prof. dr hab. Andrzej MAKOWSKI
Akademia Marynarki Wojennej
Wydział Dowodzenia i Operacji Morskich

Gdynia, 11.03.2026 r.

RECENZJA

rozprawy doktorskiej mgr. inż. Michała BARCZAKA
Model zarządzania cyberzagrożeniami w aspekcie bezpieczeństwa w organizacjach
napisanej pod kierunkiem dr. hab. Włodzimierza MISZALSKIEGO, prof. WAT

1. Podstawa formalna opracowania recenzji

W ramach realizacji uchwały Rady Dyscypliny Naukowej „Nauki o Bezpieczeństwie" Wojskowej Akademii Technicznej (uchwała nr 2/RDN NoB/2026 z dnia 28 stycznia 2026 r.) zostałem wyznaczony na recenzenta w postępowaniu doktorskim mgr. inż. Michała BARCZAKA, który przedłożył dysertację nt. „Model systemu zarządzania cyberzagrożeniami w aspekcie bezpieczeństwa w organizacjach". Recenzja rozprawy została wykonana zgodnie z wymaganiami § 6 ust. 4 *„Sposobu postępowania w sprawie nadania stopnia naukowego w Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego* (załącznik do uchwały Senatu WAT nr 36/WAT/2025 z dnia 29 maja 2025 r.

2. Ocena struktury i formy rozprawy

Recenzowana rozprawa liczy 668 stron i składa się ze wstępu, siedmiu rozdziałów, zakończenia, bibliografii, jedenastu załączników, spisów: rysunków, tabel i wzorów oraz streszczeń w języku polskim i angielskim. Jej część merytoryczna została przedstawiona na 478 stronach. Strukturę pracy oceniam jako przemyślaną, logiczną i ściśle zintegrowaną z procesem badawczym realizowanym przez Kandydata. Odzwierciedla ona w pełni zagadnienia zdefiniowane w postaci szczegółowych problemów badawczych.

Wybór tematu rozprawy został szczegółowo uzasadniony we wstępie (s. 11-16), a jego treść potwierdza fakt, że Kandydat jest dobrze przygotowany do realizacji podjętego tematu. Wstęp

zawiera również definicje terminów użytych w pracy (tabela 1, s. 17-19), co stanowi wartość dodaną dla poprawnej percepcji treści zawartych w rozprawie.

Założenia badawczo-metodologiczne zostały przedstawione w rozdziale pierwszym i biorąc pod uwagę interdyscyplinarny charakter rozprawy zostały one właściwie dobrane. W sposób poprawny ustalono obszar badań, , cel ogólny i cele szczegółowe, główny i szczegółowe problemy badawcze, hipotezę główną i hipotezy szczegółowe, strukturę procesu badawczego oraz oczekiwane rezultaty badań. Metody, techniki i narzędzia badawcze zostały przedstawione w syntetyczny sposób w tabeli 1.1 (s. 31) i należy je uznać za dobrane właściwie do tematu rozprawy. Na wyróżnienie zasługuje zastosowanie metody ankietowej i eksperckiej przy ocenie opracowanego przez Kandydata modelu zarządzania cyberzagrozeniami. Również podział organizacji badań na trzy etapy, jak również ustalenie zmiennych zależnych i niezależnych w procesie badawczym pozwoliły na utrzymanie właściwej „dyscypliny" samego procesu badawczego, co znajduje swoje odzwierciedlenie w części merytorycznej rozprawy.

Treści kolejnych trzech rozdziałów (od 2 do 4) przedstawiają rozwiązania szczegółowych problemów badawczych i kolejno dotyczą: analizy i oceny norm, standardów i aktów prawnych w zakresie cyberbezpieczeństwa wraz z propozycjami zmian oraz dodatkowych regulacji; identyfikację, charakterystykę oraz kryteria cyberzagrożeń w organizacjach; ocenę podatności i zarządzanie ryzykiem w organizacji. Jakkolwiek są one różne pod względem prezentowanych treści, to pod względem merytorycznym tworzą spójną całość, która stanowi podstawę do realizacji celu ogólnego rozprawy.

Rozdział piąty, który zawiera opis opracowanego przez Kandydata modelu systemu zarządzania cyberzagrożeniami w aspekcie bezpieczeństwa w organizacjach, należy uznać za najbardziej istotny dla recenzowanej rozprawy. Jest zasadniczą i kluczową częścią dysertacji. Przedstawiony przez Autora model jest zgodny z przedmiotem badań, celem ogólnym dysertacji, realizuje jej cele szczegółowe - zarówno poznawcze, jak i praktyczne, a także potwierdza przyjętą hipotezę główną. Odpowiada on wymogom efektywnego zarządzania cyberzagrożeniami i jest na tyle uniwersalny, że może zostać wdrożony zarówno w korporacjach (krajowych i międzynarodowych), jak i średnich i małych organizacjach. Opracowany model ma równocześnie dwa zastosowania, spełnia rolę narzędzia zarzadzania cyberzagrożeniami w aspekcie bezpieczeństwa danej organizacji, ale jest również narzędziem wspomagającym projektowanie tego typu systemów dla różnych organizacji.

W kolejnych rozdziałach (6 i 7) Autor przedstawia przykładowy projekt i implementację zintegrowanego systemu informatycznego, który wspomaga zarządzanie cyberzagrożeniami w aspekcie bezpieczeństwa w organizacjach, a następnie studium przypadku, które zawiera opis procesu wdrażania i oceny efektywności opracowanego przez niego systemu zarządzania cyberzagrożeniami. W tym miejscu warto podkreślić, że jakkolwiek głównym celem rozprawy było opracowanie modelu systemu zarządzania cyberzagrożeniami, to w omawianych rozdziałach Kandydat poddaje przykładowy model (rozdział 6) weryfikacji, poszukując odpowiedzi na pytanie, jakie systemy teleinformatyczne mogą wspomagać efektywnie proces zarzadzania cyberzagrożeniami oraz w kolejnym, wykorzystując opinie ekspertów, realizuje praktyczny, szczegółowy cel badawczy rozprawy, w którym określa jakie wymagania i ograniczenia muszą być spełnione bądź uwzględnione by efektywnie i skutecznie można było wdrożyć opracowany model.

W zakończeniu Autor podsumowuje przeprowadzony proces badawczy wskazując osiągnięcie celu głównego rozprawy, osiągnięte cele poznawcze oraz praktyczne, pozytywną weryfikację hipotezy głównej oraz hipotez szczegółowych, przedstawia w formie syntetycznej wnioski oraz uzasadnia konieczność podjęcia dalszych prac badawczych, projektowych i legislacyjnych w obszarze zarządzania cyberzagrożeniami w aspekcie bezpieczeństwa w organizacjach.

Załączona do rozprawy bibliografia zawiera 769 pozycji, na które składają się: normy, standardy i akty prawne (64); pozycje zwarte (86); artykuły (161) i źródła internetowe (458). Biorąc pod uwagę temat rozprawy, została ona dobrana właściwie pod kątem merytorycznym i ilościowym by zabezpieczyć poszczególne etapy procesu badawczego.

Struktura recenzowanej rozprawy wskazuje, że ma ona formę problemową, zaś treści poszczególnych rozdziałów mają charakter teoretyczno-utylitarny. Kandydat szczegółowo analizuje poszczególne problemy badawcze, by w oparciu o uzyskane wyniki badań opracować model systemu zarządzania cyberzagrożeniami w aspekcie bezpieczeństwa w organizacjach, a następnie poddać go weryfikacji. Podkreślić należy, że każdy z rozdziałów dysertacji zawiera obszerne podsumowanie, natomiast treści rozdziałów merytorycznych łączą się wzajemnie, tworząc logiczną całość narracyjną. Warto również wyróżnić załączniki (w liczbie 11), które stanowią integralną część pracy. Zostały one starannie opracowane pod względem merytorycznym oraz metodologicznym (szczególnie ankiety) oraz są wielokrotnie przywoływane w treści poszczególnych rozdziałów.

Materiał ikonograficzny zamieszczony w rozprawie (w znakomitej większości autorstwa Kandydata) stanowi bardzo dobre uzupełnienie jej treści, jest czytelny i powiązany z omawianymi zagadnieniami, co znakomicie ułatwia ich percepcję.

Pod względem struktury i formy przedłożoną do recenzji rozprawę oceniam pozytywnie. Spełnia ona przyjęte wymagania odnoszące się do rozpraw doktorskich. Warto podkreślić bardzo dobrą redakcję rozprawy, komunikatywność i przejrzystość zawartych w niej treści oraz wniosków, co wskazuje na doskonałą znajomość badanego przez Kandydata problemu zarówno w aspekcie teoretycznym, jak i praktycznym.

3. Ocena wartości naukowej pracy

Należy podkreślić, że w literaturze odnoszącej się do przedmiotu badań recenzowanej dysertacji, brak jest opracowań, które by traktowały problemy zarządzania cyberzagrożeniami w organizacjach w kategoriach systemowych. Tę, jak można sądzić, istotną lukę, wypełnił Autor dysertacji opracowując poprawny merytorycznie i efektywny użytkowo model zarządzania cyberzagrożeniami. Zaproponowany przez Kandydata model spełnia przy tym dwie funkcje: ma zapewnić bezpieczeństwo przed cyberzagrożeniami w różnych organizacjach oraz być narzędziem wspomagającym projektowanie takich systemów, co świadczy o uniwersalności, a także praktycznym wymiarze opracowanego modelu.

Oceniając wartość naukową rozprawy można wskazać następujące dokonania na poszczególnych etapach badań: identyfikację i krytyczną analizę aktualnego stanu wiedzy w obszarze zarządzania cyberbezpieczeństwem w organizacjach, opracowanie nowej charakterystyki, kryteriów klasyfikacji oraz identyfikacji cyberzagrożeń oraz analizę i ocenę podatności i zarządzanie ryzykiem ich wystąpienia. Zaproponowane rozwiązania mają nowatorski i oryginalny charakter. Na uwagę zasługują także, szczegółowa analiza i ocena efektywności stosowanych obecnie modeli, procedur, metod i narzędzi zarządzania cyberzagrożeniami oraz ocena funkcjonalności i użyteczności wykorzystywanych współcześnie systemów teleinformatycznych wspomagających proces zarządzania cyberzagrożeniami.

Główną wartością naukową rozprawy, wkładem Kandydata w rozwój nauk o bezpieczeństwie, jest model systemu zarządzania cyberzagrożeniami, którego zastosowanie ma zapewnić bezpieczeństwo w organizacjach. Pozwala on na efektywne pozyskiwanie, wykorzystywanie i aktualizowanie wiedzy o cyberzagrożeniach, wykrywanie podatności zasobów teleinformatycznych organizacji oraz zarządzanie ryzykiem wystąpienia cyberzagrożeń, a także umożliwia ich wykrywanie oraz reagowanie na nie i co ważne, odtwarzanie funkcjonalności zasobów teleinformatycznych po zaistnieniu cyberzagrożenia oraz utrzymanie ciągłości działania organizacji. Co istotne, ocena efektywność opracowanego modelu została potwierdzona w rozdziale siódmym rozprawy. Autor wskazał również usytuowanie opracowanego systemu w strukturze organizacji (rysunek 5.6). Równolegle model znajduje zastosowanie jako narzędzie wspomagania projektowania takich systemów dla organizacji zróżnicowanych pod względem wielkości (rozdział 6).

Warto również zaznaczyć, że kandydat w oparciu o rezultaty swoich dociekań naukowych, wskazuje na konieczność podjęcia dalszych prac badawczych, projektowych i legislacyjnych, wymieniając proponowane zagadnienia enumeratywnie w zakończeniu rozprawy.

Podsumowując, wartość naukową recenzowanej rozprawy oceniam jednoznacznie pozytywnie. Z uwagi na znaczenie oraz aktualność rozwiązanego w rozprawie problemu naukowego, chciałbym zasugerować wydanie rozprawy w formie monografii, oczywiście po niezbędnych pracach redakcyjnych.

4. Zastrzeżenia i uwagi krytyczne

Nie wnoszę zastrzeżeń do recenzowanej pracy w odniesieniu do jej struktury i formy oraz wartości naukowej. Uwagi krytyczne dotyczą jedynie kwestii redakcyjnych, takich jak sporadycznie występujące „literówki", niezbyt czytelne rysunki: 3.1. i w załączniku nr 5 (rysunki od Z7 do Z14). Także warto by było zamieścić w treści rozdziału trzeciego lub w załączniku z nim związanym, dane statystyczne odnoszące się do poszczególnych kategorii cyberzagrożeń analizowanych w rozprawie w odniesieniu choćby do Polski lub Unii Europejskiej. Również objętość rozprawy – 668 stron może sugerować, że „wygodniej" można by ją przedstawić w dwóch tomach – część merytoryczna i załączniki (oczywiście w wersji rozszerzonej). Wymienione uwagi nie wpływają na ogólną ocenę recenzowanej rozprawy.

5. Podsumowanie

Stwierdzam, że recenzowana rozprawa doktorska „Model systemu zarządzania cyberzagrożeniami w aspekcie bezpieczeństwa w organizacjach" Pana mgr. inż. Michała BARCZAKA stanowi indywidualny i oryginalny dorobek naukowo-badawczy Doktoranta. Kandydat zaprezentował w niej niezbędną i na wysokim poziomie wiedzę teoretyczną z zakresu dyscypliny naukowej bezpieczeństwo. Z kolei osiągnięte w procesie badawczym wyniki świadczą o jego dużych umiejętnościach samodzielnego rozwiązywania problemów naukowych. Autor rozprawy wykazał się głęboką wiedzą w obszarze prowadzonych badań i umiejętnością posługiwania się właściwymi dla rozwiązania problemu metodami badawczymi. Problem naukowy określony w rozprawie został dobrze zidentyfikowany i w oryginalny sposób rozwiązany zarówno w aspekcie teoretycznym, jak i utylitarnym. Recenzent chciałby również zwrócić uwagę, na aktualność tematu rozprawy i duże zapotrzebowanie różnych organizacji na implementowanie wyników badań z obszaru cyberbezpieczeństwa, szczególnie gdy zagrożenie cyberatakami możemy dzisiaj uznać za powszechne.

Recenzowana monografia mgr. inż. Michała BARCZAKA, tak pod kątem swojej struktury i formy, jak i wartości naukowej zasługuje na pozytywną ocenę, w pełni spełnia również wymagania określone w artykule 187 Ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz.U. 2018 poz. 1668), a także „zwyczajowe" wymagania stawiane rozprawom doktorskim z dziedziny nauk społecznych, w dyscyplinie nauki o bezpieczeństwie

Mając powyższe na uwadze, wnoszę o dopuszczenie Pana mgr. inż. Michała BARCZAKA do publicznej obrony recenzowanej rozprawy doktorskiej.

6. Wniosek o wyróżnienie rozprawy

Wnoszę o wyróżnienie recenzowanej rozprawy doktorskiej mgr. inż. Michała Barczaka „Model systemu zarządzania cyberzagrożeniami w aspekcie bezpieczeństwa w organizacjach", co uzasadniam następująco:

- opracowaniem oryginalnego modelu systemu zarządzania cyberzagrożeniami w aspekcie bezpieczeństwa w organizacjach, jego uniwersalność i użyteczność, a przede wszystkim,

wypełnieniem istniejącej teoretycznej luki dotyczącej zarządzania cyberzagrożeniami w organizacjach w kategoriach systemowych;

- zaprojektowaniem przykładowego zintegrowanego systemu informatycznego;
- wdrożeniem opracowanego modelu w dużej międzynarodowej korporacji;
- autorską propozycją struktury i treści procesu zarządzania ryzykiem wystąpienia cyberzagrożeń;
- autorską propozycją nowego podejścia do charakterystyki, klasyfikacji i identyfikacji cyberzagrożeń;
- unikatowym charakterem przygotowanych przez Kandydata badań ankietowych.