dr hab. Jacek NOWAK
Lotnicza Akademia Wojskowa

Dęblin, 30. 10. 2025 r.

RECENZJA
rozprawy doktorskiej
pt. **„System bezpieczeństwa informacji w instytucji publicznej na przykładzie centrum technologii bezpieczeństwa"**

opracowanej przez Pana mgr. Jacka Czecha
pod kierunkiem naukowym
Pana prof. dr. hab. inż. dr. h.c. Jarosława Wołejszy
oraz promotora pomocniczego Pana dr. inż. Łukasza Fabera

Ogólna charakterystyka rozprawy

Współczesne środowisko bezpieczeństwa charakteryzuje się dużą dynamiką. Na tą dynamikę wpływa ilość informacji, które są przetwarzane przez różne instytucje. Można powiedzieć, iż obecnie w społeczeństwie, które ma szybki i powszechny dostęp do informacji, stabilność jego rozwoju zależy w dużym stopniu od bezpieczeństwa przetwarzanej informacji.

Wiarygodna, sprawdzona informacja, przekazywana w czasie zbliżonym do rzeczywistego jest nie mniej ważnym orężem w zdobywaniu przewagi, co tradycyjne środki walki. Ma to szczególne znaczenie w turbulentnym obecnie środowisku geopolityki. Informacja może być również wykorzystywana jako narzędzie dla osiągania celów, przez wrogo nastawione do naszego społeczeństwa podmioty o charakterze państwowym i niepaństwowym.

Szczególnie ważne, w obecnej sytuacji geopolitycznej, jest zachowanie zaufania do instytucji publicznych, które dysponują rozległą informacją o społeczeństwie. Przetwarzają one ogromne ilości danych wrażliwych, obejmujących m.in. dane

wrażliwe obywateli, administracyjne, oraz szczególnie ważne, te o charakterze państwowym.

Pomimo tego, że informacja jest zasobem niematerialnym, posiada często siłę, która wpływa na ekonomię, konflikty a nawet umożliwia „sterowanie" całymi społecznościami.

Recenzowana dysertacja odnosi się do systemu bezpieczeństwa informacji w instytucji publicznej. Od czasu do czasu środki masowego przekazu informują o bardzo niebezpiecznych zdarzeniach związanych z „wyciekiem" informacji właśnie z instytucji publicznych. Są to informacje niezwykle istotne, często wręcz o charakterze strategicznym. Nie muszę tu przytaczać przykładów, ponieważ problem jest powszechnie znany i na całe szczęście dostrzegany przez organy władzy. Autor opracowania wskazuje, że *bezpieczeństwo informacji w instytucjach publicznych jest zagadnieniem interdyscyplinarnym, obejmującym zarówno aspekty techniczne, organizacyjne i prawne* (s. 12). Jest to stwierdzenie wskazujące, że Autor opracowania dostrzega w tym obszarze elementy systemowe. W opinii Recenzenta, podejście systemowe pozwala na dostrzeżenie całego spektrum zjawisk badanego obszaru i w tej dysertacji odzwierciedliło się to w przyjętym temacie.

Z tych powodów wybór tematu dysertacji jest jak najbardziej słuszny. Jest to specyficzny obszar, w którym na pewno można znaleźć wiele problemów, które są warte rozwiązania metodami naukowymi. Tak też uczynił Autor powyższego sprawozdania, w którym przedstawił wyniki swojej pracy. W ocenie Recenzenta rozprawa jest cennym opracowaniem (może zbyt obszernym, bowiem liczy 472 s.), który bezpośrednio odnosi się do trudnego, aczkolwiek bardzo ważnego dla społeczeństwa obszaru - systemów bezpieczeństwa informacji.

W nakreślonych uwarunkowaniach, za uzasadnione, uznać należy motywację Autora do podjęcia badań w ramach recenzowanej rozprawy doktorskiej. Temat rozprawy, jak i podjęte w niej problemy badawcze są istotne i mieszczą się w głównym nurcie ważnej i aktualnej tematyki badań nauk o bezpieczeństwie. Uważam zatem, za w pełni uzasadnione podjęcie tematu recenzowanej dysertacji, przeprowadzenie badań i ich pisarskie opracowanie w formie rozprawy doktorskiej.

Szczegółowa charakterystyka rozprawy

Rozprawa zawiera streszczenie, wstęp, cztery rozdziały, zakończenie, bibliografię, spis tabel i rysunków (102 tabele), spis rysunków (181 rysunków), załączniki (6 załączniki), łącznie 472 strony pracy. Ilość materiału badawczego jest bardzo obszerna, ale rozumiem dylematy Autora w jego objętościowym ograniczeniu. Bardzo trudno jest wskazać w niniejszej dysertacji mniej ważne lub zbędne fragmenty. W ocenie Recenzenta opracowanie ma klasyczny, logiczny układ i wynika z przyjętych założeń.

We wstępie Autor wprowadza w tematykę rozprawy oraz zapoznaje z przyjętym układem pisarskiego opracowania wyników badań.

Rozdział pierwszy dotyczy aspektów metodologicznych przeprowadzonych badań. W rozdziale tym, po właściwym scharakteryzowaniu sytuacji problemowej na kolejnych stronach został wskazany przedmiot, cel badań (poznawczy i pragmatyczny), problem główny i problemy szczegółowe, hipotezy robocze (główna i szczegółowe) oraz zastosowane metody, narzędzia i procedury badawcze.

Autor rozprawy w niniejszym rozdziale odnosi się również do procesu badawczego, w tym etapów badań (faz?), przyjętych ograniczeń oraz doboru i charakterystyki próby badawczej.

Pierwsza część założeń badawczych poświęcona jest sytuacji problemowej i uzasadnieniu celowości podjęcia tematu, który został sformułowany, jako *„System bezpieczeństwa informacji w instytucji publicznej na przykładzie centrum technologii bezpieczeństwa”.*

Autor dysertacji wskazując, że instytucje publiczne przetwarzają ogromne ilości danych wrażliwych, swój wywód skupia na powodach, dlaczego należy im zapewnić bezpieczeństwo. Są to: ochrona prywatności obywateli, bezpieczeństwo narodowe, stabilność funkcjonowania administracji oraz zgodność z regulacjami międzynarodowymi (s. 13).

Powody te są skorelowane z zagrożeniami dla bezpieczeństwa informacji do których Autor opracowania zaliczył: różnego typu ataki cybernetyczne, luki

w zabezpieczeniach systemów IT, brak świadomości użytkowników, dezinformacja i manipulacja danymi (s. 13).

W tym obszarze Autor sprawozdania dostrzegł lukę badawczą i na s. 14 wskazuje, że *choć temat bezpieczeństwa informacji jest szeroko omawiany, wiele obszarów związanych z jego implementacją w sektorze publicznym pozostaje niewystarczająco zbadanych, w tym analiza skuteczności polityk bezpieczeństwa oraz rola czynnika ludzkiego w cyberbezpieczeństwie instytucji publicznych.* W opinii Recenzenta jest to na pewno obszar, który warto zbadać metodami naukowymi.

Autor dysertacji za **przedmiot badań** przyjął *system bezpieczeństwa informacji w instytucji publicznej na przykładzie Centrum Technologii Bezpieczeństwa Akademii Górniczo-Hutnicze* (s. 14). Z pracy wynika, iż Doktorant podczas opracowania jej treści konsekwentnie kierował się przyjętym przedmiotem badań.

Doktorant określił w sprawozdaniu dwa **cele badań** (s. 17): poznawczy i utylitarny (pragmatyczny). Za **cel poznawczy** przyjął *zidentyfikowanie i analiza zagrożeń dla bezpieczeństwa informacji w instytucji publicznej oraz ocena istniejących metod zabezpieczeń, w celu opracowania skuteczniejszych usprawnień ochrony informacji szczególnie w środowisku akademickim* (s. 15). Cele poznawcze, z reguły związane są z opisami i wyjaśnieniami zjawisk oraz procesów zachodzących w badanej rzeczywistości społecznej. W opinii Recenzenta przyjęty w dysertacji cel poznawczy koreluje z powyższą regułą.

Za **cel utylitarny** w recenzowanej dysertacji przyjęto *opracowanie usprawnień skutecznych mechanizmów ochrony informacji z uwzględnieniem aspektów organizacyjnych, technicznych i prawnych oraz doskonalenie systemu zarządzania bezpieczeństwem informacji w instytucjach publicznych, w celu minimalizacji ryzyka utraty, modyfikacji lub nieautoryzowanego dostępu do danych*

Wg dr. hab. A. Czupryńskiego[1] cel utylitarny to rezultat, do którego zmierza postępowanie badawcze i jego efektem jest między innymi naprawa rzeczywistości.

---

[1] A. Czupryński, *Cel poznaczy i utylitarny w naukach o bezpieczeństwie*, w red. nauk. A Czupryński, B. Wiśniewski, J. Zboina, *Nauki o bezpieczeństwie. Wybrane problemy badań*, s. 39, wyd. CNBOP-PIB, Józefów 2017.

W świetle tego zapisu proszę Doktoranta o ocenę możliwości rzeczywistego wykorzystania osiągniętych wyników przeprowadzonych przez niego badań.

Realizacja wskazanych celów (cel poznaczy i praktyczny) kierunkowała proces badawczy co potwierdzą prezentowane w recenzowanym opracowaniu wyniki badań.

Główny problem badawczy, Autor rozprawy sformułował pytaniem (s. 15): *jakie zmiany należy wprowadzić do systemu bezpieczeństwa informacji instytucji publicznej, aby poprawić skuteczność jej funkcjonowania?*

Odpowiednio do przyjętego głównego problemu badawczego, starano się sprecyzować **właściwą hipotezę badawczą**. W tym miejscu mam pewne wątpliwości, bo w zasadzie w dysertacji nie ma wskazania, co jest tą hipotezą. Oczywiście czytając pracę można się domyśleć, jaki zapis tworzy tą hipotezą. W ocenie Recenzenta jest on zbyt mało precyzyjny i zbyt długi (s. 15 i 16). **Dlatego też proszę Doktoranta o wyjaśnienie głównej hipotezy badawczej.**

Problem główny podzielony został na trzy problemy szczegółowe (s. 16), a układ, treść oraz wzajemne relacje między celem, problemem ogólnym a problemami szczegółowymi w zasadzie określają kierunek badań podjętych przez Autora rozprawy.

Przyjęte **hipotezy szczegółowe** (s. 16 do 18) wykazują związek ze szczegółowymi problemami badawczymi, jednak też z tymi wskazanymi przez Doktoranta będę polemizował. W metodologii badań naukowych przyjęło się, że hipotezę badawczą można scharakteryzować jako przypuszczenie, prawdopodobieństwo wystąpienia lub wyeliminowania określonego zjawiska, wydarzenia, procesu w konkretnym czasie i miejscu. Hipoteza badawcza, po przeprowadzeniu badania, może zostać potwierdzona bądź obalona. Autor Dysertacji te wskazania respektuje, a jednocześnie „wzbogaca" przyjęte hipotezy szczegółowe stwierdzeniami w formie pytań a nie przypuszczeń (s. 16 – 18). **Proszę Doktoranta o komentarz do tego fragmentu pracy.**

Pomimo uwag, przyjęty przedmiot badań, cele, problemy i hipotezy oceniam pozytywnie, a tą ocenę wzmacnia opis zastosowanych metod, narzędzi i technik

badawczych. Autor dysertacji zastosował teoretyczne i empiryczne metody badań. Fakt przeprowadzenia badań empirycznych jest potwierdzony umieszczeniem w dysertacji właściwych wykresów, rysunków i załączników. Jest to bardzo obszerny materiał badawczy.

Od s. 27 do s. 30 Doktorant przedstawił przebieg procesu badawczego, w ujęciu „klasycznym", dzieląc ten proces na trzy fazy. Czynności jakie były realizowane w poszczególnych fazach zawiera tabela 1.2. (s. 28). W tym miejscu dostrzegamy brak konsekwencji Autora opracowania, bowiem na s. 27 pisze ... *Proces badawczy dla niniejszej pracy został zrealizowany w trzech fazach:*

- *Faza I - przygotowanie badań,*
- *Faza II - prowadzenie badań,*
- *Faza III - opracowanie badań,*

a tytuł tabeli 1.2. jest następujący – Etapy przeprowadzonego procesu badawczego (s. 28).

W opinii Recenzenta przyjęte przez Autora dysertacji ograniczenia były uzasadnione chociaż zostały wymieszane ze wskazaniem), tego co w tej pracy zrobiono (s. 29 - 30).

Metodologiczną część rozprawy oceniam pozytywnie, a zawarte w recenzji uwagi nie rzutują na ogólną wartość przyjętych założeń.

Drugi rozdział rozprawy zatytułowano *„Teoria i praktyka funkcjonowania systemów bezpieczeństwa informacji w organizacji publicznej"*. Autor opracowania dążył w nim do weryfikacji przyjętej pierwszej hipotezy szczegółowej, co potwierdza zapis ze s. 31.

Składa się on z dziewięciu podrozdziałów merytorycznych oraz jednego zawierającego wnioski. Jest to rozdział o charterze teoretycznym i empirycznym o czym świadczą zastosowane do jego opracowania metody badawcze (s. 31 - 32). Rozdział ten przedstawia istotę roli, miejsca i wartości informacji wraz z potrzebą zachowania jej bezpieczeństwa. Autor dysertacji wyeksponował w nim czynniki prawne, środowiskowe, techniczne, rolę człowieka w systemach bezpieczeństwa

informacji. Treści niniejszego rozdziału kierunkował pierwszy szczegółowy problem badawczy wyrażony pytaniem: *w jaki sposób w teorii i praktyce funkcjonuje system bezpieczeństwa informacji w organizacji publicznej?* To kierunkowanie jest widoczne w treściach rozdziału, ale można odnieść wrażenie, że Autor dysertacji jakby „zapomniał" o pierwszej szczegółowej hipotezie badawczej, ponieważ nie wskazuje, czy zweryfikował ją pozytywnie, czy też negatywnie (Podrozdział 2.10. Wnioski, s. 231). **Dlatego też podczas obrony proszę Doktoranta o wyjaśnienie tej kwestii.**

Rozdział drugi można potraktować jako wprowadzenie do całej pracy. Zawiera on teorie dotyczącą przedmiotu badań, ale też wyniki badań empirycznych, z komentarzem Autora opracowania. Jest to bardzo bogaty materiał zawierający dużą ilość rysunków i wykresów. W mojej ocenie jest to tekst wymagający od odbiorcy dobrego przygotowania teoretycznego, szczególnie w części powstałej w oparciu o badania empiryczne.

Rozdział drugi dysertacji kończą wnioski (podrozdział 2.10., s 321). W tym miejscu można poczuć pewien niedosyt. Rozdział ten zaczyna się na s. 31 a kończy się na 232. Zawiera zatem pond 200 stron tekstu, który jest wynikiem badań empirycznych i teoretycznych. Natomiast wnioski, które są zawarte w podrozdziale 2.10 liczą dwa, krótkie akapity i jeden mały rysunek. **Proszę Doktoranta o wyjaśnienie tej sytuacji podczas obrony. Czy wyniki badań zawarte na około 200 stronach tekstu nie pozwoliły na wyciągnięcie bardziej dogłębnych wniosków w aspekcie przyjętego pierwszego szczegółowego problemu badawczego i przyjętej do niego hipotezy szczegółowej?**

Drugi rozdział rozprawy oceniam pozytywnie. Doktorant opracowując jego treści wykonał określone badania, które korzystnie wpłynęły na całą dysertację. Stanowi on dobry materiał zarówno naukowy, jak też dydaktyczny. Jego zawartość świadczy o bardzo dobrym teoretycznym przygotowaniu Autora dysertacji.

Trzeci rozdział pracy zatytułowano *„System bezpieczeństwa informacji w instytucji publicznej na przykładzie centrum technologii bezpieczeństwa AGH".* Rozdział ten składa się z pięciu podrozdziałów merytorycznych i jednego podrozdziału, gdzie zawarto uogólnienia i wnioski. Autor rozprawy przy

opracowaniu jego treści kierował się drugim szczegółowym problem badawczym, który został sformułowany w postaci pytania (s. 233): *w jaki sposób funkcjonuje system bezpieczeństwa informacji w Centrum Technologii Bezpieczeństwa AGH?* Starano się w nim zweryfikować drugą hipotezę szczegółową, co potwierdza zapis ze s. 233. Rozdział został opracowany z wykorzystaniem teoretycznych i empirycznych metod badawczych (s. 233- 234).

Podrozdział 3.1 zawiera treści odnoszące się do uczelni akademickiej, jako instytucji publicznej w kontekście zagrożeń bezpieczeństwa informacji. Autor przytacza w nim informacje amerykańskiego instytutu StealthLABS odnośnie zagrożeń bezpieczeństwa informacji szkół i uniwersytetów w USA (s. 238). Wg autorów przytoczonych badań *pogorszenie sytuacji to brak wiedzy informatycznej, zdecentralizowanej polityki bezpieczeństwa i ograniczeń budżetowych. W tym kontekście pozycja instytucji akademickich i badawczych jest bardziej zagrożona. Istotą jest, aby instytucje te uznały cyberbezpieczeństwo za poważne, wręcz kluczowe ryzyko* (s. 239). Uważam, iż warto w tym obszarze przenalizować sytuację polskich uczelni, jeśli nie wszystkich to wybranych.

W podrozdziale 3.2. Autor opracowania skupił się na zagrożeniach bezpieczeństwa informacji w środowisku akademickim, a tych nie brakuje. Interesującym fragmentem tego podrozdziału jest przedstawienie przez Autora opracowania kwestii aktywności służb specjalnych, w szczególności wywiadu nad dostępem do informacji akademickiej. Doktorant zwraca również uwagę na bezpieczeństwo informacji podczas, tzw. kształcenia zdalnego (s. 269).

W kolejnym podrozdziale 3.3. nakreślono ogólny system organizacji bezpieczeństwa informacji na uczelni. Są w nim wskazane między innymi różne wymiary ochrony informacji w instytucji akademickiej (s. 274, rys. 3.21).

W podrozdziale 3.4., w zwięzły sposób Doktorant odnosi się się do bezpieczeństwo informacji w Centrum Technologii Bezpieczeństwa. Początkowo tekst dotyczy AGH, jako uczelni. Jest to fragment wprowadzający do roli i zadań Centrum Technologii Bezpieczeństwa, które zostało powołane zarządzeniem nr 21 Rektora Akademii Górniczo-Hutniczej z dnia 19 kwietnia 2021 r. Zarządzenie weszło w życie z dniem

podpisania z mocą obowiązującą od dnia 1 marca 2021 r. (s. 295). W niniejszym podrozdziale Autor dysertacji zwięźle przedstawia główne założenia polityki bezpieczeństwa informacji obowiązującej w AGH. Jest to ciekawy tekst, który powinien zainteresować każdego pracownika uczelni wyższej.

Podrozdział 3.5. jest rezultatem badania stanu bezpieczeństwa informacji w instytucji publicznej na przykładzie uczelni publicznej. Na s. 305 Autor pracy pisze *...W kontekście przedstawionego przedmiotu badań celem pracy jest próba zrozumienia, oceny oraz propozycji optymalizacji sposobu, w jaki organizacja publiczna zarządza bezpieczeństwem informacji i tworzy jej obieg* ... **Jak ten zapis, w porównaniu z przyjętymi w rozdziale metodologicznym celami należy rozumieć? Proszę o komentarz.**

Podrozdział 3.5. opracowano na postawie badań empirycznych – ankiety i wywiadu eksperckiego, który w mojej ocenie przypomina bardziej ankietę. Do wyników tych badań zastrzeżeń nie wnoszę, ale przyjętą formą wywiadu można polemizować.

Wnioski dotyczące całego rozdziału trzeciego zawarto w podrozdziale 3.6. (s. 375 - 378). Wnioski można uznać za zasadne.

Treść rozdziału trzeciego jest wynikiem analizy literatury przedmiotu i dokumentów normatywnych oraz badań empirycznych. W ocenie Recenzenta, prowadzony wywód jest dość czytelny, a uwagi Recenzenta mają raczej charakter polemiczny. Umieszczone w nim rysunki ułatwiają jego zrozumienie. Całość rozdziału oceniam pozytywnie.

Czwarty rozdział pracy pt. *„Usprawnienia systemu bezpieczeństwa informacji w organizacji publicznej"* w ocenie Recenzenta można uznać za tzw. rozdział wynikowy. Wyznacznikiem jego treści był trzeci szczegółowy problem badawczy wyrażony pytaniem: *jakie usprawnienia poprawią skuteczność bezpieczeństwa informacji w organizacji publicznej?* Do tego pytania została dobrana hipoteza szczegółowa, która w toku badań była weryfikowana przez Autora dysertacji (s. 380).

Rozdział ten składa się z czterech podrozdziałów merytorycznych i jednego podrozdziału w którym są zawarte wnioski.

Podrozdział 4.1. zatytułowano *„Świadomość nowych zagrożeń”* (s. 381). Uważam, iż z treścią tego rozdziału można polemizować. W opinii Recenzenta nie wyczerpuje on tego obszaru (tylko jedna strona tekstu), a poza tym obszar zagrożeń był już wcześniej poruszany przez Autora opracowania (pododdział 3.2., s. 259).

W kolejnym podrozdziale 4.2. (s. 382 – 391) wskazano, jak można przeciwdziałać zagrożeniom oraz co jest konieczne do ich likwidacji i skutków.

Podrozdział 4.3. dotyczy inwestycji w nowe technologie, które mają zapewnić bezpieczeństwo informacji. Między innymi wskazano w nim, iż *inwestycja w Security Operations Center (SOC) z perspektywy technicznej stanowi strategiczny krok w kierunku zapewnienia kompleksowego bezpieczeństwa infrastruktury teleinformatycznej instytucji publicznej* (s. 391).

W podrozdziale 4.4. Autor opracowania odnosi się do procesów w otoczeniu sztucznej inteligencji (s. 396 – 407). W jego opinii ... *zastosowanie sztucznej inteligencji w przeciwdziałaniu dezinformacji w kontekście bezpieczeństwa informacji instytucji publicznych staje się kluczowym narzędziem umożliwiającym skuteczne przeciwdziałanie manipulacjom informacyjnym. AI może pełnić zarówno funkcję prewencyjną, jak i operacyjną...* (s. 397). Uwag do tego podrozdziału nie wnoszę.

Wnioski z całości rozdziału zawarto w podrozdziale 4.5. Uważam, że są zasadne i wynikają z przeprowadzonych badań. Więcej uwag do tego fragmentu pracy nie wnoszę, a cały rozdział czwarty oceniam pozytywnie.

Mocną stroną opracowania jest bibliografia, która świadczy o dobrym przygotowaniu merytorycznym Autora sprawozdania.

Na s. 471 dysertacji jej Autor zamieścił Załącznik nr 6. Arkusz obserwacji. Na wskazanym arkuszu są między innymi następujące zapisy:

- CEL BADAŃ: Opracowanie usprawnień dotyczących systemowego podejścia do bezpieczeństwa informacji w instytucjach publicznych i akademickich.
- CZAS BADAŃ: ponad 35 lat pracy zawodowej oraz obserwacje z ostatnich trzech lat ze szczególnym uwzględnieniem środowiska akademickiego.

Rozdział czwarty opracowania dotyczy usprawnień, a nie ma w nim żadnego przypisu świadczącego o wykorzystaniu tej metody. Uważam też, że nie powinno się podawać czasu pracy, jako czasu badań. **Proszę o skomentowanie tej sytuacji podczas obrony.**

Podsumowanie

Rozprawę opracowano na dobrym poziomie metodycznym i redakcyjnym. Zrozumienie treści pracy ułatwia bogaty materiał graficzny. Wskazane błędy nie wpływają na pozytywną ocenę pracy. W pracy **można dostrzec logiczną spójność między założeniami badawczymi, zrealizowanym i udokumentowanym procesem badawczym a treścią dysertacji.** Na podkreślenie zasługuje dobór stosownych materiałów źródłowych, które dały podstawę do opracowania rozprawy, a także tych, dokumentujących prowadzone badania. Wartość twórczą tej rozprawy oceniam pozytywnie, a do najistotniejszych osiągnięć Autora w tym zakresie zaliczam:

- zebranie i uporządkowanie w jednym dziele wiedzy z zakresu systemu bezpieczeństwa informacji instytucji publicznej;
- wskazanie możliwych usprawnień dla systemu bezpieczeństwa informacji w organizacji publicznej.

W rozprawie odpowiednio do potrzeb badań właściwie dobrano i wykorzystano materiały źródłowe oraz literaturę. Uwagi wyrażone w recenzji do wybranych treści rozprawy mają charakter polemiczny.

Wniosek końcowy

Doktorant dzięki właściwie zaplanowanemu i zrealizowanemu procesowi badań osiągnął założony cel, a w recenzowanej dysertacji zawarł rozwiązanie problemu naukowego. Niniejsza rozprawa doktorska wykazuje ogólną wiedzę teoretyczną Doktoranta w naukach o bezpieczeństwie oraz umiejętność samodzielnego prowadzenia pracy naukowej.

Przedstawiona do recenzji dysertacja spełnia wymagania stawiane rozprawom doktorskim z dziedziny nauk społecznych, w dyscyplinie nauki o bezpieczeństwie,

zgodnie z art. 187 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (t.j. Dz.U. z 2024 r. poz. 1571 z późn. zm.).

W związku z powyższym wnoszę o dopuszczenie Doktoranta do publicznej obrony przedłożonej rozprawy doktorskiej.

Dr hab. J.Nowak

.....