

Szczecin, 12.01.2026 r.

prof. dr hab. inż. Krzysztof Okarma  
Katedra Przetwarzania Sygnałów i Inżynierii Multimedialnej  
Wydział Elektryczny  
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

**SEKRETARIAT**  
Rady Dyscypliny AEEITK

Wpłynęło dnia ...20.01.2026

Zarejestrowano pod nr ...510.6.5/25

Podpis ..... *Jm*

**RECENZJA ROZPRAWY DOKTORSKIEJ**  
**dla Rady Dyscypliny Automatyka, Elektronika, Elektrotechnika i Technologie Kosmiczne**  
**Akademii Górniczo-Hutniczej im. Stanisława Staszica w Krakowie**

*opracowana na podstawie uchwały nr 159/2025 Rady Dyscypliny Automatyka, Elektronika, Elektrotechnika i Technologie Kosmiczne Akademii Górniczo-Hutniczej im. Stanisława Staszica w Krakowie z dnia 6.11.2025 r. oraz wynikającego z niej pisma Przewodniczącego Rady Dyscypliny dr. hab. inż. Ryszarda Sroki, prof. AGH*

Tytuł rozprawy: **Elektroniczne Systemy Zabezpieczenia Technicznego jako źródło danych w procesie automatycznej obrony przed cyberatakami oraz wykrywania sprawcy przestępstwa**

Autor rozprawy: **mgr inż. Jan Kapusta**

Dyscyplina naukowa: **automatyka, elektronika, elektrotechnika i technologie kosmiczne**

Promotor: **prof. dr hab. inż. Jerzy Baranowski**

Promotor pomocniczy: **dr inż. Waldemar Bauer**

**I. TEMATYKA, TEZA NAUKOWA I CEL ROZPRAWY**

Rozprawa doktorska mgr. inż. Jana Kapusty pt. „Elektroniczne Systemy Zabezpieczenia Technicznego jako źródło danych w procesie automatycznej obrony przed cyberatakami oraz wykrywania sprawcy przestępstwa” została zrealizowana w ramach programu Doktorat Wdrożeniowy, w dyscyplinie naukowej *automatyka, elektronika, elektrotechnika i technologie kosmiczne*. Wybór tej dyscypliny należy uznać za w pełni uzasadniony, choć w pracy znajdują się pewne elementy nieco bliższe dyscyplinie *informatyka techniczna i telekomunikacja*. Stanowi to jednak dodatkowe wzbogacenie pracy, nie wpływając w żaden sposób na postrzeganie jej tematyki jako aktualnej i dobrze odpowiadającej dyscyplinie naukowej, w której Kandydat ubiega się o nadanie stopnia doktora.

Zagadnienia cyberbezpieczeństwa stały się w ostatnich latach kluczowymi elementami związanymi z ochroną zarówno infrastruktury technicznej, w tym krytycznej, jak również systemów informatycznych, co we wciąż rosnącym zakresie ma miejsce z użyciem metod sztucznej inteligencji. Połączenie aspektów analizy bezpieczeństwa w bardziej tradycyjnym rozumieniu z nowoczesnymi rozwiązaniami z zakresu cyberbezpieczeństwa i ochrony informacji wpisuje się zatem w naturalny nurt rozwoju badań, łączący

w sobie pewne elementy obu wcześniej wymienionych dyscyplin naukowych. Kandydat postawił tezę dotyczącą możliwości opracowania kompleksowego modelu cyber-fizycznych systemów ochrony, uwzględniającego w holistyczny sposób zarówno degradację komponentów, jak również zagrożenia cybernetyczne i kontekst operacyjny. W celu jej udowodnienia zaproponował trójwarstwowe rozwiązanie, w którym warstwa detekcji (percepcyjna) ma za zadanie kontekstową analizę planów architektonicznych, warstwa druga (decyzyjna) określa grafy ścieżek ataku z uwzględnieniem m.in. wskaźników degradacji, zaś ostatnia warstwa raportująca została zautomatyzowana przy użyciu dużych modeli językowych (LLM).

Kandydat zaproponował probabilistyczny model degradacji elektronicznych systemów zabezpieczenia technicznego, a także rozszerzenie metodyki EASI (ang. *Estimated Adversary Sequence Interruption*) poprzez użycie komponentów cyberodporności oraz degradacji komponentów, rozwijając również narzędzia automatycznej kontekstowej interpretacji symboli technicznych. Rozwiązania te zostały zaimplementowane w narzędziu AI-SecPA (pełna nazwa *AI - Security Path Analyzer*), co pozwoliło na udowodnienie postawionej tezy badawczej.

## II. OCENA ZAWARTOŚCI MERYTORYCZNEJ ROZPRAWY I UWAGI DYSKUSYJNE

Recenzowana rozprawa doktorska mgr. inż. Jana Kapusty dotyczy istotnego we współczesnych realiach problemu, jakim jest zapewnienie bezpieczeństwa w budynkach, zarówno pod względem fizycznym, jak też z uwzględnieniem aspektów cyberbezpieczeństwa. Niewątpliwie efektywne połączenie obu tych aspektów nie jest zagadnieniem oczywistym ani trywialnym, co pozwoliło zidentyfikować luki badawcze, których próbę wypełnienia podjął Kandydat. Doktorant trafnie przeanalizował możliwe do zastosowania technologie, dokonując wyboru szeregu algorytmów i innych rozwiązań prowadzących do opracowania prototypowego funkcjonalnego rozwiązania. Dążąc do możliwie największej automatyzacji proponowanego systemu, zastosował sieć neuronową, używając popularnego algorytmu YOLO do detekcji i klasyfikacji różnych elementów na planach budynków. Co prawda użycie tego znanego rozwiązania nie nosi znamion nowości pod względem naukowym, jednak zauważyć można dodatkowe elementy związane z analizą relacji przestrzennych i funkcjonalnych, zaproponowane w rozprawie. Istotnym usprawnieniem z punktu widzenia użytkownika jest również integracja z innymi systemami, w tym BIM (*Building Information Modelling*). Szkoda jednak, iż – jak wskazano na str. 62 – nie zapewniono odporności metody względem orientacji obiektów, gdyż wymóg niezmienniczości względem transformacji geometrycznych nie powinien stanowić zbyt dużego wyzwania dla współczesnych metod rozpoznawania kształtów opartych na głębokich sieciach neuronowych. Warto byłoby rozważyć celowość użycia innych znanych architektur sieci w tym zakresie, jak również wziąć pod uwagę ewentualność powiększenia zbioru uczącego wraz z dodatkową augmentacją danych w celu zwiększenia odporności na rotację. W klasycznych metodach analizy obrazów możliwym rozwiązaniem jest konwersja układu współrzędnych do postaci biegunowej, warto rozważyć również zastosowanie wybranych metod przetwarzania wstępnego, tak aby w pewnym stopniu skompensować niedostatki użytego algorytmu. Jak zauważa sam Doktorant na str. 65, „*Implementacja technik augmentacji danych obejmujących rotacje, skalowanie i transformacje perspektywiczne mogłaby znacząco poprawić odporność systemu na różnorodne orientacje symboli występujące w rzeczywistych planach architektonicznych*”, a zatem zdziwienie budzi fakt, iż techniki te nie zostały zastosowane w pracy. Byłoby to na pewno zadanie prostsze aniżeli wskazana również w pracy możliwość integracji z systemami rzeczywistości wirtualnej i rozszerzonej. Wskazane w sekcji 3.10 „osiągnięcia” trudno co prawda uznać za nowatorskie pod względem naukowym, gdyż stanowią w zasadzie funkcjonalności lub cechy stworzonego systemu, jednak wskazują one na kluczowe elementy pierwszej warstwy zaproponowanego rozwiązania.

Kolejnym istotnym elementem rozprawy jest koncepcja zastosowania teorii grafów do heurystycznej oceny ścieżek ataku z użyciem uprzednio rozpoznanych i sklasyfikowanych elementów budynku na podstawie automatycznej analizy jego planów. Jest to możliwe dzięki zaproponowanemu w rozprawie ustrukturyzowaniu pozyskanych informacji z użyciem grafów. Kandydat przedstawił wprowadzenie do teorii grafów, które zawiera znane informacje – można się domyślić, iż celem tej części pracy jest głównie wprowadzenie mniej zorientowanego Czytelnika w tematykę związaną z zastosowaniem grafów. Kandydat we właściwy sposób uzasadnił wybór grafów skierowanych i ograniczenie dalszych analiz do tej grupy, wskazując na typowe rozwiązania architektoniczne, takie jak jednokierunkowe drzwi awaryjne, systemy kontroli dostępu, czy też bariery przeciwpożarowe. Sposób przedstawienia informacji w rozdziale 4. dotyczącym grafów, a także w kolejnych, nie jest niestety typowy dla rozpraw doktorskich – często jest to zestaw pojęć, czy też definicji, co znacząco utrudnia lekturę rozprawy ze względu na brak logicznego związku pomiędzy kolejnymi zdaniami, a często równoważnikami zdań. W wielu miejscach struktura zdań jest zaburzona, zwłaszcza w wyliczeniach – brakuje znaków przestankowych, kolejne elementy wyliczeń w obrębie jednego zdania rozpoczynają się wielką literą, często zdarzają się niewłaściwe końcówki fleksyjne (np. w pierwszym zdaniu na str. 90, podobne niezgodności występują także w kolejnych częściach pracy, np. w wyliczeniach na str. 112 czy też str. 114, czy też na str. 135). W niektórych miejscach brak jest związku logicznego pomiędzy kolejno przedstawianymi pojęciami. Nie jest jasne, co Doktorant rozumie przez sformułowanie „bogatszą propagację gradientów” użyte na str. 52, na której znajduje się więcej pojęć wymagających wyjaśnienia. Innym przykładem są „specjalne augmentacje” (str. 53) – nie jest w żaden sposób wyjaśnione, na czym ta „specjalność” polega. W wielu miejscach tekstu w polskie zdania niezbyt fortunnie wplecione zostały angielskie nazwy, co sprawia wrażenie swoistej „slangowości” tekstu – przykładem może być „baseline” (str. 73). Takie sformułowania, jak znajdujące się na str. 57 „równoległe trajektorie loss treningowego i walidacyjnego”, nie powinny w tekście występować. Na tej samej stronie znajduje się również fragment zawierający puste podsekcje, w których nie ma żadnego tekstu (Studia porównawcze, Wpływ strategii treningu, Wpływ post-processingu).

Pomimo iż nie są to uwagi natury merytorycznej, a raczej technicznej (niektóre z nich zostały wymienione w dalszej części recenzji), to są one na tyle istotne, iż nie pozwalają na wysoką ocenę stopnia opanowania umiejętności redagowania prac naukowych przez Kandydata, choć zauważyć należy, iż w tych fragmentach pracy, w których zachowany został styl typowy dla rozpraw doktorskich, praca jest napisana poprawnym językiem, bez istotnych błędów.

Na początku rozdziału 4. Doktorant stwierdza, iż w rozdziale poprzednim została opisana automatyczna detekcja elementów z wykorzystaniem algorytmów komputerowej analizy obrazu, podczas gdy właściwie analiza ta jest ograniczona do metody YOLO. Szkoda, że nie zostały przedstawione inne metody detekcji, co na pewno wzbogaciłoby dodatkowo pracę. Należy zgodzić się z uwagą zamieszczoną na str. 74, iż szczegółowe przedstawienie wielu z metod wykracza poza ramy opracowania, jednak trudno uznać formę ich prezentacji za właściwą. Bliższego wyjaśnienia wymagałoby stwierdzenie, iż „czas całkowity pokonania ścieżki ataku stanowi splot czasów pokonania poszczególnych elementów” (str. 83) – interesujące byłoby pokazanie przykładu, w jaki sposób można taki czas można wyznaczyć dla systemu przedstawionego w rozprawie. W podsumowaniu rozdziału 4. (podrozdział 4.11) Doktorant pisze o przedstawionej „analizie teoretycznej”, jednak rozdział ten ma niestety charakter bardziej hasłowy niż typowy dla takich analiz.

Ciekawym fragmentem pracy jest rozdział 5., w którym omówione zostały duże modele językowe (LLM). Niestety również w tym rozdziale Doktorant nie ustrzegł się pewnych potknięć językowych, niepotrzebnie pisząc np. „Pretrening (unsupervised)” zamiast „Nienadzorowane uczenie wstępne”, czy też „proces fine-tuningu” zamiast „dopasowania” lub „dostrajania” (str. 93). Interesujące byłoby odniesienie się Kandydata do problemu zagrożenia tzw. „halucynacjami” modeli LLM w kontekście systemu przedstawianego

w rozprawie wraz z informacją, czy niebezpieczeństwo takie było analizowane. Ponadto, celowe byłoby przeanalizowanie aspektu wyjaśnialności w kontekście wykrywania wzorców i anomalii z użyciem LLM, wspomnianej na str. 99 rozprawy jako przewaga nad metodami klasycznymi, co jest dość dyskusyjne.

Na str. 105 Autor rozprawy stwierdził, iż zastosowany został „jeden z wiodących modeli LLM”, nie wskazując żadnego konkretnego narzędzia. Proszę o doprecyzowanie tego podczas obrony pracy wraz z przedstawieniem motywacji dokonanego wyboru.

Ważną częścią rozprawy w kontekście realizacji doktoratu wdrożeniowego jest opis implementacji narzędzia AI-SecPA przedstawiony w rozdziale 6. W rozdziale 7. Doktorant przedstawił konkluzje, wymieniając swoje główne osiągnięcia badawcze, m.in. wskazując, iż zaproponował w swej rozprawie zintegrowane i dynamiczne podejście do oceny efektywności Cyber-Fizycznych Systemów Ochrony, łącząc perspektywę probabilistyczną, uczenie maszynowe oraz wykorzystanie dużych modeli językowych (LLM), co przyczynia się do otwarcia nowych obszarów badawczych związanych z inżynierią bezpieczeństwa oraz dyscypliną naukową, w której zrealizowana została recenzowana rozprawa, tj. *automatyka, elektronika, elektrotechnika i technologie kosmiczne*. Dodatkowej wartości pracy upatrywać należy w kompleksowym interdyscyplinarnym podejściu do analizowanego zagadnienia, które pozwoliło jednakże stworzyć spójną metodykę, umożliwiającą różne aplikacje zaproponowanego systemu. Ważnym elementem jest także sformalizowanie problemu degradacji cyber-fizycznych systemów ochrony.

Doktorant trafnie wskazał kierunki dalszego rozwoju opracowanego rozwiązania, np. możliwości związane z uwzględnieniem specyfiki różnego rodzaju budynków, chociaż brak implementacji niektórych z nich pozostawia pewien niedosyt. Przykładem może być niemożność dokonywania analizy przestrzennej budynków ze względu na ograniczenie do pojedynczych kondygnacji, wynikające głównie ze sposobu automatycznej analizy obrazów planów architektonicznych.

Praca opatrzona jest bogatą bibliografią, liczącą 165 pozycji, w większości ściśle związanych z tematyką rozprawy, w której zdarzają się drobne usterki związane z formatowaniem niektórych pozycji (głównie są to braki wielkich liter wynikające w dużej mierze z użycia menedżera bibliografii).

Pomimo znacznej liczby uwag krytycznych, dotyczących głównie sposobu prezentacji treści, uważam, iż pod względem merytorycznym można ocenić przedstawioną pracę pozytywnie, zwłaszcza biorąc pod uwagę kontekst jej realizacji w ramach programu „Doktorat Wdrożeniowy”.

### III. UWAGI SZCZEGÓŁOWE

W pracy pojawiają się dość liczne błędy edytorskie, uwagę zwraca także brak numeracji wzorów, a także kropek lub przecinków po nich, jeśli stanowią część zdania, nieuzasadnione są także wcięcia przed słowem „gdzie” znajdującym się bezpośrednio po wzorze. Zdarzają się pozostawione na końcach wierszy jednowyrazowe słowa (tzw. „sieroty”). W wielu miejscach brakuje spacji po zakończeniu cudzysłowów. Rażąco jest nagminne używanie liczby mnogiej w odniesieniu do wykonanych prac (uznaliśmy, traktujemy, postanowiliśmy, zrealizowaliśmy, zaproponowaliśmy itp.). Przedstawiona do oceny praca doktorska jest opracowaniem samodzielnym, zatem nawet jeśli przedstawiane są w niej fragmenty prac współautorskich, to Kandydat powinien skupiać się na przedstawieniu swojego wkładu, stąd zastosowanie liczby mnogiej może budzić wątpliwości dotyczące rzeczywistego wkładu Doktoranta w przedstawiane wyniki badań. Publikacje współautorskie z promotorem i promotorem pomocniczym związane z tematyką realizowanego doktoratu są zupełnie naturalne, jednak taki sposób ich prezentacji w rozprawie doktorskiej, która nie ma formy zbioru powiązanych tematycznie publikacji z oświadczeniami współautorów, nie jest właściwy.

Innym istotnym problemem jest sposób opisu niektórych rysunków zamieszczonych w rozprawie, gdzie Kandydat wskazuje na „opracowanie własne na podstawie [x]”, wskazując jako źródło współautorską publikację, w której znajduje się identyczny rysunek. Takie stwierdzenie nie jest w takiej sytuacji w żaden sposób uzasadnione, ponieważ nie została dokonana żadna zmiana w rysunku – powinno tam się znaleźć zwykle cytowanie właściwej pozycji bibliograficznej. Można się domyślać, iż taki sposób opisu miał na celu wskazanie, iż to Doktorant (a nie żaden ze współautorów) był autorem poszczególnych rysunków, jednak nie zmienia to faktu niepoprawnego odniesienia się do źródła. Kuriozalne jest także odniesienie się w ten sam sposób w rysunku 3.2 do pozycji bibliograficznej [27], ponieważ publikacja taka we wskazanym czasopiśmie (*Sensors*) ostatecznie nigdy się nie ukazała. Podobny artykuł autorstwa Doktoranta wraz z promotorem i promotorem pomocniczym ukazał się za to w innym czasopiśmie (*Algorithms*) tego samego wydawnictwa, jednak zapewne już po złożeniu rozprawy doktorskiej. Zawiera on identyczny rysunek, a zatem odniesienie się do materiału źródłowego w tym przypadku jest niewłaściwe.

Wspomniany już sposób prezentacji niektórych treści w połączeniu z powyższymi uwagami, niestety znacząco obniża całościową ocenę rozprawy doktorskiej, która powinna nie tylko demonstrować umiejętność samodzielnego rozwiązywania problemów naukowych, ale także opanowanie sposobu opisu oraz dokumentacji uzyskiwanych wyników. Można odnieść wrażenie, iż przedstawiony dokument miejscami ma charakter bardziej raportu technicznego aniżeli rozprawy doktorskiej. Zbyt dużo jest także sformułowań o charakterze dywagacyjnym („mogłyby”, „wydaje się” – zwrot ten występuje w rozprawie kilkanaście razy). Rozprawa doktorska powinna być wolna od tego rodzaju sformułowań, zamiast których oczekiwane są przede wszystkim stwierdzenia o zdecydowanie większym stopniu konkretności, wynikające przede wszystkim z przeprowadzonych badań.

W pracy znajduje się pewna liczba potknięć językowych, spośród których wymienione zostały tylko niektóre, np. „przetwarzanie przekraczające 30 klatek na sekundę” (na str. 61 – powinna być: prędkość przetwarzania), „podczas analizy dużych portfeli obiektów” (również na str. 61), rozpoczęcie zdania od słowa „natomiast” (str. 62), „system osiąga praktycznie perfekcyjne wyniki” (str. 62 – czyli właściwie jakie wyniki?). Na str. 62 znajduje się także obszerny powtórzony fragment tekstu, a także inny, który wygląda na wcześniejszą wersję podpisu pod rysunkiem (powinien być usunięty). Z kolei zamiast sformułowania „niezmiennność względem transformacji” lepiej byłoby użyć zwrotu „niezmienniczość”, podobnie jak „analizy obrazu” zamiast „analitiky obrazu” (str. 14). W wyliczeniu na str. 75 brak jest odmiany wyrazów i ciągłości zdania. Niektóre anglojęzyczne skróty nie zostały wyjaśnione i rozwinięte przy pierwszym użyciu, np. ASS na str. 14, czy NMS oraz IoU na str. 51, bądź HVAC (str. 86). W pracy zdarzają się też kalki językowe np. „pozwoliła nam znaleźć ten etap jako dobry punkt wyjścia” (str. 41) czy „znaleźliśmy [...] metodę jako obiecującą” (str. 42) „rafinację detekcji” (str. 50), jak też typowe dla języka angielskiego używanie przecinka jako separatora tysięcy (np. na str. 46, 47, 92, czy 135), co nie powinno mieć miejsca w pracy pisanej w języku polskim, podobnie zresztą jak używanie skrótu „vs.”, czy też nadużywanie słowa „versus” (str. 76), w środku zdania w języku polskim. Podobna uwaga dotyczy nieoczywistego skrótu „s.t.” (*such that*) we wzorze na str. 76, czy też zwrotu „naruszających określone constraints” (str. 96) zamiast użycia słowa „ograniczenia”. W kilku miejscach zamiast słowa „perymetryczne” użyte jest słowo „perimetryczne”, zamiast „Chebysheva” w języku polskim używa się zapisu „Czebyszewa”, zamiast „Markova” – „Markowa”, natomiast nazwisko „Bentley” powinno być zawsze odmieniane (str. 81). Zamiast „optymalizacji wielokryterialnej” częściej stosuje się pojęcie „optymalizacji wielokryterialnej”, z kolei zamiast „przestrzeni wysokowymiarowej” raczej operuje się pojęciem „przestrzeni wielowymiarowej”. Usterkę o zbliżonym charakterze jest w rozprawie więcej, jednakże nie jest celowe wymienianie ich wszystkich.

Powyższe uwagi wpływają niestety nieco na ogólną ocenę pracy, jednak – jak wspomniano wcześniej – nie podważają jej merytorycznych zalet, co stanowi najważniejszy aspekt rozprawy.

#### IV. WNIOSKI KOŃCOWE

Recenzowana rozprawa stanowi rozwiązanie problemu naukowego o charakterze wdrożeniowym z elementami interdyscyplinarności, wpisując się jednak głównie w dyscyplinę naukową *automatyka, elektronika, elektrotechnika i technologie kosmiczne*, w której Kandydat realizował kształcenie w ramach programu „Doktorat Wdrożeniowy”.

Stwierdzam, iż przedstawiona do recenzji rozprawa doktorska **mgr. inż. Jana Kapusty** pt. *„Elektroniczne Systemy Zabezpieczenia Technicznego jako źródło danych w procesie automatycznej obrony przez cyberatakami oraz wykrywania sprawcy przestępstwa”*, której promotorem jest prof. dr hab. inż. Jerzy Baranowski a promotorem pomocniczym dr inż. Waldemar Bauer, zrealizowana w dziedzinie nauk inżynieryjno-technicznych w dyscyplinie *automatyka, elektronika, elektrotechnika i technologie kosmiczne*, pomimo licznych uwag krytycznych, w wystarczającym stopniu **spełnia wymagania stawiane rozprawom doktorskim** przez aktualnie obowiązującą ustawę *Prawo o szkolnictwie wyższym i nauce* z dnia 20 lipca 2018 roku (tekst jednolity Dz. U. z 2024 r. poz. 1571). **Wniosuję zatem o jej przyjęcie i dopuszczenie do publicznej obrony.**

