Recenzja w postępowaniu w sprawie nadania stopnia doktora habilitowanego Pani dr Joannie Antczak

Zostałem wyznaczony do sporządzenia Recenzji przez Radę Doskonałości Naukowej[1]. Przedmiotem recenzji jest dorobek Pani dr Joanny Antczak, nazywanej w recenzji także Kandydatką. Monografię *Zarządzanie cyberbezpieczeństwem w przedsiębiorstwie - doświadczenia wybranych państw Unii Europejskiej* przedstawiono jako główne osiągnięcie naukowe.

Spełnienie warunku określonego w art. 219 ust. 1 pkt 1[2].

Warunek określony w art. 219 ust. 1 pkt 1 stanowi, że Kandydatka powinna legitymować się dyplomem uzyskania stopnia doktora. Jest to warunek konieczny do uzyskania stopnia doktora habilitowanego. Przedłożona dokumentacja zawiera odpis dyplomu doktora nauk ekonomicznych w dyscyplinie ekonomia wystawiony Pani Joannie Antczak. Stopień ten przyznała Akademia Finansów w Warszawie. Odpis, który otrzymałem, jest kopią niepotwierdzoną. Zakładam, że wiarygodność tej kopii nie podlega wątpliwości. Pozostałe dane o Kandydatce związane z § 2 pkt. 4.1[3] mogę zaczerpnąć jedynie z przesłanej dokumentacji. Nie widzę powodu do ich podważania. Podobnie nie mam żadnych przesłanek do uzupełnienia informacji związanych z § 2 pkt. 4.3[4] a przedstawionych w w przesłanej mi dokumentacji habilitacyjnej, a w tym w szczególnie autoreferatu.

Kandydatka ubiega się o uzyskanie stopnia doktora habilitowanego w dziedzinie nauk społecznych w dyscyplinie nauki o zarządzaniu i jakości. Wobec powyższego stwierdzam, że **warunek określony w artykule 219 ustęp 1 punkt 1 został przez Kandydatkę spełniony.**

Z wielkim zainteresowaniem zapoznałem się z sylwetką Kandydatki. Pani Joannie Antczak jest zastępcą dyrektora ds naukowych Instytutu Zarządzania Wojskowej Akademii Technicznej w Warszawie. Uprzednio pracowała w Akademii Sztuki Wojennej oraz Instytucie Nauk Ekonomicznych Polskiej Akademii Nauk w Warszawie, a także pięciu uczelniach prywatnych. Kandydatka ma szerokie doświadczenie w pracy poza uczelniami. Zatrudniona była w bankach, szkole ponadpodstawowej oraz biurze rachunkowym. Imponuje różnorodność zajęć zawodowych świadcząca o zdolnościach Kandydatki do dostosowywania się do zmieniających oczekiwań rynku pracy oraz rozpoznania nowych szans zawodowych. Ostatnie stanowisko pracy zastępcy dyrektora ds naukowych instytutu w elitarnej uczelni wojskowej w Kraju świadczy tym, że Kandydatka potrafi sprostać niebanalnym obowiązkom. Gratuluję!

---

[1] Pismo DRKN.Z5.400.174.2025.

[2] Prawo o szkolnictwie wyższym i nauce, Dz. U. 2018 poz. 1668 i § 2 pkt. 4.2 umowy o dzieło jaką zawarłem z Politechniką Częstochowską o przeniesieniu autorskich praw majątkowych w sprawie opracowania recenzji w postępowaniu habilitacyjnym

[3] Umowa o dzieło jaką zawarłem z Politechniką Częstochowską o przeniesieniu autorskich praw majątkowych w sprawie opracowania recenzji w postępowaniu habilitacyjnym

[4] Umowa o dzieło jaką zawarłem z Politechniką Częstochowską o przeniesieniu autorskich praw majątkowych w sprawie opracowania recenzji w postępowaniu habilitacyjnym

Prof. dr hab. Witold Abramowicz
Witold@Abramowicz.pl

Spełnienie warunku określonego w art. 219 ust. 1 pkt 2[5].

Kandydata wybrała do oceny monografię naukową wydaną przez wydawnictwo, które w roku opublikowania monografii w ostatecznej formie było ujęte w wykazie sporządzonym zgodnie z przepisami wydanymi na podstawie art. 267 ust. 2 pkt 2 lit. a. Ponieważ Wydawnictwo Difin zostało ujęte w wykazie[6], można zatem przyjąć, że **warunek formalny i konieczny określony w punkcie drugim ustawy został spełniony**.

Wobec rosnącego zagrożenia bezpieczeństwa osób, społeczności, podmiotów gospodarczych, jednostek samorządowych oraz instytucji Państwa, cyberbezpieczeństwo budzi powszechne zainteresowanie. W środowiskach akademickich jest jedną z dynamicznie rozwijających się specjalizacji. Wspomniane zagrożenia mogą mieć bardzo zróżnicowanych charakter, np. jako wyzwania techniczne, mogą być związane z naruszeniami prawa lub zasad współżycia społecznego w Internecie. Naruszenie cyberbezpieczeństwa mogą prowadzić do daleko idących konsekwencji, np. zrujnowania sieci telekomunikacyjnych, doprowadzenia do niewydolności systemu ochrony zdrowia, destabilizacji relacji społecznych. Kandydatka skupiła swoje zainteresowanie na zagadnieniach związanym z zapewnieniem cyberbezpieczeństwa przedsiębiorstw. Wybór przedmiotu badań jest aktualny i odnosi się do ogromnej liczby różniących się przedsiębiorstw. Ta różnorodność wynika między innym z przedmiotu działania przedsiębiorstw, ich form własnościowych, wielkości, intensywności uczestnictwa w łańcucha dostaw oraz dystrybucji, w tym poziomu internacjonalizacji takich łańcuchów. Do tych wyzwań Kandydatka dodała dodatkowy wymiar trudności deklarując gotowość do odwołania się do doświadczeń wybranych państw Unii Europejskiej.

Proces badawczy opisano w monografii i dostarczonej dokumentacji wielokrotnie w różnych formach. Odpowiada on wzorcom stosowanym w naukach zarządzania w Polsce[7].

Analiza literaturowa została przeprowadzona z wykorzystaniem wystarczającej liczby źródeł. Jednak stwierdzam nadreprezentatywność źródeł polskojęzycznych w stosunku do obcojęzycznych. Jest to zaskakujące, ponieważ znakomita większość wyników oryginalnych badań została opisana w językach obcych. Zauważam także doskwierający brak wystarczającego odwoływania się do aktualnych publikacji w czasopismach naukowych zarówno polskojęzycznych jak i międzynarodowych. Wiedza w zakresie cyberbezpieczeństwa podlega szybkiej erozji.

W hipotezie głównej podkreślono ogromne znaczenie dynamizm cyberzagrożeń. Pomijanie zatem aktualnych publikacji z międzynarodowych czasopism naukowych utrudnia określenie nowych determinantów skutecznego zarządzania cyberbezpieczeństwem w przedsiębiorstwie.

Hipotezy szczegółowe oceniam jako banalne i oczywiste. Na przykład hipoteza piąta głosi, że zarządzanie cyberbezpieczeństwem zależy od wielkości, profilu działalności i własności przedsiębiorstwa. Oczywistym jest, że te czynniki wpływają na kształtowanie zarządzania cyberbezpieczeństwem. Inaczej zarządza się cyberbezpieczeństwem w firmie zarządzającej flotą pojazdów, a inaczej w zakładach produkcji amunicji, a jeszcze inaczej funduszem inwestycyjnym. Inne wyzwania i uwarunkowania prawne występują w firmach należących do Państwa, inne w podmiotach

---

[5] Prawo o szkolnictwie wyższym i nauce, Dz. U. 2018 poz. 1668 § 2 pkt. 4.2 umowy o dzieło jaką zawarłem z Politechniką Częstochowską o przeniesieniu autorskich praw majątkowych w sprawie opracowania recenzji w postępowaniu habilitacyjnym

[6] https://difin.pl/difin-w-ministerialnym-wykazie-wydawnictw/

[7] W.Dyduch 2024

gospodarczych, których np. akcje są przedmiotem obrotu na giełdach papierów wartościowych, a jeszcze inne w start upach.

Jako hipotezy banalne oceniam także H3, H5 i H6.[8]

W kontekście postulowanej w hipotezie piątej różnorodności podejść do zarządzania cyberbezpieczeństwem z ogromnym zainteresowaniem podszedłem do realizacji celów pracy. Niestety Autorka monografii nie uwzględnia tej różnorodności tracąc szansę osiągnięcia mniej banalnych celów.

Monografię przeczytałem z wielkim zainteresowaniem, ponieważ wraz z moim zespołem w ostatnich latach zajmowaliśmy się przynajmniej dwoma obszarami wspomagającymi zapewnienie cyberbezpieczeństwa zarówno na poziomie państw jaki i na poziomie przedsiębiorstw, które wdrożyły nasze narzędzia.

Projekty *SIMMO1, SIMMO2*[9] i *HANSA* oferują narzędzia pozwalające przeprowadzać nie tylko bieżącą, ale także retrospektywną analizę ruch statków na wszystkich oceanach i morzach. Dane gromadzone są przez satelity, a analizowane przez nasze narzędzia. Analiza retrospektywa pozwala trafniej badać zachowania statków w czasie rzeczywistym, ale także przewidywać ich możliwe operacje. Analizy predykcyjne są bardzo przydatne na przykład dla przedsiębiorstw logistycznych skupiających się zarządzaniu logistyką nośników energii lub innych zasobów krytycznych[10]. Poprawność prowadzonych analiz stwarza przesłanki do poprawy cyberbezpieczeństwa żeglugi, a w konsekwencji do zapewnienia cyberbezpieczeństwa łańcuchów dostaw.

Drugi wątek naszych badań dotyczących cyberbezpieczeństwa związanych jest z naszym projektem - *OpenFact,* który doprowadził do przygotowania platformy wyspecjalizowanych narzędzi służącymi przeciwdziałania dezinformacji.

Porównanie obu wątków badań pokazuje, że badanie ruchów statków na morzach i oceanach świata może być przedmiotem dezinformacji. W konsekwencji nawet najbardziej precyzyjne wyniki zastosowania narzędzi służących analizie nawigacji mogą być zakłócane przez dezinformację. Aby zapewnić odpowiedni poziom cyberbezpieczeństwa w opisanych scenariuszach potrzebujemy obu naszych narzędzi. Ten rozbudowany przykład wskazuje na złożoność przedmiotu badań, którymi zainteresowała się Kandydatka.

Niestety banalność hipotez sformułowanych w monografii przekreśliła szanse możliwość znalezienia rekomendacji dla efektywnego zarządzania naszymi narzędziami w przedsiębiorstwach. Skuteczne zapewnienie cyberbezpieczeństwa możliwe jest tylko, kiedy w przedsiębiorstwie wdrożymy specjalizowane narzędzia odpowiadające jego celom.

Do realizacji celów monografii wybrano studium przypadku, badania ankietowe i wywiady eksperckie. Stosowane metody i techniki badań odpowiadają narzędziom stosowanym w naukach o zarządzaniu.

---

[8] por. Monografia str. 14.

[9] Realizowane na zlecenie Europejskiej Agencji Obrony.

[10] W trakcie pisania tej recenzji wyniki badań zostały potwierdzone analizami kontroli żeglugi nad cieśninę Ormuz, przez którą przepływa ok. 20% światowych dostaw ropy. Globalne analiza możliwości nawigacji pozwala badać konsekwencje tego konfliktu logistyki innych surowców.

Bardzo skromna lista aktów prawnych odnoszących się do cyberbezpieczeństwa pozwala wnosić, że Kandydatka skupiła się na rekomendacjach dla podmiotów gospodarczych działających w Polsce[11]. Z tytułu można wnosić, że monografia poświęcona jest nieokreślonym bliżej państwom Unii Europejskiej. Jednakże z lektury monografii wynika zainteresowanie Kandydatki tylko krajami Trójkąta Weimarskiego. Nie świadczy to o spójność pomiędzy tytułem monografii i jej zawartością. Bardzo skromna lista aktów prawnych cytowanych w monografii pomija zupełnie Francuskie i NIemieckie **akty** prawne, z których można byłoby wywnioskować **normy** prawne odnoszące się do cyberbezpieczeństwa w poszczególnych krajach. Nie można przeprowadzić solidnej rekomendacji dla zarządzania cyberbezpieczeństwem bez analizy uwarunkowań prawnych badanego przedsiębiorstwa. Różnorodność systemów prawa, norm prawnych oraz pragmatyki w ich stosowaniu różnicuje determinanty będące przedmiotem rozważania w ocenianej monografii.

Oprócz aktów prawnych, podstawy normatywne działań w zakresie cyberbezpieczeństwa mogą być sformułowane w formie standardów i norm pozaprawnych, np technicznych. Analiza wybranych norm i standardów została przedstawione w formie tabelarycznej w monografii[12]. Niestety nie uwzględniono zakresu obowiązywania tych norm i standardów dla Polskich, Francuskich i Niemieckich podmiotów gospodarczych. Ponieważ monografia nie obejmuje komparatystyki prawniczej i normatywnej, zapewne łatwiejsze byłoby wskazanie jedynie uregulowań normatywnych odnoszących się do badanych państw.

Z dużym zainteresowaniem zapoznałem się z częścią monografii poświęconym praktycznym aspektom zarządzania cyberbezpieczeństwem. Poprawnie zastosowano zróżnicowane metody badawcze. Zapewne każdy z czytelników chciałby dowiedzieć się czegoś innego, dlatego nie podaję dyskusji wyników tych badań. Tę część monografii oceniam najwyżej.

Ponieważ hipotezy szczegółowe oceniłem jako banalne i oczywiste, to wyniki przeprowadzonych badań niestety nie grzeszą oryginalnością. Niemniej mimo tej wady, to w kontekście ich bardzo wysokiej aktualności[13] pozwalam sobie rekomendować je czytelnikom[14].

Mimo krytycznych uwag oceniam monografię pozytywie. Za tą oceną przemawia poprawnie i konsekwentnie przeprowadzony proces badawczy. Interesujące są badania związane z praktycznymi aspektami zarządzania cyberbezpieczeństwem w trzech wybranych państwach. Pozanaukowym argumentem dla pozytywnej oceny monografii jest jej trudne do przecenienia stworzenie kolejnej okazji do refleksji nad cyberbezpieczeństwem.

Warunek konieczny określony w artykule 219 ustęp 1 punkt 2 został przez Kandydatkę spełniony, ponieważ w minimalnym stopniu przyczyniła się do rozwoju dyscypliny o zarządzaniu i jakości.

[11] Por. Monografia str. 115 - 117.

[12] Por. Monografia str. 307 i 308.

[13] Przynajmniej w czasie publikacji monografii. Takie podejście uważam za właściwe przy ocenie ex post prac naukowych.

[14] Por. Monografia str. 298

Spełnienie warunku określonego w art. 219 ust. 1 pkt 3[15].

Analiza dorobku Kandydatki ujętych w bazach *Web of Science, Scopus, Google Scholar* sporządzona przez Centrum Analiz Bibliometrycznych i Komunikacji Naukowej Wojskowej Akademii Technicznej wykazuje, że główne osiągnięcie naukowe, czyli monografia *Zarządzanie cyberbezpieczeństwem w przedsiębiorstwie - doświadczenia wybranych państw Unii Europejskiej,* ***n*ie było cytowane ani razu**. Jest to niepokojące, ponieważ monografia została opublikowana w znanym wydawnictwie, które mimo upływu czasu w dalszym ciągu sprzedaje książkę wydaną w roku 2024, która niestety zdaniem czytelników nie zasługuje na cytowania[16]. **W konsekwencji nie można uznać głównego osiągnięcia naukowego jako dowodu świadczącego o zauważeniu dorobku naukowego Kandydatki przez środowisko naukowe**.

Łączna analiza dorobku przygotowanego przez cytowane Centrum WAT prezentuje następujące dane naukometryczne:

Sumaryczny IF = 0

Web of Science

- *Liczba publikacji 2*
- *Liczba cytowań 1*
- *Indeks Hirscha 1*

Scopus

- *Liczba publikacji 1*
- *Liczba cytowań 3*
- *Indeks Hirscha 1*

Google Scholar

- *Liczba publikacji 45*
- *Liczba cytowań 90*
- *Indeks Hirscha 4*

Tak niski IF oraz indeks Hirscha nie wskazuje na istotną aktywność naukową Kandydatki udokumentowaną publikacjami cieszącymi się uznaniem w środowisku naukowym.

Kandydatka odbyła 6 miesięczny staż w Politechnice Częstochowskiej. Jest on bardzo dobrze udokumentowany publikacjami krajowymi i zbudowaniem różnorodnych form współpracy z

---

[15] Prawo o szkolnictwie wyższym i nauce, Dz. U. 2018 poz. 1668 § 2 pkt. 4.2 umowy o dzieło jaką zawarłem z Politechniką Częstochowską o przeniesieniu autorskich praw majątkowych w sprawie opracowania recenzji w postępowaniu habilitacyjnym

[16] https://ksiegarnia.difin.pl/zarzadzanie-cyberbezpieczenstwem-w-przedsiebiorstwie-doswiadczenia-wybranych-panstw-unii-europejskiej?search=antczak

pracownikami PCz. **Spełnione jest zatem kryterium istotnej aktywności naukowej na więcej niż jednej uczelni (w tym przypadku WAT i PCz)**.

Kandydatka dokumentuje swój udział w projektach[17]. Ocenia je jako międzynarodowe oraz jako naukowe.

Projekt DIMAS (Digital Mathematics Applied in Defence and Security Education) jest projektem międzynarodowym, ale **nie jest projektem badawczym**. Jego celem jest zwiększenie zainteresowania nauką matematyki studentów uczelni wojskowych i cywilnych. Skupiono się na kierunkach związanych z bezpieczeństwem. Celem projektu jest skłonienie studentów i uczelni do lepszego wykorzystanie nowoczesnych narzędzi cyfrowych (np. Python, Matlab, SolidWorks) oraz scenariuszy opartych na rzeczywistych problemach z zakresu obronności[18].

Drugi projekt o nazwie *Innowacyjna i sprawna administracja źródłem sukcesu w gospodarce opartej na wiedzy* był realizowany przez Związek Powiatów Polskich (lider projektu) i Uczelnię Vistula. Nie był projektem badawczym, nie był też projektem międzynarodowym[19]. Umieszczenie tego projektu na liście dokumentującej międzynarodową współpracę naukową jest działaniem nieetycznym.

W rezultacie nie spełniono kryterium istotnej współpracy naukowej z przynajmniej jedną uczelnią zagraniczną.

Warunek konieczny określony w artykule 219 ustęp 1 punkt 3 nie został przez Kandydatkę spełniony.

Wnioski

Na podstawie podsumowań cząstkowych sformułowanych w recenzji stwierdzam, że:

1) Warunek określony w artykule 219 ustęp 1 punkt 1 został przez Kandydatkę spełniony.
2) Warunek określony w artykule 219 ustęp 1 punkt 2 został przez Kandydatkę spełniony w minimalnym zakresie.
3) Warunek określony w artykule 219 ustęp 1 punkt 3 nie został przez Kandydatkę spełniony.

Oceniając powyższe aspekty dorobku naukowego Pani dr Joanny Antczak **nie rekomenduję kontynuowania postępowania w sprawie nadania Kandydatce stopnia doktora habilitowanego.**

PODPIS ZAUFANY
WITOLD ROBERT
ABRAMOWICZ
11.04.2026 14:20:02 GMT+0200
Dokument podpisany elektronicznie
podpisem zaufanym

[17] Por. Wykaz osiągnięć naukowych albo artystycznych… str. 17

[18] https://dimas-project.eu/

[19] https://www.zpp.pl/artykul/654-innowacyjna-i-sprawna-administracja-zrodlem-sukcesu-w-gospodarce-opartej-na-wiedzy