny stabilności wyjaśnień, opartą na analizie odporności tych wyjaśnień na zakłócenia danych, przy wykorzystaniu miar korelacji. W ramach prac w obszarze xAI, aspekt stabilności pozostaje niedostatecznie rozpoznany, a przedstawiona propozycja wypełnia tę lukę. Analiza przeprowadzona na czterech zbiorach danych – Breast Cancer, Iris, Wine oraz CIC-IDS2018 – wykazała, że wartości SHAP są wrażliwe na różne typy zakłóceń, a wpływ ten różni się w zależności od charakterystyki zbioru. To jest jedna z dwóch prac z cyklu, której jedynym autorem jest Habilitant.

Jednym z mniej oczywistych, ale niezwykle istotnych zagadnień jest podatność algorytmów xAI na wykorzystanie ich do celów ofensywnych, takich jak ataki typu adversarial [7]. W przeprowadzonych badaniach wykazano, że techniki generowania kontrfaktualnych wyjaśnień, jak DiCE, mogą zostać użyte do tworzenia przykładów omijających systemy NIDS. Takie podejście ujawnia istotne ryzyko, które do tej pory było słabo rozpoznane w literaturze dotyczącej wyjaśnialności AI.

Kolejne zagadnienie dotyczy interpretowalności przedmodelowej (PMI), czyli oceny znaczenia cech jeszcze przed rozpoczęciem procesu uczenia [8]. Habilitant wprowadził tę koncepcję wraz z nowymi metrykami – ARIA, HaRIA i GeRIA – które umożliwiają analizę wpływu cech na potencjalne zachowanie modelu. Podejście to pozwala na wczesne wykrycie problematycznych zmiennych, co może znacząco zwiększyć niezawodność i efektywność późniejszego modelowania. Wartością dodaną tej metody jest możliwość oceny jakości danych bez konieczności budowania i trenowania modelu. Metryki PMI mogą również stanowić punkt odniesienia dla dalszej interpretacji wyników generowanych przez techniki xAI. To jest kolejna praca, której samodzielnym autorem jest Habilitant.

Ostatnia praca z cyklu koncentruje się na identyfikacji kluczowych kierunków rozwoju w obszarze wyjaśnialnej sztucznej inteligencji (xAI), co ma duże znaczenie dla dalszych prac badawczych [9]. Na podstawie kompleksowego przeglądu literatury habilitant zidentyfikował 25 głównych wyzwań i możliwości, obejmujących m.in. potrzebę standaryzacji metod, kwestie prywatności oraz kompromis między wydajnością a wyjaśnialnością. Taka systematyzacja pozwala lepiej zrozumieć aktualny stan badań oraz luki, które wymagają dalszej eksploracji. Praca stanowi punkt wyjścia dla przyszłych projektów naukowych oraz praktycznych wdrożeń.

Biorąc pod uwagę powyższe, uważam, że przedstawione osiągnięcie w pełni spełnia wymogi stawiane w procesie habilitacyjnym.

3. Ocena dorobku naukowego

Doktor inżynier Marek Pawlicki uzyskał w roku 2011 tytuł magistra w Wyższej Szkole Informatyki w Łodzi. W roku 2020 obronił doktorat w dyscyplinie informatyka techniczna i telekomunikacja na Uniwersytecie Technologiczno-Przyrodniczego im J. i J. Śniadeckich w Bydgoszczy.

W bazie w bazie WoS indeksowanych jest 67 publikacji Habilitanta, w Scopus 104, w Goole Scholar 112 prac. Indeks Hirsha wg.: WoS - 13, Scopus – 17, Google Scholar – 22. Liczba cytowani wg.: WoS – 680 (bez autocytowań – 538), Scopus – 1124 (bez autocytowań – 853), Google Scholar – 1745. Warto zwrócić uwagę, że zdecydowana

większość dorobku naukowego została uzyskana po doktoracie, czyli od lipca 2020 roku. Według mnie jest to poziom zdecydowanie wyróżniający na tym etapie rozwoju naukowego i wskazuje na bardzo wysoki wkład opublikowanych prac habilitanta do dziedziny.

Habilitant odbył trzymiesięczny staż naukowy na Uniwersytecie Neapolitańskim „Parthenope" w Neapolu we Włoszech, gdzie prowadził badania naukowe dotyczące zastosowania sztucznej inteligencji w cyberbezpieczeństwie. W trakcie stażu opracował nową metodę zwiększania odporności systemów wykrywania włamań na ataki typu adversarial. Uzyskane wyniki zostały zaprezentowane podczas prestiżowej konferencji ESORICS 2024 (CORE A). Warto dodać, że habilitant współpracuje z czołowymi zespołami badawczymi w dziedzinie cyberbezpieczeństwa w Polsce – z Politechniką Warszawską oraz Politechniką Wrocławską.

Wartym zauważenia jest uczestnictwo Habilitanta jako wykonawcy w 11 projektach badawczo-rozwojowych (10 po doktoracie) finansowanych ze środków europejskich w ramach programów Horyzont 2020 (9), NCBiR (1) oraz NAWA (1). W tych projektach pełnił głownie rolę Eksperta: AI, xAI oraz cyberbezpieczeństwa. Zdecydowanym plusem jest fakt, że większość z tych projektów realizowana była w szerszej współpracy naukowej z ośrodkami zagranicznymi. Udział w takiej liczbie projektów jest bardzo dobrym osiągnięciem i wskazuje między innymi na dużą umiejętność habilitanta pracy w międzynarodowych zespołach badawczych.

Innym aspektem wyróżniającym jest fakt, że duża część prowadzonych badań w projektach realizowana była z partnerami z przemysłu (Orange Polska, CESNET Czechy, Telprom Słowenia, RoEduNet Rumunia, Collins Aerospace Irlandia) i miała swoje zastosowanie w produktach oferowanych przez te firmy. Moim zdaniem tego typu badania przemysłowe są szczególnie cenne i warto podkreślenia. Zebrane doświadczenia w takich projektach będą mogły w przyszłości zaowocować skuteczną pracą nad nowymi technologiami, które dalej będą stanowiły podstawę do nowych produktów technologicznych.

Podsumowując, oceniam dorobek naukowy habilitanta jako wyróżniający i w pełni spełniający wymagania stawiane w procesie habilitacyjnym.

4. Ocena dorobku dydaktycznego i popularyzatorskiego

Doktor inżynier Marek Pawlicki został dziesięciokrotnie nagrodzony za osiągnięcia naukowe. Szczególnie warto zwrócić uwagę na uzyskane w 2024 Stypendium Ministra Nauki dla wybitnych młodych naukowców.

ul. Jagiellońska 57/59
03-301 Warszawa

tel 22 519 21 00
akademia@kozminski.edu.pl

kozminski.edu.pl

Istotnym aspektem działalności akademickiej habilitanta jest zaangażowanie w opiekę nad pracami dyplomowymi na poziomie magisterskim i inżynierskim. Efektem wysokiej jakości tej współpracy jest fakt, że habilitant jest współautorem kilku publikacji naukowych o zasięgu międzynarodowym, które powstały we współpracy ze studentami. Świadczy to o wysokim poziomie merytorycznym prowadzonych prac dyplomowych oraz ich związku z aktualnymi i istotnymi problemami badawczymi.

Habilitant aktywnie angażuje się również w popularyzację nauki, wygłaszając liczne wykłady i prelekcje poświęcone zagadnieniom sztucznej inteligencji (AI) oraz wyjaśnialnej sztucznej inteligencji (xAI) w kontekście cyberbezpieczeństwa. Na szczególne podkreślenie zasługuje fakt, że występował jako mówca typu keynote na kluczowych międzynarodowych konferencjach z zakresu cyberbezpieczeństwa, takich jak ARES 2024 oraz ESORICS 2024, co świadczy o jego uznanej pozycji w środowisku naukowym.

Warto zwrócić uwagę na działalność doktora inżyniera Marka Pawlickiego jako członka komitetów naukowych oraz organizacyjnych wielu międzynarodowych konferencji naukowych. Wśród nich można wymienić: ESORICS (2024(, IP&C (2023, 2021), ICCCI (2024), ARES (2024, 2023, 2022), ENS (2022, 2023, 2024), ICIC (2022, 2021), EICC 2021.

O wysokiej rozpoznawalności naukowej habilitanta świadczy fakt wykonania wielu recenzji dla czasopism oraz konferencji naukowych, w tym tych z listy JCR posiadających IF powyżej 5, czyli: Future Generation Computer Systems (Elsevier) (IF=6.2), Artificial Intelligence Review (Springer) (IF=10.7), Applied Soft Computing (Elsevier) (IF=7.2), Neurocomputing (Elsevier) (IF=5.5).

Bardzo wysoko oceniam działalność dydaktyczną i popularyzatorską habilitanta, który aktywnie uczestniczy w życiu społeczności naukowej oraz angażuje się we wspieranie młodej kadry akademickiej.

5. Konkluzja końcowa

Biorąc pod uwagę osiągnięcia związane z przedstawionym cyklem publikacji oraz dorobkiem naukowym, stwierdzam, że wymagania określone w art. 219 ust. 1 pkt. 2 i 3 ustawy „Prawo o szkolnictwie wyższym i nauce" zostały w pełni spełnione i wnioskuję o dopuszczenie doktora inżyniera Marka Pawlickiego do dalszych etapów postępowania habilitacyjnego w dyscyplinie informatyka techniczna i telekomunikacja, w dziedzinie nauk inżynieryjno-technicznych.

dr hab. Bogdan Księżopolski