prof. dr hab. inż. Zbigniew Ciekanowski
Akademia Sztuki Wojennej

Warszawa dn. 28.10.2025 r.

RECENZJA
ROZPRAWY DOKTORSKIEJ

mgr. Jacka CZECHA

opracowanej pod tytułem

SYSTEM BEZPIECZEŃSTWA INFORMACJI W INSTYTUCJI PUBLICZNEJ NA PRZYKŁADZIE CENTRUM TECHNOLOGII BEZPIECZEŃSTWA

1. Ocena ogólna

Na podstawie uchwały nr 56/NOB/2025 Rady Naukowej Dyscypliny Nauk o Bezpieczeństwie Uniwersytetu Kaliskiego im. Prezydenta Stanisława Wojciechowskiego z dnia 25 września 2025 roku w sprawie powołania recenzentów postępowaniu w sprawie nadania stopnia doktora w dziedzinie nauk społecznych w dyscyplinie nauki o bezpieczeństwie, dokonano oceny rozprawy doktorskiej. Celem przedmiotowej recenzji jest ocena przedłożonej rozprawy doktorskiej pod kątem spełnienia wymagań określonych w artykule 187 Ustawy z dnia 20 lipca 2018 roku – Prawo o szkolnictwie wyższym (Dz.U. 2024 poz. 1571).

Rozprawa doktorska pod tytułem *System bezpieczeństwa informacji w instytucji publicznej na przykładzie centrum technologii bezpieczeństwa*, *napisana* przez magistra Jacka CZECHA, pod kierunkiem naukowym profesora doktora habilitowanego inżyniera doktora honoris causa Jarosława WOŁEJSZO oraz promotora pomocniczego doktora inżyniera Łukasza FABERA, jest niewątpliwie interesująca z naukowego punktu widzenia. Tematyka dysertacji odnosi się do analizy zagadnień organizacyjnych, technicznych i prawnych

związanych z bezpieczeństwem informacji w instytucjach publicznych, ze szczególnym uwzględnieniem środowiska akademickiego. Badając problematykę, Autor poddał analizie obowiązujące regulacje prawne, standardy i procedury w zakresie ochrony informacji, a także praktyczne rozwiązania stosowane w jednostkach sektora publicznego. Doktorant skoncentrował uwagę na procesach zapewniania bezpieczeństwa danych i funkcjonowania systemów informatycznych w uczelniach wyższych, wskazując na potrzebę ich automatyzacji oraz integracji z obowiązującymi przepisami i normami bezpieczeństwa.

Praca w swoim wymiarze poznawczym przyczyniła się do pogłębienia wiedzy o funkcjonowaniu systemów ochrony informacji w instytucjach publicznych oraz o możliwościach ich doskonalenia w kontekście współczesnych wyzwań technologicznych i legislacyjnych. Autor wykazał się szeroką znajomością problematyki bezpieczeństwa informacji, łącząc analizę teoretyczną z badaniami empirycznymi przeprowadzonymi w wybranych jednostkach sektora akademickiego. W badaniach zastosowano podejście analityczno-diagnostyczne, wykorzystując metody sondażu diagnostycznego. Opracowanie ma charakter interdyscyplinarny, łącząc zagadnienia nauk o bezpieczeństwie, zarządzania oraz technologii informacyjnych, co nadaje mu walor zarówno naukowy, jak i aplikacyjny.

Doktorant na wstępie przedstawia sytuację problemową i uzasadnia aktualność podejmowanej tematyki badawczej. Autor wychodzi naprzeciw konieczności uzupełnienia tematyki funkcjonowania systemu bezpieczeństwa informacji w instytucjach publicznych – zarówno od strony teoretycznej, jak i rekomendacji dla poprawy jego funkcjonowania. Warto zaznaczyć kilkunastoletnie doświadczenie zawodowe Doktoranta w omawianej tematyce, które bez wątpienia pozwoliło na odniesienie ustaleń pozyskanych w toku badania do własnych spostrzeżeń i refleksji dotyczących wybranego fragmentu rzeczywistości.

Wskazane połączenie teorii i praktyki przez Badacza tematu powoduje, że analizowana treść rozprawy naukowej jest niewątpliwie interesująca w swej jakościowej płaszczyźnie. Jej szczególnym walorem jest praktyczne ukierunkowanie rozważań oraz możliwość wykorzystania zaproponowanych rozwiązań w działalności instytucji publicznych. W opinii Autora kluczowe znaczenie ma stworzenie takiego systemu bezpieczeństwa informacji, który pozwalałby na skuteczną automatyzację procesów reagowania na incydenty oraz integrację działań organizacyjnych, technicznych i prawnych. Istotne jest również zapewnienie współdziałania pomiędzy różnymi poziomami zarządzania bezpieczeństwem – od struktur uczelnianych po administrację publiczną – w celu osiągnięcia spójności procedur, efektywności wymiany informacji oraz racjonalnego wykorzystania zasobów w procesie ochrony danych i reagowania na zagrożenia.

W ciekawej treściowo dysertacji daje się zauważyć etapowość prowadzonej narracji i argumentacji. Całość opisu procesu badawczego jest opracowana poprawnie, co unaocznia umiejętności Autora w kwestiach właściwego kształtowania procedury poznawczej. To z kolei jest konieczne przy dokumentowaniu przygotowania autorskiego do pełnienia funkcji przypisywanych pracownikowi naukowemu i tym samym merytorycznej zasadności uzyskania pierwszego stopnia naukowego.

Już na etapie uzasadnienia wyboru tematu, Autor przedstawia rolę instytucji akademickich jako kluczowych podmiotów w tworzeniu i wdrażaniu innowacyjnych rozwiązań w zakresie bezpieczeństwa danych, podkreślając ich odpowiedzialność za rozwój skutecznych systemów ochrony informacji. Wskazuje ponadto, że współczesne uczelnie, jako centra nauki i innowacji, powinny inwestować w kompetencje technologiczne, organizacyjne i strategiczne, by sprostać wyzwaniom XXI wieku. Zwraca uwagę na znaczenie regulacji prawnych, takich jak RODO czy dyrektywa NIS2, a także na wpływ sztucznej inteligencji i zjawiska dezinformacji na bezpieczeństwo informacyjne. W pracy autor przedstawia zarówno część teoretyczną, obejmującą analizę norm, regulacji i modeli zarządzania bezpieczeństwem informacji, jak i część empiryczną, opartą na badaniach przeprowadzonych w Centrum Technologii Bezpieczeństwa AGH. We wnioskach autor podkreśla znaczenie opracowania skutecznych strategii ochrony danych, zwiększenia poziomu zabezpieczeń oraz podniesienia świadomości użytkowników systemów informacyjnych w środowisku akademickim.

Warto również zauważyć, że Autor wskazuje, iż bezpieczeństwo informacji stanowi jeden z kluczowych obszarów funkcjonowania instytucji publicznych w XXI wieku, zwłaszcza w kontekście postępującej cyfryzacji administracji, wzrostu zagrożeń cybernetycznych oraz zmian regulacji prawnych. Doktorant dostrzegł rosnącą potrzebą ochrony danych w środowisku akademickim, które – ze względu na swoją otwartość, wymianę wiedzy i międzynarodowy charakter – jest szczególnie narażone na utratę poufnych informacji. Uczelnie wyższe, charakteryzujące się złożoną i zdecentralizowaną strukturą, mają trudności w tworzeniu spójnych polityk bezpieczeństwa.

Autor podkreśla również, że instytucje publiczne przetwarzają ogromne ilości danych wrażliwych, co czyni bezpieczeństwo informacji kwestią strategiczną. Wskazuje cztery główne powody jej znaczenia: ochronę prywatności obywateli, zapewnienie bezpieczeństwa narodowego, stabilność administracji oraz zgodność z regulacjami międzynarodowymi. Zwraca uwagę na typowe zagrożenia, takie jak cyberataki (np. ransomware, phishing, DDoS, APT), luki w systemach IT, niski poziom świadomości użytkowników oraz zjawisko dezinformacji.

Trudno również nie zgodzić się z Autorem, iż prowadzenie badań w omawianym zakresie ma istotne znaczenie praktyczne – może przyczynić się do poprawy efektywności ochrony informacji, ograniczenia słabych punktów w systemach IT instytucji publicznych, zwiększenia świadomości pracowników oraz opracowania skuteczniejszych strategii bezpieczeństwa. Wobec rosnącej liczby zagrożeń cybernetycznych bezpieczeństwo informacji w środowisku akademickim powinno być traktowane jako jeden z kluczowych priorytetów współczesnej administracji publicznej.

2. Metodologiczna ocena rozprawy

Uwzględniając złożoność przedmiotu poznania należy stwierdzić, że Doktorant podjął się trudnego zadania, wymagającego rozległej i żmudnej pracy badawczej, związanej ze złożonością zdarzeń czy opinii przekładających się logicznie na obraz realnej przedmiotowo rzeczywistości. Analiza metodologiczna aspektów pracy doktorskiej wskazuje, iż jest ona skonstruowana poprawnie i odpowiada wymogom metodologicznym nauk społecznych. Dysertacja ma przejrzystą i logiczną strukturę, całość obejmująca 472 strony składa się z wstępu, czterech rozdziałów, zakończenia, bibliografii, spisu elementów graficznych oraz załączników (tj. narzędzi badawczych). Układ pracy jest konsekwentny i odpowiada wymogom naukowym stawianym opracowaniom o charakterze badawczym. Kolejność poszczególnych rozdziałów jest logiczna i wynika z toku prowadzonego procesu poznawczego.

We wstępie (zawartym na stronach 9-11) Doktorant wprowadził czytelnika do tematyki rozprawy doktorskiej oraz omówił znaczenie ochrony informacji w dobie dynamicznego rozwoju technologii cyfrowych oraz wzrostu zagrożeń cybernetycznych.

W rozdziale pierwszym (strony 12-30) pod tytułem *Metodologia badań,* Autor przedstawia uzasadnienie wyboru tematu, określa przedmiot i cel pracy oraz definiuje główny problem badawczy wraz z problemami szczegółowymi i hipotezami. Omawia zastosowane metody, techniki oraz narzędzia, a także charakteryzuje grupę respondentów oraz organizację i przebieg badań. Rozdział kończą wnioski z etapu metodologicznego, które stanowią punkt wyjścia do analizy empirycznej. Celem tej części jest stworzenie solidnych podstaw naukowych do weryfikacji postawionych hipotez dotyczących funkcjonowania systemów bezpieczeństwa informacji w środowisku akademickim.

Rozdział drugi (strony 31-232) zatytułowany *Teoria i praktyka funkcjonowania systemów bezpieczeństwa informacji w organizacji publicznej,* ma charakter teoretyczny

i obejmuje szerokie omówienie zagadnień związanych z bezpieczeństwem informacji w organizacjach publicznych. Autor analizuje istotę informacji i jej znaczenie jako zasobu, przedstawia modele bezpieczeństwa informacji, a także omawia aspekty prawne i normatywne związane z ochroną danych. Wskazuje na skuteczność prawa i jego wpływ na bezpieczeństwo informacji, przedstawia również współczesne wyzwania, takie jak aktywne przeciwdziałanie zagrożeniom, automatyzacja polityk bezpieczeństwa oraz wykorzystanie nowoczesnych technologii. W końcowej części rozdziału Doktorant analizuje funkcjonowanie systemów bezpieczeństwa informacji w środowisku akademickim oraz formułuje wnioski z przeprowadzonych rozważań.

W rozdziale trzecim (strony 233-379), pod tytułem *System bezpieczeństwa informacji w instytucji publicznej na przykładzie Centrum Technologii Bezpieczeństwa AGH,* Doktorant prezentuje wyniki badań empirycznych, a tym samym przedstawia analizę funkcjonowania systemu bezpieczeństwa informacji w środowisku akademickim, na przykładzie wybranego podmiotu. Autor opisuje specyfikę uczelni jako instytucji publicznej, analizując kontekst zagrożeń informacyjnych, strukturę organizacyjną oraz poziom bezpieczeństwa danych. Omawia główne obszary ryzyka, stan zabezpieczeń, strategie ochrony informacji oraz standardy obowiązujące w uczelni. W rozdziale przedstawiono również wyniki badań dotyczących świadomości użytkowników i skuteczności istniejących procedur bezpieczeństwa. Rozdział ten zakończony jest wnioskami, w których zidentyfikowano kluczowe problemy i potrzeby doskonalenia systemu bezpieczeństwa informacji w akademickim środowisku pracy.

Rozdział czwarty (strony 380-408) pod tytułem *Usprawnienia systemu bezpieczeństwa informacji w organizacji publicznej,* ma charakter aplikacyjny i zawiera propozycje usprawnień wynikające z wcześniejszych analiz i badań. Autor omawia znaczenie podnoszenia świadomości nowych zagrożeń, potrzebę aktywnego przeciwdziałania atakom oraz inwestowania w nowe technologie wspierające ochronę danych. Szczególną uwagę poświęca zmianom wynikającym z rozwoju sztucznej inteligencji i nowej roli procesów AI w kształtowaniu środowiska bezpieczeństwa informacji. Podobnie jak w poprzednich częściach pracy rozdział kończy się wnioskami (konkluzjami), odnoszącymi się do postawionej problematyki w tej części dysertacji.

W zakończeniu (umieszczonym na stronach 409-410), Doktorant dokonał syntetycznego podsumowania analizowanych treści oraz odniósł się do założeń badawczych na poziomie konceptualizacji, wskazując osiągnięcie celu badawczego.

Dysertacja w sposób kompleksowy obejmuje analizowany przedmiot badań oraz w pełni realizuje przyjęte założenia badawcze. Autor wnikliwie i rzetelnie opracował zarówno

część teoretyczną, jak i empiryczną, opierając swoje rozważania na szerokim przeglądzie literatury przedmiotu oraz bogatym materiale badawczym. Całość badań została przeprowadzona z zastosowaniem adekwatnych metod, technik i narzędzi, co zapewniło wysoką wartość poznawczą oraz wiarygodność uzyskanych wyników.

Analiza problemów badawczych zaprezentowanych w dysertacji pozwala stwierdzić, że stanowią one ambitne zadanie badawcze o charakterze deskrypcyjnym, eksplanacyjnym, diagnostycznym, jak i częściowo predyktywnym. Sformułowane problemy szczegółowe stanowią logiczny fundament procesu badawczego, nadając mu spójny kierunek oraz zapewniając przejrzystość, precyzję i merytoryczną trafność prowadzonych analiz.

Hipotezy robocze, przyjęte przez Doktoranta na potrzeby badań, korespondują zarówno z wyznaczonymi celami badań, jak i z problemami badawczymi, jak również są rozbudowane i szczegółowo opisane. Do rozwiązywania problemów oraz weryfikacji hipotez zastosowano podejście z wykorzystaniem teoretycznych i empirycznych metod badawczych.

Układ treści wykazuje logiczną ciągłość i spójność z przebiegiem procesu badawczego, a kolejność rozdziałów odzwierciedla naturalny tok poznania naukowego. Struktura wewnętrzna każdego z rozdziałów jest klarowna i konsekwentna, co umożliwia czytelne przedstawienie etapów badań oraz logiczne zaprezentowanie uzyskanych wyników.

Literatura przedmiotu (140 pozycji zwartych oraz periodycznych, 28 aktów prawnych, 62 źródła internetowe) dotycząca rozmaitych aspektów rozpatrywanej problematyki została dobrana i wykorzystana poprawnie. Obejmuje ona szeroki i zróżnicowany zestaw źródeł, od klasycznych opracowań teoretycznych po najnowsze publikacje naukowe dotyczące bezpieczeństwa informacji, cyberbezpieczeństwa i zarządzania ryzykiem w instytucjach publicznych. Uwzględniono w niej zarówno prace polskich, jak i zagranicznych autorów reprezentujących różne dziedziny nauki – nauki o bezpieczeństwie, zarządzanie, prawo, informatykę, socjologię oraz nauki techniczne. Znaczącą część stanowią monografie i artykuły naukowe poświęcone aspektom ochrony informacji, modelom bezpieczeństwa systemów IT, przeciwdziałaniu cyberatakom oraz wpływowi sztucznej inteligencji i dezinformacji na współczesne zagrożenia informacyjne. Widoczna jest również obecność literatury klasycznej z zakresu teorii informacji (m.in. Shannon, Wiener), publikacji metodologicznych (np. Babbie, Pilch) oraz pozycji odnoszących się do problematyki politycznej i strategicznej ochrony danych. Całość literatury została dobrana w sposób przemyślany i interdyscyplinarny, co wskazuje na szerokie ujęcie problemu badawczego oraz solidne podstawy teoretyczne dysertacji. Innymi słowy, można konkludować, że Doktorant wykazał, że nie tylko potrafi zgromadzić materiał badawczy, uporządkować i dokonać selekcji, lecz także posiada umiejętność swobodnego

prezentowania treści w formie pożądanej dla prac naukowych. Za wystarczający należy uznać zbiór tabel i rysunków, pozwalających zarówno na pełniejszy opis podejmowanych kwestii, jak i na zrozumienie analizowanego problemu.

Rekapitulując, należy stwierdzić na bazie przedstawionej do recenzji pracy, że Doktorant z całą pewnością jest przygotowany do samodzielnego prowadzenia badań.

3. Ocena merytoryczna

Recenzowana rozprawa doktorska stanowi zwarte i przemyślane opracowanie naukowe liczące 472 strony, w tym obszerną bibliografię, streszczenia oraz liczne załączniki dokumentujące przebieg badań.

Pod względem merytorycznym dysertacja wnosi do dorobku nauk o bezpieczeństwie istotne wartości poznawcze i aplikacyjne. Wypełnia zauważalną lukę badawczą w obszarze zintegrowanego podejścia do bezpieczeństwa informacji w instytucjach publicznych, ze szczególnym uwzględnieniem środowiska akademickiego. Autor w sposób systematyczny przeanalizował problematykę funkcjonowania systemów ochrony informacji, wskazując na uwarunkowania prawne, technologiczne oraz organizacyjne determinujące poziom bezpieczeństwa w sektorze publicznym. Wartość naukowa pracy przejawia się w kompleksowym ujęciu zjawiska, obejmującym analizę teoretyczną, studia przypadków oraz badania empiryczne. Wyniki badań potwierdzają zasadność przyjętych hipotez oraz pozwalają na sformułowanie praktycznych rekomendacji w zakresie podnoszenia odporności systemów informacyjnych na zagrożenia cybernetyczne i organizacyjne.

Autor przeprowadził również szeroką analizę literatury krajowej i zagranicznej, w której zidentyfikował brak syntetycznych opracowań dotyczących integracji działań z zakresu bezpieczeństwa informacji w środowisku uczelni wyższych. W analizie bibliograficznej uwzględniono publikacje z obszarów: zarządzania bezpieczeństwem informacji, cyberbezpieczeństwa, prawa ochrony danych, administracji publicznej, polityk bezpieczeństwa, a także aspektów edukacyjnych i technologicznych. Rozprawa trafnie wpisuje się w aktualne potrzeby badawcze i praktyczne, stanowiąc ważny głos w dyskusji nad modernizacją systemów bezpieczeństwa informacji w instytucjach publicznych i akademickich oraz dostarczając cennych wskazówek dla decydentów i praktyków odpowiedzialnych za rozwój polityki bezpieczeństwa w sektorze publicznym.

W zakończeniu dysertacji Doktorant podsumowuje przeprowadzone badania, umieszczając swoje spostrzeżenia z przeprowadzonego procesu poznawczego. Uzyskane wyniki pozwalają konstatować, że cel badań jaki został założony — osiągnięto.

Podczas wnikliwej analizy treści rozprawy dostrzec można pewne kwestie, które wymagają wyjaśnienia. Proszę o ich uściślenie:

1. W pracy wskazał Pan zastosowanie metody obserwacji uczestniczącej, jednak przedstawiony arkusz obserwacyjny (załącznik nr 6) ma charakter raczej opisowy i refleksyjny, i nie spełnia w pełni wymogów formalnych obserwacji naukowej. Wskazane spostrzeżenia odnoszą się przede wszystkim do doświadczeń zawodowych Autora i jego długotrwałej obserwacji środowiska akademickiego, co zwiększa wartość aplikacyjną pracy, lecz ogranicza jej rygor metodologiczny. Czy mógłby Pan wyjaśnić, na czym polega zasadnicza różnica między obserwacją naukową a refleksją opartą na doświadczeniu zawodowym? Jakie elementy metodologiczne należałoby wprowadzić, aby taka obserwacja spełniała kryteria naukowości?
2. W części metodologicznej zauważalne jest pewne nieporozumienie dotyczące klasyfikacji zmiennych i doboru testów statystycznych. Można odnieść wrażenie, że Autor utożsamia zmienne o charakterze liczbowym z ilościowymi (s. 26), co prowadzi do nie do końca adekwatnego zastosowania współczynnika korelacji R Pearsona. Zastosowanie w części empirycznej współczynników korelacji bez wątpienia świadczy o świadomości statystycznej Autora, jednak nie podano uzasadnienia wyboru konkretnych metod analizy danych (tj. R Pearsona i Tau B Kendalla). Należy przede wszystkim zauważyć, że część analizowanych cech ma charakter nominalny, a w takich przypadkach zasadne byłoby rozważenie użycia współczynników nieparametrycznych, np. testu chi-kwadrat lub V Craméra, które są lepiej dostosowane do natury wybranych zmiennych. Na tej podstawie proszę, aby odpowiedział Pan na dwa pytania: 1) jakie były powody wyboru tych metod analizy danych oraz 2) co to jest zmienna ilościowa i jakie wartości przyjmuje?
3. W analizie ryzyka wskazał Pan czynnik ludzki jako jedno z głównych źródeł zagrożeń, jednak nie rozwinięto w pełni zagadnienia edukacji użytkowników i kształtowania kultury bezpieczeństwa. W związku z tym nasuwa się pytanie, jak widzi Pan rolę edukacji i kompetencji cyfrowych w ograniczaniu ryzyka ludzkiego w systemach bezpieczeństwa informacji?
4. Autor słusznie zauważa rosnącą rolę sztucznej inteligencji w procesach bezpieczeństwa, jednak temat ten mógłby być pogłębiony o kwestie etyczne

i odpowiedzialności algorytmów. To z kolei prowadzi do pytania. jak postrzega Pan wyzwania etyczne związane z automatyzacją bezpieczeństwa informacji i wykorzystaniem sztucznej inteligencji?

5. W kontekście sztucznej inteligencji, zastanawia również, jakie widzi Pan kierunki dalszych badań nad integracją AI i cyberbezpieczeństwa w kontekście edukacji wyższej – zwłaszcza w świetle wchodzącego w życie AI Act i rozwoju technologii kwantowych?
6. W pracy trafnie wskazano problemy wynikające z opóźnień legislacyjnych (np. implementacji NIS2). Warto byłoby jednak doprecyzować, jak te zmiany wpływają na praktyczne funkcjonowanie uczelni. Innymi słowy, jakie rozwiązania prawne uważa Pan za najbardziej istotne dla poprawy bezpieczeństwa informacji w sektorze akademickim?
7. W swoich rekomendacjach dla skutecznego wdrożenia nowelizacji KSC (s. 142) postuluje Pan edukację i szkolenia dla sektora publicznego. Jakie formy lub metody kształcenia uznaje Pan za najbardziej efektywne w podnoszeniu świadomości cyberbezpieczeństwa w administracji i na uczelniach?

W podsumowaniu należy stwierdzić, że rozprawa jest napisana poprawnym i precyzyjnym językiem. Mimo, iż w pracy występują błędy edycyjne (niejednolitość w kontekście czcionki, akapitów, wypunktowań a także potknięcia interpunkcyjne i tak zwane literówki), to nie obniżają one wartości merytorycznej pracy. Argumentacja tez oraz przedstawione propozycje nie wzbudzają większych wątpliwości. Dążenie do poprawności analiz podnoszą w moim przekonaniu wartość dysertacji, podobnie jak styl opisu naukowego.

4. Wniosek końcowy

Rozprawa doktorska pod tytułem *System bezpieczeństwa informacji w instytucji publicznej na przykładzie centrum technologii bezpieczeństwa*, *napisana* przez magistra Jacka CZECHA, pod kierunkiem naukowym profesora doktora habilitowanego inżyniera doktora honoris causa Jarosława WOŁEJSZO oraz promotora pomocniczego doktora inżyniera Łukasza FABER, zasługuje na ogólną ocenę pozytywną. Logiczna i spójna całość rozważań pozwalają stwierdzić, że rozprawa spełnia warunki i wymagania niezbędne do nadania stopnia doktora w dziedzinie nauk społecznych. Dysertacja stanowi oryginalne rozwiązanie problemu

naukowego i wskazuje autorskie rozwiązania w zakresie zastosowania wyników własnych badań naukowych w sferze społecznej.

Biorąc pod uwagę metodologiczny i merytoryczny poziom przedstawiony w rozprawie rozwiązań a także ich oryginalność i użyteczność stwierdzam, że recenzowana rozprawa doktorska spełnia wymagania określone w artykule 187 Ustawy z dnia 20 lipca 2018 roku - Prawo o szkolnictwie wyższym i nauce (Dz.U. 2024 poz. 1571). Tym samym rekomenduję jej przyjęcie do dalszego postępowania kwalifikacyjnego i wnoszę o dopuszczenie magistra Jacka CZECHA do publicznej obrony rozprawy doktorskiej.