Warszawa dn. 26.03.2026 r.

Dr hab. inż. Józef Buczyński

Profesor Wyższej Szkoły Bezpieczeństwa

Poznań

RECENZJA

rozprawy doktorskiej mgr inż. Michała Barczaka

„ MODEL SYSTEMU ZARZĄDZANIA CYBERZAGROŻENIAMI W ASPEKCIE BEZPIECZEŃSTWA W ORGANIZACJACH ”

1. PODSTAWA FORMALNA OPRACOWANIA RECENZJI.

Recenzję przygotowano na podstawie uchwały nr 2 Rady Dyscypliny Naukowej „ Nauki o Bezpieczeństwie Wojskowej Akademii Technicznej ” z dnia 28 stycznia 2026 r. oraz zgodnie z ustawą z dnia 20 lipca 2018 r „ Prawo o szkolnictwie wyższym i nauce ” i rozporządzeniem Ministra Nauki i Szkolnictwa Wyższego z 28 września 2018 r. w sprawie stopni naukowych oraz właściwymi regulacjami postępowań obowiązującymi w uczelni.

2. OCENA STRUKTURY I FORMY ROZPRAWY

Rozprawa ma formę monografii naukowej w której w sposób oryginalny i twórczy eksponuje się komponent projektowy którym jest model systemu zarządzania cyberzagrożeniami w aspekcie bezpieczeństwa w organizacjach Monografia ogółem liczy 668 stron i jest podzielona na 7 rozdziałów poprzedzonych wstępem i zakończonych obszerną, dobrze dobraną do tematu pracy bibliografią która łącznie liczy 769 pozycji, w tym 64 pozycji to normy, standardy i akty prawne, 86 to pozycje zwarte, 161 to artykuły i 458 pozycji to źródła internetowe. Postępowanie badawcze autora zyskało bardzo dobrą oprawę edycyjną w postaci załączników (11), spisu rysunków, tabel i

wzorów które stanowią tak jak i jej streszczenie oraz abstrakt integralną część rozprawy.

Teść pracy zgodna jest z jej tytułem, a treści poszczególnych rozdziałów z ich tytułami. Nagłówki rozdziałów dają syntetyczny pogląd na omawiane w nich treści. Każdy rozdział kończy się syntetycznym podsumowaniem – wnioskami, a zakończenie rozprawy ogólną ich syntezą, która zawiera także szerokie omówienie celów poznawczych i praktycznych które zostały postawione w rozdziale metodologiczny i osiągnięte w przeprowadzonym w pracy procesie badawczym co świadczy o pragmatyźmie naukowym autora.

Praca napisana jest zwięzłym, komunikatywnym, poprawnym i logicznie spójnym językiem, w dużym stopniu opartym na właściwej dla prezentowanej dziedziny specjalistycznej terminologii. Na podkreślenie zasługuje to iż w pracy dominuje wiele odwołań do źródeł (bibliografia, normy, cytaty). Wszystko to sprawia, że strona metodyczna pracy jest poprawna, jej struktura jest logiczna i przejrzysta, zasługuje na uznanie i tym samym spełnia wszystkie kryteria rozprawy naukowej.

3. OCENA MERYTORYCZNA I METODOLOGICZNA ROZPRAWY

Rozprawa doktorska przygotowana przez Pana mgr. Michała BARCZAKA zarówno pod względem merytorycznym jak i metodologicznym ze wszech miar zasługuje na uznanie. Doktorant we wstępie do pracy w sposób w pełni przekonywujący odniósł się do konieczności podjęcia badań nad systemem zarządzania cyberzagrożeniami i tym samym problematyką bezpieczeństwa w cyberprzestrzeni w czasie dynamicznie rozwijającej się rewolucji informacyjnej. Jasno też wskazał i dobrze uzasadnił podjęty w pracy problem badawczy którego finalnym efektem jest opracowanie i prezentacja modelu systemu zarządzania cyberzagrożeniami w aspekcie bezpieczeństwa w organizacjach.

Wyjściowa teza rozprawy, że w aktualnej sytuacji rewolucji informacyjnej istnieje potrzeba opracowania systemu zarządzania cyberzagrożeniami w aspekcie bezpieczeństwa w organizacjach znalazła swoje pełne odzwierciedlenie w sformułowanych w pracy celach, zarówno ogólnych jak i szczegółowych, problemach badawczych oraz głównej i szczegółowej hipotezie roboczej. Na podkreślenie zasługuje również to, że w rozdziale metodologicznym autor zaprezentował także logicznie spójną i przejrzystą strukturę procesu badawczego którego konsekwentna realizacja pozwoliła autorowi na osiągnięcie zamierzonego celu którym było zaprezentowanie modelu systemu zarządzania cyberzagrożeniami w aspekcie bezpieczeństwa w organizacjach.

Metodologiczną spójność tej części pracy dopełniają w pełni adekwatne do postawionych przez autora celów, problemów i hipotez metody i

techniki badawcze których komplementarna implementacja, wspierana przez zaprezentowaną organizację badań była gwarantem końcowego sukcesu procesu badawczego

Rozdział 2 pracy prezentuje podstawę formalno – prawną platformę prowadzonych badań w sferze zarządzania cyberbezpieczeństwem. Wykazano, że aktualne unormowania normatywne i standaryzacyjne w tej dziedzinie nie uwzględniają wszystkich aspektów tej problematyki zwłaszcza procesu pozyskiwania, wykorzystywania i aktualizacji wiedzy o cyberzagrożeniach, wykrywania i zarządzania ryzykiem czy procesu wykrywania, reagowania na cyberzagrożenia. W tych dokumentach autor dostrzega również brak precyzyjnych definicji metod i procedur wspomagających poszczególne fazy procesu zarządzania cyberzagrożeniami. Konkluzją przeprowadzonych analiz jest wskazana przez doktoranta pilna potrzeba wypełnienia swoistej luki poznawczej i normatywnej w tym obszarze i konieczność podjęcia prac legislacyjnych w celu normatywnego uregulowania, w ujęciu systemowym, całokształtu problematyki zarządzania cyberzagrożeniami. Szkoda jednak że pomimo tych wskazań w finale pracy i wnioskach końcowych nie zawarto żadnych istotnych rekomendacji w tej dziedzinie.

Rozdział 3 dysertacji dotyczy bardzo istotnych zagadnień bowiem charakteryzuje zarówno kryteria klasyfikacji jak i identyfikacji cyberzagrożeń oraz ich wpływu na bezpieczeństwo funkcjonalne organizacji. Przedstawione w tym rozdziale kompleksowe i logicznie spójne podejście do definiowania oraz identyfikacji zagrożeń stanowi swoiste sedno prowadzonego procesu badawczego którego finalnym produktem jest zaprezentowana propozycja modelu zarządzania cyberzagrożeniami w aspekcie bezpieczeństwa w organizacjach.

Wskazano, na podstawie analizy literatury przedmiotu badań, oraz licznych źródeł internetowych i raportów różnych organizacji, na najbardziej podatne obszary występowania zagrożeń którymi najczęściej są złośliwe w tym i szpiegowskie oprogramowanie generujące całe spektrum wirusów. W pracy dokonano ich kwalifikacji i szeroko omówiono ich wpływ na zagrożenia dla bezpieczeństwa. Poddano również krytycznej analizie ataki techniczne na systemy i sieci oraz wykazano jak istotnym zagrożeniem dla bezpieczeństwa jest aktywność człowieka w cyberprzestrzeni, w tym między innymi korzystanie ze sztucznej inteligencji, ryzyka zawiązane z chmurą obliczeniową, coraz powszechniej stosowana praca zdalna czy aktywność w mediach społecznościowych, szeroko rozumiana jako inżynieria społeczna.

Na podkreślenie zasługuje to, że w wyniku przeprowadzenia analitycznego procesy badawczego, autor w pracy zaprezentował swój, autorski, katalog zagrożeń które są największymi wyzwaniami dla bezpieczeństwa w cyberprzestrzeni. Katalog który wpisuje się w treść raportu opublikowanego w

2024 r. przez Agencję Unii Europejskiej do spraw Cyberbezpieczeństwa. Istotnym walorem pracy jest nie tylko opracowanie i przedstawienie tego katalogu ale również to, że autor w wyniku pogłębionej analizy zaproponował metody identyfikacji poszczególnych zagrożeń oraz zaproponował procedury ich zwalczania co może stanowić swoisty suplement do w/w Raportu. W pracy wskazano, że w dobie dynamicznego rozwoju społeczeństwa informacyjnego który to proces dotyka nie tylko indywidulnie poszczególnych osób ale również każdej organizacji której aktywność przenosi się do sieci generując tym samy cale spektrum wyzwań i zagrożeń pilną potrzebą staje się budowa efektywnych metod i modeli zarządzania cyberzagrożeniami i tym samym zapewnienie bezpieczeństwem funkcjonowania organizacji.

Zaprezentowane w tym rozdziale wnioski z przeprowadzonych analiz i badań są zakończeniem pierwszego i dużej cześć drugiego przedstawionego w pracy przez autora etapu organizacji badań. Stanowią też bardzo ważną platformę informacyjną do kontynuowania procesu badawczego nad budową modelu systemu zarządzania przed cyberzagrożeniami w aspekcie bezpieczeństwa w organizacjach.

Kolejny rozdział pracy koncentruje się na ocenie podatności systemów informatycznych na zagrożenie oraz procedurach zarzadzania ryzkiem przed cyberzagrożeniami w organizacjach.

Podatność organizacji na cyberzagrożenia to problem bardzo ważny dla sprawnego funkcjonowania każdej organizacji aktywnej w cyberprzestrzeni. Niestety, zbyt często, dopóki nie wydarzy się incydent z naruszeniem bezpieczeństwa systemu informatycznego danej organizacji, jest on marginalizowany i niedoceniany. Dopiero wtedy okazuje się, że słabości – luki i podatność na zagrożenia była widoczna od dawna – tylko nikt jej nie traktował priorytetowo, nie przeprowadzono audytu podatności i nie wprowadzono adekwatnych do jego wyników procedur i polityk zarządzania bezpieczeństwem.

Autor, przez pryzmat wniosków płynących z raportów wielu organizacji międzynarodowych i wyników badań własnych, szeroko omawia znaczenie i rangę problemu badania i oceny podatności i zarządzania ryzykiem przed cyberzagrożeniami w organizacjach wykorzystujących zasoby informatyczne. Wskazuje na konieczność włożenia dużego wysiłku i zwrócenia szczególnej uwagi przede wszystkim na to co chronimy czyli na identyfikację zasobów, analizę zagrożeń, identyfikacji podatności tych zasobów na zagrożenia, ocenę ryzyka dla każdej podatności i wypracowanie procedur zarządzania tym ryzykiem.

Kanwą prowadzonych rozważań i analiz jest zdefiniowany w poprzednim rozdziale katalog cyberzagrożeń dla organizacji, a wynikiem przeprowadzonych badań własnych w tym badań ankietowych jest opracowany i przedstawiona na stronach dysertacji (230-231) autorska klasyfikacja podatności

zasobów informatycznych organizacji na cyberzagrożenia uwzględniająca zarówno aspekty techniczne jak i aktywność czynnika ludzkiego (np. hakerzy) w cyberprzestrzeni.

Autor również wskazuje, że z uwagi na dynamicznie zmieniające się środowisko teleinformatyczne istnieje konieczność systematycznego prowadzenia audytu cyberzagrożeń i oceny podatności organizacji na te zagrożenia, a wnioski z tych analiz powinny być platformą wyjściową do różnych metod i form oceny ryzyka i aktualizacji systemu zarządzania ryzykiem w aspekcie bezpieczeństwa w organizacji.

Synergia wyników dotychczas prowadzonego procesu badawczego były dla Autora swoistą wyjściową platformą informacyjną przystąpienia do zaprezentowania najważniejszej części dysertacji jakim są modele systemu zarządzania cyberzagrożeniami w aspekcie bezpieczeństwa organizacji oraz opracowania przykładowego projektu takiego modelu oraz procedury jego implementacji.

System zarządzania cyberzagrożeniami to sposób organizowania działań, narzędzi i procesów które pozwalają wykrywać - identyfikować, analizować, ograniczać i zapobiegać pojawiającym się zagrożeniom. W praktyce to połączenie technologii, procedur i ludzi którzy wspólnie odpowiadają za bezpieczeństwo informacyjne organizacji. W aktualnie dostępnych i analizowanych przez Autora normach, standardach i aktach prawnych, jak wskazuje doktorant, jest potrzeba konsolidacji i aktualizacji wymogów dotyczących cyberbezpieczeństwa oraz opracowania i posiadania przez organizację spójnego systemu zarządzania ryzykiem oraz wykrywania i reagowania na cyberzagrożenia. Skłoniło to Autora do opracowania i zaprezentowania modułowej, wielowarstwowej, szczegółowej, struktury - modelu systemu zarządzania cyberzagrożenimi którego kompozycja została szeroko omówiona w pracy. Wyraźnie widać, że ważnym walorem takiego podejścia prezentującego model jako spójna całość oraz poszczególnych jego modułów była ich komplementarność i kompetencyjna konwergencja pozwalająca na łatwą jego implementację. Budowa prezentowanego modelu rozpoczyna się od szerokiego omówienia znaczenia problemów zarzadzania cyberbezpieczeństwem i prowadzi do omówienia poszczególnych warstw - modułów - modelu w których możemy wyróżnić takie elemnty jak : pozyskiwanie , wykorzystywanie i aktualizacja wiedzy o cyberzagrożeniach, ocena podatności i zarządzania ryzykiem cyberzagrożeń, wykrywania (identyfikacja), reagowanie na cyberzagrożenia oraz odtwarzanie systemów informatycznych po awarii i tym samy zapewnienie ciągłości funkcjonowania organizacji.

Ważnymi komponentami tak zdefiniowanego systemu jest także cała warstwa technologiczna – zestaw narzędzi wspierających procesy zarządzania systemem bezpieczeństwa oraz procedury ciągłego jego doskonalenia (audyty,

testy, aktualizacja procedur). Istotny wpływ na tak zdefiniowany i przedstawiony w pracy model systemu zarządzania cyberzagrożeniami w aspekcie bezpieczeństwa organizacji ma także środowisko cyberprzestrzeni funkcjonowania organizacji. Można je określić mianem kultury bezpieczeństwa organizacji na którą składają się takie czynniki jak świadomość i odpowiedzialność personelu organizacji, współpraca oraz jasne zasady odpowiedzialności za zgłaszanie incydentów – zagrożeń dla cyberzpieczeństwa organizacji.

Konkluzją wszystkich przeprowadzonych w rozdziale piątym pracy badań i analiz jest zaprezentowany na str. 431 dysertacji autorski, graficzny model usytuowania systemu zarządzania cyberzagrożeniami i zespołu cyberbezpieczeństwa w strukturze organizacji. Prezentuje on w bardzo przejrzystej formie wszystkie omówione moduły systemu zarządzania cyberzagrożeniami z wyeksponowaniem bardzo ważnej roli zespołu cyberbezpieczeństwa w organizacji który w wymiarze personalnym odpowiada za szeroko rozumianą kulturę jej bezpieczeństwa.

Wychodząc z analizy już istniejących rozwiązań i aplikacji systemów Informatycznych wspomagających procesy zarzadzania cyberbezpieczeństwem w aspekcie bezpieczeństwa organizacji Autor wskazuje na wady i ograniczenia tych rozwiązań i wskazuje na wymagania jakie taki system powinien spełniać. Proponuje również własne, wspomagające wszystkie procesy realizowane w poszczególnych opisanych w pracy modułach, procedury zwiększające bezpieczeństwo organizacji przed cyberzagrożeniami

W pracy sformułowano funkcjonalne i niefunkcjonalne wymogi tak zdefiniowanego systemu oraz zaprezentowano, w ujęciu modułowym, jego strukturę organizacyjno – funkcjonalną która ma ułatwić jego implementację w rzeczywistej organizacji. Modelując strukturę systemu Autor posłużył się notacją UML (Unified Modeling Language) – standardowym językiem graficznym - i całą gamą oferowanych przez tą notację diagramów strukturalnych i behawioralnych – umożliwiających w ujęciu dynamicznym ocenę działania systemu - które szeroko i wnikliwie zostały omówione w pracy. Ponadto Autor wskazuje na istotne walory opracowanego przez niego projektu systemu informatycznego zarządzania cyberzagrożeniami który nie jest rozwiązaniem zamkniętym lecz ma on walory systemu otwartego na inne podejścia projektowe, głównie w obszarze jego implementacji w organizacjach aktywnie działających w cyberprzestrzeni.

Kierując się zdefiniowanymi w rozwiązaniu modelowym systemu kryteriami funkcjonalności Autor dokonał pogłębionej analizy organizacji funkcjonujących w cyberprzestrzeni w których jego rozwiązanie mogłoby być wdrożone. Wybór padł na globalną, światową, korporację z branży medyczno – farmaceutycznej. Organizację o rozbudowanej strukturze orgazniacyjno – funkcjonalnej o bardzo szerokiej gamie procesów i procedur infromacyjno –

decyzyjnych realizowanych w środowisku cyberprzestrzeni i tym samym bardzo podatnej na płynące z tego środowiska cyberzagrożenia.

Autor osobiście, z pełnym zaangażowaniem, włączył się w proces wdrażania zaprojektowanego systemu. Jego dyskusje , konsultacje i telekonferencje z kierownictwem tej organizacji oraz szefami zespołów odpowiedzianych za jej cyberbezpieczeństwo, a także wyniki przeprowadzonych badań ankietowych w pełni potwierdziły użyteczność opracowanego systemu. Pozwoliły one zarówno na uwypuklenie całego pakietu mocnych stron, walorów użyteczności systemu, które uwidoczniły się w trakcie jego eksploatacji. Pozwoliły też na wskazanie na jego słabszych stron mając ujemny wpływ na ocenę jego funkcjonalności. Wszystkie wyniki tych badań zostały zaprezentowane i szczegółowo omówione w załącznikach do dysertacji.

Na pokreślenie zasługuje to, że wszyscy uczestnicy procesu analityczno – badawczego zgodnie stwierdzili, że opracowany przez Autora model systemu zarządzania cyberzagrożeniemi w aspekcie bezpieczeństwa w organizacjach który został zaproponowany im do implementacji jest, w porównaniu do innych aplikacji, rozwiązaniem nowatorskim, w wielu aspektach ze wszech miar użytecznym który spełnia uwagi wymogi i walory rozwiązania systemowego.

4. OCENA WARTOŚCI NAUKOWEJ PRACY

Przedłożona do recenzji rozprawa doktorska od wstępu, poprzez rozdział metodologiczny oraz siedem rozdziałów merytorycznych, aż po zakończenie, stanowi logicznie ułożoną, zamkniętą merytorycznie i spójną metodologicznie całość. Autor podjął temat niezwykle aktualny, o dużym, nie tylko naukowym ale i praktycznym znaczeniu. Temat pracy i zaprezentowane problemy badawcze wpisują się w główny nurt dyskusji analizującej globalne trendy zawiązane z rosnącą liczbą zagrożeń i różnego rodzaju incydentów w cyberprzestrzeni, złożonością środowiska IT oraz koniecznością budowania systemowych rozwiązań - modeli - zwiększających bezpieczeństwo organizacji funkcjonujących w cyberprzestrzeni.

Prezentowana praca doktorska jest opracowaniem wartościowym, bogatym w treści analityczne i empiryczne. Opracowaniem w którym autor wykazał się szeroką, interdyscyplinarną wiedzą z zakresu informatyki, cyberbezpieczeństwa, zarządzania ryzykiem, narodowych i międzynarodowych norm, aktów prawnych i standardów w zarządzaniu cyberbezpieczeństwem oraz modelowaniu procesów zarządzania cyberbezpieczeństwem w nowoczesnych organizacjach.

Doktorant w pracy zaprezentował kilka własnych intersujących rozwiązań do których min. można zaliczyć autorski katalog cyberzagrożeń czy klasyfikację podatności zasobów informatycznych organizacji na cyberzagrożenia. Najważniejszym osiągnięciem Autora jest opracowanie i aplikacyjne wdrożenie modelu systemu zarządzania cyberzagrożeniami w aspekcie bezpieczeństwa w organizacjach. Modelu którego struktura poprzez podejście procesowe integruje w sobie : audyt ceberzagrożeń, zarządzanie ryzykiem, wykrywanie podatności organizacji na zagrożenia, reagowanie na cyberzagrożenia oraz w procesie dynamicznym odtwarzanie utraconych po awarii zasobów tak aby była zapewniona ciągłość funkcjonowania organizacji. Zaprezentowany model wyróżnia się kompleksowością oraz możliwością jego adaptacji do różnych typów organizacji – zarówno dużych podmiotów korporacyjnych jak i mniejszych jednostek np. administracji publicznej co stanowi istotny wkład w rozwój badań nad cyberzagrożeniami i cyberbezpieczeństwem organizacyjnym.

Zastosowana metodologia jest adekwatna do postawionych przez Autora celów rozprawy, a proces badawczy został przeprowadzony z dużą starannością. Zdefiniowany przedmiot badań i problemy badawcze oraz cele i hipotezy – główna i szczegółowa dobrze wpisują się w temat dysertacji co czyni rozprawę metodologicznie spójną. Przedstawione w poszczególnych rozdziałach dysertacji wyniki badań oraz, sformułowane po zakończeniu procesu wdrażania modelu systemu, oceny ekspertów, wskazują na walory użytkowe opracowanych zaprezentowanych w pracy rozwiązań. Wskazują także na konieczność dalszych prac badawczych i projektowych w tej dziedzinie co powinno być swoistym wyzwaniem dla Autora do ich kontynuacji w dalszych pracach badawczych.

Jak już wspomniałem, doktorant przy opracowaniu dysertacji korzystał z bardzo bogatej literatury – normy, standardy, akty prawne czy źródła internetowe, można wręcz odnieś wrażenie pewnego nadmiaru tych pozycji. Szkoda jednak, że w zaprezentowanym katalogu bibliografii znalazły się tylko dwie i to jako współautor pozycje doktoranta.

Reasumując, stronę merytoryczną i metodologiczną pracy, należy wskazać na oryginalność tematu pracy, na jasność i zasadność postawionych problemów badawczych oraz walory praktyczne proponowanych rozwiązań systemowych. Zaprezentowane w pracy analizy i wnioski są przekonywujące, rzetelne, logiczne, merytorycznie słuszne, właściwie osadzone w kontekście teoretycznym oraz dobrze udokumentowane Przegląd literatury wskazuje na adekwatność i aktualność źródeł oraz zdolność doktoranta do ich wykorzystania oraz krytycznej ich analizy i oceny. Praca cechuje się kompleksowości i praktyczną użytecznością. Obejmuje pełen cykl życia cyberzagrożeń w sieci, od ich identyfikacji i analizę, po ewolucję, ocenę podatności organizacji na zagrożenia i propozycję skutecznych metod zarządzania i przeciwdziałania tym zagrożeniom co zostało zaprezentowane w pracy jako model systemu zarządzania cyberzagrożeniami w aspekcie bezpieczeństwa w organizacjach.

5. WNIOSEK KOŃCOWY

Stwierdzam że rozprawa doktorska Pan mgr. inż. Michała Barczaka prezentuje wysoki poziom merytoryczny, oryginalność oraz dużą wartość naukową i praktyczną którą wnosi do tak ważnej problematyki jaką obecnie jest cyberbezpieczestwo. Opracowany model systemu zarządzania cyberzagrożeniami w aspekcie bezpieczeństwa w organizacjach stanowi istotny wkład w rozwój badań nad tak aktualnym zagadnieniem jak cyberzagrożenia i tym samym bezpieczeństwo funkcjonowania organizacji aktywnych w cyberprzestrzeni. Praca spełnia kryteria i wymagania określone w ustawie z dnia 20 lipca 2018 r. Prawo o Szkolnictwie Wyższym i Nauce - art. 187 Ustawy, zatem wnoszę o przyjęcie rozprawy i dopuszczenie jej do publicznej obrony.

.....