dr hab. inż. Zbigniew Ciekanowski
Menedżerska Akademia Nauk Stosowanych
w Warszawie

Warszawa dn. 17.07.2023 r.

RECENZJA
ROZPRAWY DOKTORSKIEJ

mgr. Grzegorza MĄKOSĘ

opracowanej pod tytułem

KONCEPCJA DOSKONALENIA ORGANIZACJI SYSTEMU CYBERBEZPIECZEŃSTWA RZECZYPOSPOLITEJ POLSKIEJ

1. Ocena ogólna

Rozprawa doktorska pod tytułem *Koncepcja doskonalenia organizacji systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej*, napisana przez magistra Grzegorza MĄKOSĘ pod kierunkiem naukowym profesora doktora habilitowanego Bogusława JAGUSIAKA, jest niewątpliwie interesująca z naukowego punktu widzenia. Tematyka pracy odnosi się do problematyki cyberbezpieczeństwa jako procesu zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego struktur, osób fizycznych, prawnych i nieposiadających osobowości prawnej, a także zasobów informacyjnych i systemów teleinformatycznych cyberprzestrzeni.

W pracy Doktorant skoncentrował się na organizacji systemu cyberbezpieczeństwa RP zdefiniowanego na podstawie regulacji prawnych i dokumentów strategicznych dotyczących bezpieczeństwa państwa, w zakresie: zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym, zorganizowania struktur i relacji operacyjnych zarządzania, doboru sektorów i typów podmiotów oraz wskazania norm, metodyk i standardów zarządzania bezpieczeństwem systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa.

Celem niniejszej recenzji jest ocena przedłożonej rozprawy doktorskiej pod kątem spełnienia wymagań określonych w artykule 13 ust.1 Ustawy z dnia 14 marca 2003 roku o stopniach naukowych i tytule naukowym oraz stopniach i tytule w zakresie sztuki (tj. Dz. U. 2017 r. poz. 1789) w związku z art. 187 Ustawy z dnia 20 lipca 2018 roku - Prawo o szkolnictwie wyższym i nauce (tj. Dz. U. z 2022 r. poz. 574).

Doktorant na wstępie podkreśla, że współczesne bezpieczeństwo państwa w sferze militarnej i pozamilitarnej, zewnętrznej i wewnętrznej zyskało dodatkowy wymiar, jakim, obok lądu, wody, powietrza i przestrzeni kosmicznej, jest cyberprzestrzeń oraz dodatkowy sektor bezpieczeństwa, jakim jest cyberbezpieczeństwo. Postępująca globalizacja i integracja, rozwój społeczeństwa informacyjnego i technologii teleinformatycznych zmieniły obecne środowisko bezpieczeństwa państw, w tym również Rzeczypospolitej Polskiej. Rozwój technologii teleinformatycznych korzystnie wpływa na rozwój społeczeństwa informacyjnego oraz rozwój gospodarczy. Niestety wpływa również na rozwój negatywnych zjawisk w cyberprzestrzeni, tj. cyberprzestępczości, cyberkonfliktów, cyberwalki czy walki informacyjnej. Postęp w teleinformatyce sprawił, że domena cyberprzestrzeni, nie tylko przyczynia się do rozwoju podmiotów państwowych (pozapaństwowych) czy jednostki, ale jest również źródłem poważnych zagrożeń dla ich bezpieczeństwa. Ciągły rozwój technologii sprawia, że cyberataki są coraz bardziej wysublimowane, przyjmują nowe formy i są kierowane w coraz to nowsze obszary funkcjonalne otoczenia administracyjno-społeczno-gospodarczego państwa. Warunkiem zapewniającym ciągłe utrzymywanie inicjatywy na poziomie strategicznym zarządzania bezpieczeństwem państwa jest przewaga informacyjna, która ma bezpośrednie przełożenie na koncepcje doktrynalne odnoszące się do infrastruktury cywilnej i wojskowej systemów kierowania państwem i dowodzenia siłami zbrojnymi, a także szeroko rozumianych operacji informacyjnych.

Doktorant również wskazuje, że bezpieczeństwo informacyjne bywa określane jako zakres bezpieczeństwa przyjmujący wzrost znaczenia informacji w zachowaniu stabilności współczesnych, międzynarodowych systemów ekonomicznych. Ma to odzwierciedlenie w płaszczyznach bezpieczeństwa politycznego, militarnego, ekonomicznego, społecznego, kulturowego, ekologicznego czy zdrowotnego. Bezpieczeństwo informacyjne staje się zatem gwarantem bezpieczeństwa militarnego, finansowego, gospodarczego, zarówno w skali lokalnej pojedynczego państwa, jak i na arenie międzynarodowej. Sektory te mają kluczowe znaczenie dla utrzymania krytycznej działalności społecznej i gospodarczej, realizują usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służą zapewnieniu sprawnego

funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców, są realizowane w celu ochrony interesu publicznego.

Jak Doktorant słusznie zauważa, kwestia zapewnienia bezpieczeństwa informacyjnego i cyberbezpieczeństwa jest przede wszystkim odpowiedzialnością i domeną państwa. Właściwe organy państwa opracowały i wdrożyły dokumenty poziomu strategicznego i operacyjnego właściwe dla zapewnienia cyberbezpieczeństwa państwa i tworzące jego system cyberbezpieczeństwa. Dokumenty te wyznaczają strategiczną perspektywę, punkty odniesienia i ramy cyberbezpieczeństwa, a także cele i zadania do osiągnięcia odpowiedniego jego poziomu. Kwestie cyberbezpieczeństwa, z racji swojego znaczenia dla bezpieczeństwa państwa, są przedmiotem zainteresowania i wpływu regulacji prawnych, w tym, w szczególny sposób, Ustawy o zarządzaniu kryzysowym, Ustawy o krajowym systemie cyberbezpieczeństwa i Ustawy o informatyzacji podmiotów realizujących zadania publiczne wraz z towarzyszącymi im aktami wykonawczymi i pomocniczymi. Regulacje prawne definiują zagadnienia cyberbezpieczeństwa, podmioty zaangażowane oraz ich odpowiedzialność, przedmiot zainteresowania danej regulacji oraz aspekty organizacyjne i struktury funkcjonowania systemu cyberbezpieczeństwa. Definiują również wymagania wobec podmiotów nimi objętych, dotyczące wdrożenia odpowiednich rozwiązań organizacyjnych i technicznych bezpieczeństwa oraz systemu zarządzania bezpieczeństwem systemów teleinformatycznych i informacji w celu zapewnienia właściwego poziomu ich bezpieczeństwa. Bezpieczeństwo państwa wymaga nowych rozwiązań w zakresie bezpieczeństwa, tym samym podjęcie przez Doktoranta badań w omawianym obszarze stanowi cenny wkład w potrzeby rozwoju wiedzy i wzbogacenia kompetencji oraz praktycznego zastosowania posiadanych umiejętności w obrębie rozwiązań systemowych.

W ciekawej treściowo dysertacji daje się zauważyć etapowość prowadzonej narracji i argumentacji. Całość opisu procesu badawczego jest opracowana poprawnie, co unaocznia umiejętności autorskie 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.

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, często tylko w poszukiwaniu drobnych fragmentów przekładających się logicznie na obraz realnej przedmiotowo rzeczywistości. W związku z powyższym należy stwierdzić, że analiza metodologiczna aspektów pracy doktorskiej wskazuje, iż jest ona skonstruowana poprawnie i odpowiada wymogom metodologicznym nauk społecznych.

Recenzowana praca doktorska jest to obszerne opracowanie, składające się z sześciu rozdziałów, streszczenia, wstępu, zakończenia, bibliografii oraz załączników, spisu tabel, wykresów i rysunków, zawartych na 565 stronach.

We wstępie (zawartym na stronach 7-12) Doktorant przedstawił wprowadzenie do tematyki rozprawy doktorskiej, następnie przedstawił główny cel badań oraz główną hipotezę badawczą. Autor nakreślił sytuację problemową, określając wstępnie lukę poznawczą, oraz rzetelnie opisał strukturę pracy.

W rozdziale pierwszym (strony 13-41) pod tytułem *Metodologiczne podstawy badań*, Doktorant skoncentrował się na metodologii badań, uzasadnił zasadność podjęcia badań, określił cel główny badań i cele szczegółowe, przedmiot badań, główny problem badawczy i problemy szczegółowe oraz hipotezę główną i hipotezy pomocnicze. Dość wnikliwie scharakteryzował metody, techniki i narzędzia badawcze. Przedstawił szczegóły organizacji procesu badawczego, założenia i ograniczenia badawcze, a także dokonał krytycznej analizy literatury. Za szczególnie cenne uznaję opis doboru próby badawczej i wysiłek jaki Autor włożył w pozyskanie materiału pierwotnego. Opisana procedura wskazuje na determinację i samodyscyplinę w zachowaniu rzetelności i przyjętych w nauce zasad realizacji etapu operacjonalizacji.

W rozdziale drugim (strony 42-168) pod tytułem *Cyberbezpieczeństwo w bezpieczeństwie narodowym RP,* Doktorant przeprowadził rozważania nad istotą i pojęciami bezpieczeństwa narodowego oraz współczesnym pojęciem cyberbezpieczeństwa, jego istotą i rolą, jak również poświęcił uwagę zagadnieniom teoretycznym i aktualnemu faktycznemu stanowi bezpieczeństwa polskiej cyberprzestrzeni w odniesieniu do wyzwań, zagrożeń i incydentów cyberbezpieczeństwa. Rozdział stanowi odpowiedź na postawiony problem badawczy: *Jakie są aktualne kontekst, warunki i środowisko prawne, strategiczne i normatywno-standaryzacyjne systemu cyberbezpieczeństwa RP i czy ich rozpoznanie*

stanowić będzie podstawę opracowania koncepcji doskonalenia systemu cyberbezpieczeństwa RP? Rozdział kończy się interesującymi wnioskami.

W rozdziale trzecim (strony 169-207), pod tytułem *Organizacja zarządzania cyberbezpieczeństwem na poziomie krajowym*, Doktorant dokonał próby rozstrzygnięcia problemu badawczego dotyczącego zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym - *Jaka jest aktualna organizacja zarządzania cyberbezpieczeństwem RP na poziomie krajowym i w jaki sposób zapewnić jej efektywność?* W tym celu Autor przeprowadził kompleksowy proces badawczy, w ramach którego dokonał przeglądu rozwiązań zarządzania cyberbezpieczeństwem na poziomie krajowym w systemie zarządzania kryzysowego i krajowym systemie cyberbezpieczeństwa. Przeprowadzone analizy porównawcze rozwiązań zastanych zostały skonfrontowane z wynikami przeprowadzonych badań własnych w tym zakresie, co pozwoliło na częściowe opracowanie autorskiej koncepcji zorganizowania zarządzania cyberbezpieczeństwem na poziomie krajowym. Rozdział kończy się podsumowaniem i wnioskami.

W rozdziale czwartym (strony 208-307) pod tytułem *Struktury i relacje operacyjne zarządzania w systemie cyberbezpieczeństwa,* Doktorant skupił się na próbie rozstrzygnięcia problemu badawczego dotyczącego struktur i relacji operacyjnych w systemie cyberbezpieczeństwa na poziomie krajowym - *Jakie są aktualne struktury i relacje operacyjne zarządzania cyberbezpieczeństwem RP na poziomie krajowym i w jaki sposób zapewnić ich efektywność?* Dla realizacji tego celu Autor przeprowadził proces badawczy związany z przeglądem struktur i relacji operacyjnych zarządzania cyberbezpieczeństwem na poziomie krajowym w systemie zarządzania kryzysowego i krajowym systemie cyberbezpieczeństwa oraz dokonał analizy porównawczej rozwiązań. Doktorant przedstawił wyniki przeprowadzonych badań własnych w tym zakresie, co zaowocowało kolejnym wkładem merytorycznym w element tworzonej autorskiej koncepcji usprawnień wybranego obszaru systemu cyberbezpieczeństwa RP. Rozdział kończy się podsumowaniem i wnioskami, odnoszącymi się do postawionej w pracy hipotezy głównej i hipotezy pomocniczej odpowiednio dla tego rozdziału.

W rozdziale piątym (strony 308-350) pod tytułem *Sektory i podmioty systemu cyberbezpieczeństwa RP,* Doktorant dokonał próby rozstrzygnięcia problemu badawczego dotyczącego doboru sektorów i typów podmiotów systemu cyberbezpieczeństwa - *Jakie sektory i typy podmiotów są aktualnie objęte systemem cyberbezpieczeństwa RP i jakie powinny zostać nim objęte, aby zapewnić jego efektywność i odpowiedni poziom bezpieczeństwa kraju?* Powtarzana w poprzednich rozdziałach i merytorycznie zasadna procedura postępowania

badawczego i opisu wyników badań umożliwiła potwierdzenie (częściowe) przyjętej hipotezy szczegółowej odnoszącej się do przeglądu systemów, sektorów i typów podmiotów w systemie zarządzania kryzysowego, krajowym systemie cyberbezpieczeństwa i systemie informatyzacji podmiotów publicznych. Rozdział kończy się podsumowaniem i wnioskami.

W rozdziale szóstym (strony 351-398) pod tytułem *Bezpieczeństwo systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP*, Doktorant dokonał próby rozstrzygnięcia problemu badawczego dotyczącego rozwiązań normatywnych bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa, *Jakie międzynarodowe i krajowe normy, metodyki i standardy zarządzania bezpieczeństwem systemów teleinformatycznych są aktualnie wymagane i jakie powinny zostać wskazane do stosowania, aby zapewnić odpowiedni poziom bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa RP?* Doktorant przedstawił wyniki przeprowadzonych badań własnych w tym zakresie i dokonał ich analizy jak również przedstawił opracowaną autorską koncepcję wykazu norm, metodyk i standardów bezpieczeństwa systemów teleinformatycznych podmiotów systemu cyberbezpieczeństwa. Rozdział kończy się podsumowaniem i wnioskami, odnoszącymi się do postawionej w pracy hipotezy głównej i hipotezy pomocniczej odpowiednio dla tego rozdziału.

W podsumowaniu i zakończeniu (umieszczonym na stronach od 399 do 442), Doktorant syntetyzuje uzyskane rezultaty badań z odniesieniami do rozwiązania problemów oraz hipotez badawczych, a także wykorzystania poszczególnych metod w prowadzonych rozważaniach. W zakończeniu rozprawy Doktorant nakreślił kierunki i rekomendacje do podjęcia dalszych badań.

Analizując treść problemów badawczych przedstawionych w dysertacji, należy podkreślić, że stanowią one ambitne zadanie badawcze o charakterze deskrypcyjnym, eksplanacyjnym, diagnostycznym i w jakimś stopniu również predyktywnym. Wygenerowane problemy szczegółowe wyznaczyły drogę postępowania badawczego, którego cechami są zwięzłość, etapowość, konsekwencja i rzeczowość.

Hipotezy robocze, przyjęte przez Doktoranta na potrzeby badań, są ściśle powiązane zarówno z wyznaczonymi celami badań, jak i z problemami badawczymi. Do rozwiązywania problemów zastosowano podejście z wykorzystaniem teoretycznych i empirycznych metod badawczych. Doktorant wskazuje jednocześnie na jakościowy wymiar zastosowanych metod (choć należy wskazać, że w pracy znajdują się również minimalne odniesienia do analiz ilościowych).

Analizując układ dysertacji z punktu widzenia proporcji między wielkością (obszernością) poszczególnych rozdziałów, należy go uznać za poprawny. Kolejność poszczególnych rozdziałów wynika logicznie z toku prowadzonego procesu poznawczego. Poprawna jest również struktura poszczególnych rozdziałów. Wyraźnie jest w nich dostrzegalna etapowość prowadzonego poznania, jak również logika prezentacji osiągniętych efektów badań.

Literatura przedmiotu (288 pozycji) dotycząca rozmaitych aspektów rozpatrywanej problematyki została dobrana i wykorzystana poprawnie. W całościowym ujęciu 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 grafik, tabel i wykresów, pozwalających zarówno na pełniejszy opis podejmowanych kwestii, jak i na zrozumienie analizowanego problemu. W ostatniej części dysertacji Doktorant zamieścił bardzo interesujące odpowiedzi ekspertów, co czyni proces poznawczy przejrzystym oraz umożliwia jego potencjalne udoskonalenie w przypadku chęci przeprowadzenia ponownego badania np. w formie badań panelowych, co dopiero pomogłoby uzyskać informację na temat efektywności potencjalnie wprowadzonych rozwiązań, stanowiących zasadniczy koncept dysertacji.

Rekapitulując należy stwierdzić, że Doktorant jest przygotowany do samodzielnego prowadzenia badań.

3. Ocena merytoryczna

Recenzowana rozprawa doktorska stanowi zwarte opracowanie naukowe liczące 460 stron, bibliografię oraz załączniki (razem 565 stron).

Pod względem merytorycznym dysertacja wnosi nowe wartości poznawcze. Opracowana przez Doktoranta koncepcja wykazu sektorów i typów podmiotów systemu cyberbezpieczeństwa RP stanowi nowe ujęcie problemu, wypełnia zdiagnozowaną lukę, brak i dysfunkcyjność krajowego systemu cyberbezpieczeństwa poprzez zdefiniowanie konieczności ustanowienia właściwego (rozszerzonego) wykazu sektorów i typów podmiotów. Według koncepcji system cyberbezpieczeństwa RP powinien obejmować wszystkie sektory, systemy i typy podmiotów systemu zarządzania kryzysowego, krajowego systemu cyberbezpieczeństwa i systemu informatyzacji podmiotów realizujące zadania publiczne oraz najszerszy możliwy katalog wszystkich innych typów podmiotów mających odpowiednio duży wpływ na kształtowanie bezpieczeństwa publicznego. Implementacja tak sformułowanego

postulatu objęłaby systemem cyberbezpieczeństwa wielokrotnie więcej podmiotów, a przez to (zdaniem Autora) przyczyniłaby się do zwiększenia poziomu cyberbezpieczeństwa i bezpieczeństwa państwa.

W zakończeniu dysertacji Doktorant podsumowuje przeprowadzone badania, umieszczając swoje spostrzeżenia z przeprowadzonego procesu poznawczego. Wyniki analizy badań wykazują, że cel badań jaki został założony — osiągnięto.

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

1. Na podstawie dokonanej analizy krytycznej literatury przedmiotu i własnych refleksji, doświadczenia i wiedzy **jak zdefiniowałby Doktorant granice polskiej cyberprzestrzeni?**
2. Proszę o wyjaśnienie **jak stosował Pan obserwację jako technikę a jak jako metodę naukową?**
3. Setki razy w tekście pracy Doktorant użył nazwy „respondenci". Zastanawia mnie czy był to zabieg celowy i **czy za zasadne uznaje Doktorant rozróżnienie pojęć „respondent" i „badany" — omawiając technikę wywiadu eksperckiego?**
4. W czterech z pięciu hipotez szczegółowych Doktorant wskazuje, że dane operacje, działania „(...) zapewnią efektywność systemu cyberbezpieczeństwa RP i odpowiedni poziom bezpieczeństwa państwa" (s. 20 i 21). Interesujące jest **jak Doktorant rozumie skuteczność i efektywność oraz czy jest w stanie zmierzyć tę ostatnią biorąc pod uwagę przedmiot badań?**
5. Weryfikacja (niezależnie czy pozytywna czy negatywna) wymaga z reguły logicznego lub statystycznego sprawdzenia, przy wykorzystaniu zdań inferencyjnych lub zmiennych i wskaźników poddanych operacjom statystycznym (testy istotności, korelacje, siły związku itp.). **W jaki sposób Doktorant weryfikował hipotezy?**
6. Dbając o trafność badawczą, tworząc narzędzie badawcze postuluje się konstrukcję pytań zachowując rozdzielność badanych kategorii w jednym pytaniu. **Czy znana jest Doktorantowi ta zasada oraz czy stosował ją w realizowanym badaniu?**

W podsumowaniu należy stwierdzić, że rozprawa jest napisana poprawnym i precyzyjnym językiem. Choć czasami występują w niej błędy edycyjne (interpunkcyjne i tak zwane literówki), trzeba zaznaczyć, że nie obniżają one wartości pracy. Argumentacja tez oraz przedstawione propozycje nie wzbudzają większych wątpliwości.

4. Wniosek końcowy

Rozprawa doktorska pod tytułem *Koncepcja doskonalenia organizacji systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej*, napisana przez magistra Grzegorza MĄKOSĘ pod kierunkiem naukowym profesora doktora habilitowanego Bogusława JAGUSIAKA, zasługuje na ogólną ocenę pozytywną. Logiczna i spójna całość rozważań pozwalają stwierdzić, że rozprawa spełnia warunki i wymagania niezbędne do nadania stopnia doktora dziedzinie nauk społecznych. Dysertacja stanowi oryginalne rozwiązanie problemu naukowego, w zakresie zastosowania wyników własnych badań w sferze społecznej. Dotyczy to głównie sformułowanej koncepcji zorganizowania struktur i relacji operacyjnych systemu cyberbezpieczeństwa RP przy porównaniu z obecnymi strukturami systemu zarządzania kryzysowego i krajowego systemu cyberbezpieczeństwa.

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 13 ust.1 Ustawy z dnia 14 marca 2003 roku o stopniach naukowych i tytule naukowym oraz stopniach i tytule w zakresie sztuki (tj. Dz. U. 2017 r. poz. 1789) w związku z art. 187 Ustawy z dnia 20 lipca 2018 roku - Prawo o szkolnictwie wyższym i nauce (tj. Dz. U. z 2022 r. poz. 574).

Tym samym rekomenduję przyjęcie dysertacji do dalszego postępowania kwalifikacyjnego i wnoszę o dopuszczenie magistra Grzegorza MĄKOSĘ do publicznej obrony rozprawy doktorskiej.