prof. dr hab. inż. Zbigniew Kotulski
Instytut Telekomunikacji i Cyberbezpieczeństwa
Politechniki Warszawskiej
ul. Nowowiejska 15/19, 00-665 Warszawa

Warszawa, 15.08.2025 r.

**Recenzja osiągnięcia naukowego, dorobku naukowo-badawczego, dydaktycznego i popularyzatorskiego oraz współpracy międzynarodowej pani doktor inżynier Sabiny Szymoniak w związku z postępowaniem w sprawie nadania stopnia doktora habilitowanego w dziedzinie nauk inżynieryjno-technicznych w dyscyplinie informatyka techniczna i telekomunikacja, wszczętym w dniu 30 grudnia 2024 r.**

## 1. Wprowadzenie

Niniejsza recenzja została sporządzona związku z powołaniem mnie przez Radę Doskonałości Naukowej na recenzenta w postępowaniu w sprawie nadania stopnia doktora habilitowanego w dziedzinie nauk inżynieryjno-technicznych w dyscyplinie informatyka techniczna i telekomunikacja wszczętego w dniu 30 grudnia 2024 r. na wniosek dr inż. Sabiny Szymoniak oraz z Uchwałą Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja Politechniki Częstochowskiej, o czym zostałem poinformowany pismem Prodziekana ds. nauki Informatyka techniczna i telekomunikacja, Wydział Informatyki i Sztucznej Inteligencji dr. hab. inż. Adama Kulawika, profesora Politechniki Częstochowskiej z dnia 3 czerwca 2025 roku, R-WiiSI-BOD.521.1.2025.

Recenzja wykonana jest na podstawie nadesłanej dokumentacji postępowania habilitacyjnego (teczka z dokumentami oraz dokumenty na nośniku elektronicznym), na którą składają się:

- Zbiór14 artykułów stanowiących osiągniecie naukowe pani dr inż. Sabiny Szymoniak opatrzonych wspólnym tytułem „*Metody wzmacniania bezpieczeństwa systemów cyberfizycznych*”,
- kopia dyplomu potwierdzającego nadanie pani Sabinie Szymoniak stopnia doktora nauk technicznych w zakresie informatyki nadanego przez Radę Wydziału Inżynierii Mechanicznej i Informatyki Politechniki Częstochowskiej w dniu 29 czerwca 2017 roku;

- autoreferat w języku polskim,
- wykaz osiągnięć naukowych stanowiących znaczny wkład w rozwój dyscypliny informatyka techniczna i telekomunikacja,
- 27 zaświadczeń potwierdzających różne formy aktywności Habilitantki wykazane w dokumentacji wniosku,
- kopie oświadczeń współautorów o merytorycznym wkładzie w powstawanie prac wchodzących w skład osiągnięcia,
- dane osobowe wnioskodawcy, w tym wskazanie miejsca zatrudnienia i adresu korespondencyjnego.

## 2. Opinia o osiągnięciu naukowym przedstawionym do oceny

Jako swoje osiągnięcie naukowe wymagane we wniosku o przeprowadzenie postępowania habilitacyjnego pani doktor inżynier Sabina Szymoniak przedstawiła cykl czternastu publikacji naukowych powiązanych tematycznie (9 artykułów w czasopismach i 5 publikacji konferencyjnych), zatytułowany *„Metody wzmacniania bezpieczeństwa systemów cyberfizycznych”*, opublikowanych w latach 2021-2024. Wśród tych publikacji, 5 jest indywidualnymi pracami Habilitantki (ocenianymi przez Ministerstwo na 200, 140, 100, 100 i 70 punktów). Pozostałe publikacje są współautorskie: cztery prace dwóch autorów, trzy prace trzech autorów oraz po jednej pracy czterech i pięciu autorów. W sześciu spośród dziesięciu prac wspólnych, pani doktor Sabina Szymoniak jest pierwszym współautorem. Jej deklarowany procentowy udział w tych pracach wynosi: 90% w trzech artykułach i 45% w jednym artykule (dominujący wkład) oraz 33,3% w dwóch, 50% w jednej, 25% w jednej i 20% w jednej (równy udział). Jak widać z powyższego zestawienia, pani doktor Sabina Szymoniak przedstawiła cykl artykułów wskazujący dominujący indywidualny wkład do badań przedstawionych jako osiągniecie naukowe a zarazem umiejętność pracy w zespole naukowym, w tym identyfikowaniu i formułowaniu ważnych problemów badawczych i kierowaniu pracami prowadzącymi do powstania publikacji akceptowanych w renomowanych czasopismach. Łączna liczba punktów przedstawionych artykułów to PM=1460, a wskaźnik wpływu IF5Y=45,72. Są to wartości bardzo wysokie.

Artykuły naukowe przedstawione pod wspólnym tytułem „*Metody wzmacniania bezpieczeństwa systemów cyberfizycznych*” dotyczą szerokiego zakresu badań

dotyczących protokołów kryptograficznych i ich zastosowań. Niektóre z nich mają charakter przeglądowy, inne są prezentacja konkretnych rozwiązań bezpieczeństwa lub nowych metod badawczych. Dlatego też każda z przedstawionych publikacji wymaga niezależnego omówienia. Habilitantka przedstawiła wykaz artykułów stanowiących osiągniecie naukowe w kolejności rankingowej miejsca ich publikacji. Dla celów sporządzenia tej recenzji zmieniłem tę kolejność grupując prace do następujących kategorii: prac przeglądowych, prac dotyczących rozwiązań bezpieczeństwa chroniących przed fałszywymi połączeniami, monitorowaniem zanieczyszczeń powietrza, ochroną urządzeń IoT, wykorzystaniem metod sztucznej inteligencji oraz badaniem poprawności i bezpieczeństwa protokołów kryptograficznych. W swoim autoreferacie Habilitantka również zmieniła kolejność omawiania publikacji w stosunku do ich wykazu grupując tematycznie swoje wyniki w nieco inny sposób niż przedstawiony powyżej. Ja jednak zaprezentuje ocenę tych osiągnięć w innej kolejności.

**Artykuły przeglądowe.**

Spośród artykułów przeglądowych swojego autorstwa Habilitantka wybrała trzy prace tematycznie związane z obszarem badawczym osiągnięcia naukowego. Prace te są opublikowane w prestiżowych czasopismach i w stosunkowo krótkim czasie od opublikowania uzyskały wiele cytowań: [P4] 2022 rok, 39 cytowań, [P1] 2024 rok, 19 cytowań, [P6] 2023 rok, 8 cytowań. Dwie pierwsze z tych prac: *[P4] Szymoniak Sabina, Kesar Shalini, "Key Agreement and Authentication Protocols in the Internet of Things: A Survey", Applied Sciences, 13, 404, 2022* oraz [*P1] Szymoniak Sabina, "Key Distribution and Authentication Protocols in Wireless Sensor Networks: A Survey", ACM Computing Surveys, 56, 1–31, 2024* poświęcone są problematyce zapewnienia bezpiecznych kluczy kryptograficznych urządzeniom sieci słabych urządzeń oraz ich uwierzytelnienia i wzajemnego uwierzytelnienia. Prace mają podobną strukturę: zawierają omówienie znanych protokołów bezpieczeństwa i przedstawienie znanych ataków dla, odpowiednio, sieci IoT oraz WSN. Wartościowym i twórczym ich elementem są tabele przedstawiające dla omawianych protokołów wskazane zastosowania, znane ataki, wykryte podatności, itd. Problematyka tych prac należy już do klasyki metod ochrony informacji. W kontekście przedstawionego do oceny osiągnięcia naukowego prace te stanowią jednak

niezbędny wstęp przedstawiający stan sztuki w zakresie budowy kryptograficznych protokołów bezpieczeństwa dla systemów cyberfizycznych.

Trzecia z prac przeglądowych przedstawionych przez Habilitantkę, czyli *[P6] Szymoniak Sabina, Depta Filip, Karbowiak Łukasz, Kubanek Mariusz, "Trustworthy Artificial Intelligence Methods for Users' Physical and Environmental Security: A Comprehensive Review", Applied Sciences, 13, 12068, 2023*, dotyczy tematyki dzisiaj bardzo aktualnej, czyli sztucznej inteligencji w zastosowaniach związanych z bezpieczeństwem osób (użytkowników). W tym wypadku istotne jest zarówno zadbanie o bezpieczeństwo użytkowników, czyli przygotowania odpowiednich zabezpieczeń, jak również zapewnienie bezpieczeństwa samej metody ochrony często atakowanej różnorodnymi technikami, także z wykorzystaniem sztucznej inteligencji. W pracy omówiono różne aspekty tematyki takie jak przegląd metod AI przydatnych do ochrony użytkowników, zastosowania w różnych obszarach technologii informatycznych, wykaz baz danych w różnych obszarach zastosowań służących do treningu w uczeniu maszynowym oraz przykłady ataków na metody AI. Wszystkie te przykłady związane są z cytowanymi publikacjami i są usystematyzowane w poglądowych tabelach. Ta publikacja jest dobrym wstępem i przedstawieniem stanu sztuki dla publikacji oryginalnych dotyczących wykorzystania AI w bezpieczeństwie systemów cyberfizycznych.

Jak widać z powyższego omówienia załączonych prac, wśród publikacji przeglądowych nie ma jedynie artykułu dotyczącego formalnych metod badania poprawności i bezpieczeństwa protokołów kryptograficznych i ich zastosowań. W dalszej części tej recenzji omówię publikacje dotyczące bezpieczeństwa protokołów kryptograficznych w różnych zastosowaniach: ochrony przed fałszywymi połączeniami (linkami), bezpiecznego monitorowania propagacji zanieczyszczeń i bezpieczeństwa sieci IoT w zastosowaniach,

**Publikacje dotyczące ochrony przed fałszywymi linkami.**

Tej tematyce poświęcone są dwie indywidualne prace Habilitantki: mający 7 cytowań artykuł konferencyjny *[P13] Szymoniak Sabina, "Using A Security Protocol To Protect Against False Links", Moving technology ethics at the forefront of society, organisations and governments, 513–525, 2021* oraz jego rozszerzona i poprawiona wersja z czasopisma: *[P2] Szymoniak Sabina, "Amelia—A new security protocol for*

*protection against false links", Computer Communications, 179, 73–81, 2021* (16 cytowań). W tych artykułach zaproponowano protokół zabezpieczający łącza internetowe (o nazwie Amelia) pozwalający na weryfikację adresów URL w komunikacji klient-serwer ze wsparciem dwóch niezależnych urzędów certyfikacji. Prezentacja protokołu pomija etapy ustanawiania kluczy publicznych i prywatnych (rejestracji użytkowników) i zakłada ustanowiony bezpieczny kanał komunikacyjny między urzędami DC i AC. Protokół Amelia składa się z dwóch podprotokołów: zgłoszenia przez użytkownika chęci skorzystania z połączenia do urzędów certyfikacji oraz dostarczenia klucza połączenia przez serwer łączącemu się użytkownikowi, uwiarygodnionego przez urzędy certyfikacji. W publikacji [P2] ten podprotokół jest uzupełniony o piąty krok -handshake. W pierwszym z tych artykułów brak jest wyodrębnionych definicji oznaczeń identyfikatorów i kluczy użytych w specyfikacji protokołu. W drugiej publikacji przedstawiono oznaczenia tych wielkości; oznaczenie definicji klucza symetrycznego do komunikacji między klientem i serwerem zawiera błąd literowy. Przedstawiony protokół został zweryfikowany pod względem bezpieczeństwa działania z wykorzystaniem czterech współcześnie używanych narządzi programistycznych (w tym jednym współautorstwa Habilitantki) oraz czasu realizacji kroków protokołu.

**Publikacje dotyczące monitorowania propagacji zanieczyszczeń.**

Są to dwa artykuły autorstwa trzech osób: publikacja konferencyjna *[P11] Bobulski Janusz, Szymoniak Sabina, Pasternak Kamila, "Safe data transmission in IoT system for air pollution monitoring", 2023 IEEE International Conference on Big Data (BigData), 5438–5443, 2023* i jej poszerzona wersja opublikowana w czasopiśmie naukowym: [*P8] Bobulski Janusz, Szymoniak Sabina, Pasternak Kamila, "An IoT System for Air Pollution Monitoring with Safe Data Transmission", Sensors, 24, 445, 2024*. Prace przedstawiają raport z badań terenowych systemu monitorowania zanieczyszczeń, w których system bezpiecznej komunikacji wykorzystuje protokół Amelia. Zaprezentowano tu architekturę systemu i wyniki badań wydajności jego elementów. Ta praca w stosunkowo krótkim czasie uzyskała 20 cytowań w publikacjach naukowych.

**Bezpieczeństwo sieci IoT.**

Kolejna grupa trzech artykułów poświęcona jest ustanawianiu bezpiecznej komunikacji między urządzeniami IoT. Wspólnym elementem protokołów

bezpieczeństwa występującym w proponowanych rozwiązaniach jest korzystanie z centralnego serwera uwierzytelniającego uczestników komunikacji i dostarczającego kluczy symetrycznych do zabezpieczania przesyłanych komunikatów. Artykuł *[P12] Szymoniak Sabina, Siedlecka-Lamch Olga, "Securing Meetings in D2D IoT Systems", Effectiveness of ICT ethics – How do we help solve ethical problems in the field of ICT? pp.30–41, 2022*, cytowany 7 razy, proponuje system do komunikacji w grupie urządzeń przenośnych w sesji zainicjowanej przez jednego z uczestników z możliwością dołączania innych urządzeń. Protokół bezpieczeństwa składa się z trzech podprotokołów: rejestracji użytkowników, dystrybucji klucza sesyjnego do zarejestrowanych użytkowników wskazanych przez inicjatora sesji oraz dystrybucji informacji od inicjatora sesji do pozostałych uczestników. W artykule brakuje wykazu oznaczeń dla podprotokołów 2 i 3 oraz występują niejednoznaczności w oznaczeniach inicjatora sesji (czasem jako jednolity tekst, czasem z indeksem dolnym). Podobne niekonsekwencje oznaczeń są zawarte w autoreferacie. W pracy przeprowadzono wstępną analizę bezpieczeństwa tego protokołu wykorzystując analizę czasów wykonywania kroków protokołu, co jest ciekawym podejściem do tego problemu.

Podobny trzyetapowy protokół bezpieczeństwa przeznaczony dla zastosowań w służbie zdrowia został zaproponowany w pracy *[P9] Szymoniak Sabina, "Secure System with Security Protocol for Interactions in Healthcare Internet of Things", Bulletin of the Polish Academy of Sciences Technical Sciences, 72, e151049, 2024*. Tutaj również analizę bezpieczeństwa przeprowadzono na podstawie przebiegów czasowych operacji bezpieczeństwa w podprotokołach.

Trzeci z tej grupy artykułów: *[P10] Szymoniak Sabina, "Security protocol for securing notifications about dangerous events in the agglomeration", Pervasive and Mobile Computing, 105, 101977, 2024* dotyczy bezpiecznej komunikacji między różnorakimi urządzeniami służącymi do monitorowania bezpieczeństwa w terenach zurbanizowanych. W szczególności, celem protokołu jest umożliwienie obywatelom dołączenie do systemu i przesyłanie danych ze swoich prywatnych urządzeń. Do uwierzytelnienia tych urządzeń służą bilety zawierające klucze symetryczne (nazwane przez autorkę certyfikatami) dystrybuowane w fazie rejestracji. Cały protokół bezpieczeństwa składa się z sześciu podprotokołów. Te podprotokoły zostały przedstawione w notacji Alice-Bob oraz szczegółowo rozpisane w notacji

BAN (co jednak nie jest weryfikacją ich poprawności i bezpieczeństwa: do tego potrzebne byłoby użycie jednego z programów formalnej analizy bezpieczeństwa). Przeprowadzona została analiza czasowa tych podprotokołów. Przedstawiono też argumenty, że zastosowane rozwiązanie chroni przed wybranymi typami ataków oraz przeprowadzono jego analizę wydajnościową.

**Sztuczna inteligencja i inteligentne miasta.**

Kolejne dwie prace przedstawione jako składowe osiągnięci naukowego podlegającego ocenie dotyczą systemów bezpieczeństwa wspomaganych metodami sztucznej inteligencji w zastosowaniach związanych z inteligentną gospodarką municypalną. Prace konferencyjne: *[P14] Szymoniak Sabina, Kesar Shalini, "How can best practices of cybersecurity include artificial intelligence within smart cities", The Leading Role of Smart Ethics in the Digital World, 135–142, 2024* oraz *[P3] Szymoniak Sabina, Kubanek Mariusz, Kesar Shalini, "AI-Based Enhancing of the Smart City Residents' Safety", Harnessing Opportunities: Reshaping ISD in the post-COVID-19 and Generative AI Era (ISD2024), International Conference on Information Systems Development, Gdańsk, Poland, August 26 – 28, 2024, 2024* prezentują zarys architektury bezpieczeństwa w systemach monitoringu miejskiego wykorzystującego rozwiązania oparte na sztucznej inteligencji uzupełnione o element powiadamiania ratunkowego. Obie prace mają podobny charakter. Przedstawiają wymagane podprotokoły i elementy funkcjonalne protokołów bez specyfikacji ich kroków. Stanowią dyskusję stanu sztuki i możliwych sposobów wspomagania zabezpieczeń metodami sztucznej inteligencji. Są raczej zapowiedzią przyszłych i oczekiwanych badań niż prezentacją uzyskanych wyników.

**Weryfikacja protokołów.**

Ostatnia grupa artykułów przedstawionych do oceny dotyczy weryfikacji protokołów bezpieczeństwa, w szczególności protokołów przeznaczonych dla sieci sensorowych. Wspólnym elementem metod zaprezentowanych w dwóch artykułach jest uwzględnienie czasu wykonywania operacji jako elementu oceny bezpieczeństwa. Prace te są najbliższe metodologicznie tematyce rozprawy doktorskiej Habilitantki, stanowią twórcze rozwinięcie prowadzonych tam badań. Pierwsza z prac: *[P5] Szymoniak Sabina, Siedlecka-Lamch Olga, Zbrzezny Agnieszka, Zbrzezny Andrzej, Kurkowski Mirosław, "SAT and SMT-based verification of security protocols including time aspects", Sensors, 21, 3055, 2021*, cytowana w 17 artykułach naukowych,

dotyczy formalnego modelowania protokołów bezpieczeństwa jako sieci zsynchronizowanych automatów czasowych z uwzględnieniem opóźnień w sieci oraz zastosowania dwóch metod nazwanych SAT (ang. Boolean Satisfiability Problem, Problem Spełnialności Formuły Boolowskiej ) i SMT (ang. Satisfiability Modulo Theories, Teoria Spełnialności Modulo) do testów osiągalności stanów. Metody te zostały formalnie zdefiniowane i następnie zilustrowane eksperymentalnie na przykładzie różnych wersji protokołu WooLamPi (WLP) oraz protokołu SNEP.

Druga praca z tego obszaru badań, *[P7] Piątkowski Jacek, Szymoniak Sabina, "Methodology of Testing the Security of Cryptographic Protocols Using the CMMTree Framework", Applied Sciences, 13, 12668, 2023,* 4 cytowania w literaturze, poświęcona jest budowie metody weryfikacji protokołów bezpieczeństwa z wykorzystaniem metody Conditional Multiway Mapped Tree (CMMTree). Habilitantka skonstruowała predykat dla CMMTree pozwalający zbudować drzewo wszystkich możliwych wykonań protokołu bezpieczeństwa oraz wskazać ewentualne wykonania mogące stanowić atak na protokół. Również w tej pracy przedstawiono metodę a następnie zilustrowano jej działanie dla trzech protokołów: Andrew, Andrew-Lowe modified i Needham Schroeder Public Key.

Artykułu przedstawione jako osiągniecie naukowe dokumentują, że pani doktor Sabina Szymoniak wśród swoich dokonań naukowych posiada zarówno artykuły w renomowanych czasopismach jak i prace prezentowane na ważnych konferencjach naukowych. Tak obszerny zastaw prac nie jest jednak konieczny do prezentacji osiągniętych rezultatów badawczych. W kilku przypadkach prace w czasopismach przedstawiają te same wyniki co publikacje konferencyjne, w wersji poszerzonej i poprawionej. Różna jest również wartość naukowa przedstawionych wyników.

Za najważniejsze wyniki naukowe zawarte w tym cyklu publikacji uważam przedstawione metody badania poprawności i bezpieczeństwa protokołów uwzględniające czasy wykonywania poszczególnych kroków i operacji bezpieczeństwa. Ten element jest zarówno głównym przedmiotem publikacji, jak i elementem badania poprawności w pracach przedstawiających protokoły i ich zastosowania. Również wyniki dotyczące konstrukcji nowych protokołów bezpieczeństwa stanowią ważny i nowy rezultat z zakresu ochrony informacji, co potwierdzają liczne cytowania przedstawiających je artykułów.

Pozostałe dwa obszary reprezentowane w recenzowanym cyklu prac to opis stanu sztuki wybranych zakresów ochrony informacji oraz zwrócenie uwagi na wagę problematyki sztucznej inteligencji w ochronie informacji w systemach cyberfizycznych. Pierwszy z nich można uznać za budowę solidnego warsztatu badawczego Habilitantki z równoczesnym dostarczeniem innym badaczom przydatnych informacji (prace z dużą liczbą cytowań). Drugi obszar to prawidłowe zidentyfikowanie przyszłych kierunków rozwoju metod bezpieczeństwa układów cyberfizycznych i zainicjowanie badań w tym zakresie.

Podsumowując tę część recenzji stwierdzam, że wyniki naukowe przedstawione cyklu 14 publikacji są w znacznej większości nowatorskie i oryginalne. Stanowią znaczący wkład do rozwoju wiedzy w dyscyplinie naukowej informatyka techniczna i telekomunikacja w zakresie bezpieczeństwa systemów cyberfizycznych, w szczególności zastosowań Internetu Rzeczy (IoT). Można zatem stwierdzić, że zaprezentowany cykl artykułów w czasopismach i publikacji konferencyjnych stanowi osiągnięcie naukowe wymagane w postępowaniu habilitacyjnym przez *USTAWĘ z dnia 20 lipca 2018 r. „Prawo o szkolnictwie wyższym i nauce”* z późniejszymi zmianami, Dz. U. 2018 poz. 1668. Zawiera zarówno artykuły przeglądowe przedstawiające stan sztuki w wybranych obszarach wykorzystania protokołów kryptograficznych, jak i prace definiujące nowe rozwiązania bezpieczeństwa zgodne ze stanem sztuki. Przedstawiony materiał naukowy może stanowić podstawę przygotowania monografii naukowe wnoszącej istotny wkład do problematyki bezpiecznych aplikacji dla małych urządzań IoT.

## 3. Ocena dorobku naukowo-badawczego i pozostałej działalności naukowej Habilitantki

Pozostały dorobek naukowy pani doktor inżynier Sabiny Szymoniak jest obszerny i wartościowy. Obejmuje 26 publikacji w materiałach konferencyjnych zakwalifikowanych formalnie w dokumentacji wniosku jako rozdziały w monografiach oraz 9 artykułów w czasopismach naukowych. Wszystkie te prace są punktowane zgodnie z rekomendacjami Ministerstwa, w tym także zakwalifikowane jako prace 200, 140 i 100 punktowe. Tematyka wszystkich tych prac jest zbliżona do tematyko artykułów zawartych w osiągnięciu naukowym, jednak obejmuje szerszy obszar zagadnień badawczych. W kilku pracach współautorskich wkład Habilitantki jest

mniejszy niż pozostałych autorów (10%), jednak jest tam też 8 prac indywidualnych. Wśród tych publikacji jest kilka uzyskanych bezpośrednio po uzyskaniu stopnia doktora (od 2017 roku), podczas gdy publikacje zaliczone do osiągniecia naukowego są głównie z lat 2023 i 2024, a najstarsza jest z 2021 roku. Można zatem stwierdzić, że podział całokształtu dorobku naukowego pani doktor Sabiny Szymoniak na część obejmująca osiągniecie naukowe o nadanym mu tytule „*Metody wzmacniania bezpieczeństwa systemów cyberfizycznych*" oraz pozostały dorobek publikacyjny jest merytorycznie uzasadniony zarówno zmieniającymi się w czasie zainteresowaniami naukowymi Habilitantki, jak i koncentracją na określonych problemach badawczych. Obie grupy artykułów są merytorycznie wartościowe, opublikowane w renomowanych czasopismach lub zaprezentowane na ważnych dla dyscypliny naukowej konferencjach. Warto zauważyć, że praca naukowa Habilitantki i będące jej wynikiem publikacje są przygotowywane w różnych konfiguracjach autorskich: zarówno z badaczami bardziej doświadczonymi (np. z promotorem Jej rozprawy doktorskiej), współpracownikami będącymi na podobnym etapie kariery naukowej, z młodszymi współpracownikami (studentami i doktorantami), a także indywidualnie, co obecnie nie jest zjawiskiem powszechnym w nauce. Świadczy o dużej aktywności i inicjatywie naukowej Habilitantki. Co ważne, po złożeniu przez Habilitantkę wniosku o przeprowadzenie postępowania w sprawie nadania stopnia doktora habilitowanego nastąpił wzrost wskaźników we wszystkich pozycjach tabeli bibliometrycznej, zarówno liczby publikacji jak i cytowań. Świadczy to o trwającej aktywności naukowej Habilitantki i zainteresowaniu Jej pracami.

| Baza | Web of Science | | Scopus | | Google Scholar` | |
|---|---|---|---|---|---|---|
| | 2024 | 12.08.25 | 2024 | 12.08.25 | 2024 | 12.08.25 |
| publikacji | **24** | **32** | **34** | **39** | **56** | **62** |
| cytowań | **89** | **129** | **167** | **232** | **271** | **397** |
| bez autocytowań | **49** | **72** | **96** | **-** | **143** | **-** |
| H-indeks | **6** | **7** | **8** | **9** | **10** | **13** |

Oprócz przygotowywania publikacji Habilitantka wykazała się też dużą aktywnością w zakresie organizacji i wspomagania nauki uczestnicząc w komitetach naukowych konferencji oraz przygotowując recenzje publikacji dla czasopism i konferencji.

Aktywność ta stanowi znaczący wkład w dyscyplinę naukową informatyka techniczna i telekomunikacja i potwierdza wysoka pozycje naukowa Habilitantki.

## 4. Ocena współpracy z otoczeniem społecznym i gospodarczym

W tym punkcie dokumentacji Habilitantka nie wyszczególniła żadnych rodzajów aktywności. Prawdopodobnie nie chciała powtarzać części informacji z wcześniejszych punktów, między innymi danych projektów badawczych realizowanych na rzecz gospodarki narodowej lub wspólnie z organizacjami gospodarczymi. Do tego typu aktywności można też zaliczyć prelekcje na konferencjach dla organizacji gospodarczych wymienione w innym punkcie wniosku. Działania te nie są szczególnie liczne, jednak świadczą o możliwości prowadzenia przez Habilitantkę pracy zorientowanej praktycznie.

## 5. Oceny dorobku dydaktycznego i popularyzatorskiego oraz współpracy międzynarodowej

Pani doktor inżynier Sabina Szymoniak jako pracownik naukowo-dydaktyczny uczelni, ma bogaty dorobek w zakresie przygotowywania i prowadzenia wykładów oraz opieki na pracami dyplomowymi. Należy również do niego prowadzenie zajęć na inne uczelni niż macierzysta Politechnika Częstochowska (w tym wypadku - UKSW) w Warszawie). Do ponadstandardowych aktywności z zakresie dydaktyki należą: opieka nad studiami w zakresie cyberbezpieczeństwa, kołem naukowym studentów i jedną doktorantką (jako promotor pomocniczy). Godne uwagi jest też angażowanie studentów do wspólnego publikowania wyników badań (8 artykułów) oraz działalność popularyzatorska (wykłady dla uczniów w szkołach średnich, organizowanie na uczelni wydarzeń popularyzujących Cyberbezpieczeństwo, udział w audycjach radiowych i telewizyjnych, itd.). Habilitantka współpracuje z dwoma zagranicznymi ośrodkami naukowymi. Współpraca ta zaowocowała kilkoma wspólnymi publikacjami naukowymi z uczonymi zagranicznymi.

Podsumowując ten wykaz aktywności dydaktycznej i popularyzatorskiej Habilitantki można stwierdzić, że jest on obszerny i różnorodny. Oceniając łącznie dorobek dydaktyczny, popularyzatorski oraz współpracę międzynarodową uważam, że spełniają one wymogi Ustawy.

## 6. Opinia końcowa

Pani dr inż. Sabina Szymoniak przedstawiła jako swoje osiągnięcie naukowe cykl powiązanych tematycznie publikacji, w tym część współautorskich w których jej udział w pracy badawczej został należycie udokumentowany. Przedstawiła również wykaż innych publikacji naukowych świadczący o jej dużej aktywności naukowej prowadzonej także we współpracy z badaczami z innych uczelni, w tym uczelni zagranicznych. Udokumentowała także swoją aktywność w zakresie organizacji nauki i prace popularyzatorskie w zakresie nauki. Przedstawiona dokumentacja wniosku mogłaby być bardziej szczegółowa w zakresie wyszczególniania i opisu poszczególnych obszarów aktywności Habilitantki, jednak nawet w obecnej postaci pozwala potwierdzić spełnienie wszystkich wymagań stawianych wnioskom habilitacyjnym przez Ustawę. Bezsprzecznie najsilniejszym elementem wniosku jest obszerny i znaczący dorobek publikacyjny.

Reasumując stwierdzam, że wyniki naukowe pani doktor inżynier Sabiny Szymoniak uzyskane w drodze badań przeprowadzonych indywidualnie i w zespołach badawczych, udokumentowane przedstawionymi publikacjami (w szczególności zbiorem stanowiącym osiągnięcie naukowe zatytułowane „*Metody wzmacniania bezpieczeństwa systemów cyberfizycznych*"), spełniają wymaganie stawiane przez *Ustawę z dnia 20 lipca 2018 r. „Prawo o szkolnictwie wyższym i nauce" z późniejszymi zmianami, Dz. U. 2018 poz. 1668*. Wnioskuję zatem o nadanie pani doktorowi inżynier Sabinie Szymoniak stopnia doktora habilitowanego w dziedzinie nauk inżynieryjno-technicznych w dyscyplinie informatyka techniczna i telekomunikacja.

.....

prof. dr hab. inż. Zbigniew Kotulski