ul. Jagiellońska 57/59
03-301 Warszawa
tel. 22 519 21 00
akademia@kozminski.edu.pl
kozminski.edu.pl

AKADEMIA
LEONA KOŹMIŃSKIEGO

dr hab. Bogdan Księżopolski
Katedra Cyberbezpieczeństwa
Akademia Leona Koźmińskiego

Warszawa, 31.08.2025 r.

Recenzja osiągnięć naukowych oraz istotnej aktywności naukowej w postępowaniu habilitacyjnym dr inż. Sabiny Szymoniak w dziedzinie nauk technicznych, w dyscyplinie informatyka techniczna i telekomunikacja

1. Wprowadznie

Niniejsza recenzja została przygotowana na zlecenie Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja Politechniki Częstochowskiej (Uchwała nr 19/2024/2025 z dnia 20 marca 2025 r.) oraz na podstawie zawiadomienia o wyznaczeniu na recenzenta w komisji habilitacyjnej w postępowaniu w sprawie nadania stopnia doktora habilitowanego podpisanego przez Przewodniczącego Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja Politechniki Częstochowskiej dr. hab. inż. Mariusza Kubanka (z dnia 11 czerwca 2025 r.).

Recenzja została przygotowana w oparciu o materiały prezentujące (1) osiągnięcie naukowe dr inż. Sabiny Szymoniak wraz z autoreferatem oraz (2) dorobek naukowy, w szczególności wykaz opublikowanych prac naukowych, a także informacje o działalności naukowej. Na początku wyrażę opinię na temat osiągnięcia dr inż. Sabiny Szymoniak, a następnie odniosę się do dorobku naukowego oraz dydaktycznego.

2. Ocena osiągnięcia naukowego

Przedmiotem oceny jest osiągnięcie naukowe w formie cyklu publikacji powiązanych ze sobą tematycznie, obejmujących 14 pozycji opublikowanych w latach 2021-2024. Prace te są opublikowane: w czasopismach z IF (9 pozycji) oraz w materiałach konferencyjnych (5 pozycji). Osiągnięcie jest zatytułowane: „**Metody wzmacniania bezpieczeństwa systemów cyberfizycznych**”. Są to wyszczególnione poniżej publikacje (w porządku określonym w autoreferacie):

1. Szymoniak Sabina, “**Key Distribution and Authentication Protocols in Wireless Sensor Networks: A Survey**”, ACM Computing Surveys, 56, 1–31, 2024. IF5Y = 21.1, Q1, WoS, PM=200, U=100%
2. Szymoniak Sabina, “**Amelia - A new security protocol for protection against false links**”, Computer Communications, 179, 73–81, 2021. IF5Y = 4.07, Q1, WoS, PM=140, U=100%

3. 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. PM=140, U=45%
4. Szymoniak Sabina, Kesar Shalini, "**Key Agreement and Authentication Protocols in the Internet of Things: A Survey**", Applied Sciences, 13, 404, 2022. IF5Y = 2.9, Q2, WoS, PM=100, U=90%
5. 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. IF5Y = 4.05, Q2, WoS, PM=100, U=20%
6. 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. IF5Y = 2.7, Q2, WoS, PM=100, U=25%
7. Piątkowski Jacek, Szymoniak Sabina, "**Methodology of Testing the Security of Cryptographic Protocols Using the CMMTree Framework**", Applied Sciences, 13, 12668, 2023. IF5Y = 2.7, Q2, WoS, PM=100, U=50%
8. Bobulski Janusz, Szymoniak Sabina, Pasternak Kamila, "**An IoT System for Air Pollution Monitoring with Safe Data Transmission**", Sensors, 24, 445, 2024. IF5Y = 3.7, Q2, WoS, PM=100, U=33,3%
9. Szymoniak Sabina, "**Secure System with Security Protocol for Interactions i Healthcare Internet of Things**", Bulletin of the Polish Academy of Sciences Technical Sciences, 72, e151049, 2024. IF5Y = 1.1, Q2, PM=100, U=100%.
10. Szymoniak Sabina, "**Security protocol for securing notifications about dangerous events in the agglomeration**", Pervasive and Mobile Computing, 105, 101977, 2024. IF5Y = 3.4, Q2, WoS, PM=100, U=100%
11. 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. PM=70, U=33,3%
12. 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?, 30–41, 2022. PM=70, U=90%
13. 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. PM=70, U=100%

14. 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. PM=70, U=90%

Dwie prace z przedstawionego cyklu opublikowane zostały w renomowanych czasopismach z wysokim wskaźnikiem IF (ACM Computing Surveys, Computer Communications). Prace dotyczą siedmiu zagadnień badawczych:

1. Opracowanie efektywnej metody weryfikacji protokołów sensorowych przy użyciu technik SAT i SMT.
2. Opracowanie efektywnej metody weryfikacji protokołów sensorowych przy użyciu CMMTree.
3. Opracowanie bezpiecznej metody komunikacji chroniącej przed fałszywymi adresami URL.
4. Opracowanie architektury bezpiecznego systemu cyberfizycznego opartego na IoT służącego do monitorowania zanieczyszczeń powietrza, z dedykowanym protokołem zabezpieczającym.
5. Opracowanie bezpiecznej metody komunikacji służącej do uzgadniania spotkań, uwzględniającej architekturę bezpiecznego systemu cyberfizycznego oraz dedykowany protokół zabezpieczający.
6. Opracowanie bezpiecznej metody komunikacji służącej do sprawnego powiadamiania służb ratunkowych o niebezpiecznych zdarzeniach, uwzględniającej architekturę bezpiecznego systemu cyberfizycznego oraz dedykowany protokół zabezpieczający.
7. Opracowanie bezpiecznej metody komunikacji służącej do wymiany komunikatów w rozwiązaniach IoT w służbie zdrowia, uwzględniającej architekturę bezpiecznego systemu cyberfizycznego oraz dedykowany protokół zabezpieczający.

W literaturze weryfikacja protokołów bezpieczeństwa, zwłaszcza dla urządzeń sensorowych/IoT, rozwija się w trzech nurtach: podejścia symboliczne (np. ProVerif), automaty czasowe oraz oparte o modele SAT/SMT. Na tym tle praca [P5] należy do trzeciego nurtu. Habilitantka zaadaptowała model sieci komunikujących się automatów czasowych do protokołów sensorowych i sformułowała sprawdzanie dwóch klas własności: (i) poprawności przebiegów uczciwych (osiągalność stanów akceptujących) oraz (ii) podatności na ataki (osiągalność stanów końcowych przy obecności intruza i możliwość zdobycia przezeń wiedzy niezbędnej do ukończenia protokołu w danych ograniczeniach czasowych). Analiza parametrów czasowych ujawniła scenariusze ataków, co potwierdza poprawność przyjętej metody. Ponadto wykazano, że nawet przy braku pełnego ataku odpowiedni dobór parametrów pozwala na wykrywalność intruza i ograniczenie zakłóceń. Wyniki zostały opublikowane w *Sensors* [P5].

Drugie zagadnienie badawcze dotyczy weryfikacji protokołów sensorowych metodą CMMTree. Motywacją była struktura Conditional Multiway Mapped Tree umożliwiająca zdefiniowanie predykatu generującego drzewo wszystkich możliwych wykonań protokołu i identyfikacje ścieżek pozwalających na atak. Habilitantka, we współpracy z zespołem, zaprojektowała predykat oraz wprowadziła „przycinacze" optymalizujące eksplorację, która prowadzi to tego, że węzły, w których intruz nie pozyskuje wiedzy niezbędnej do przeprowadzenia lub ukończenia ataku, są pomijane. Formalizację ujęto m.in. w funkcji, która, w zależności od roli intruza, decyduje o dołączeniu kandydata do drzewa. Zastosowane przycinanie znacząco skraca czas konstrukcji drzewa i weryfikacji istnienia ataku, czyniąc CMMTree efektywną metodą dla protokołów sensorowych. Wyniki opublikowano w *Applied Sciences* [P7].

Kolejne zagadnienie dotyczy ochrony przed fałszywymi linkami/URL. W literaturze zagadnienie to opiera się na kilku uzupełniających się kierunkach: (i) umacnianiu tożsamości serwera i kanału, co ogranicza przestrzeń ataków MiTM i przekierowań; (ii) kryptograficznym „wiązaniu" treści lub żądań z adresem/pochodzeniem, a w praktyce także podpisywaniu samych linków („signed URLs") z kontrolą integralności i czasu ważności; (iii) uwierzytelnianiu odpornym na phishing (np. FIDO2); oraz (iv) filtracji/reputacji URL, co jednak nie daje dowodu autentyczności. Osiągnięcie habilitantki obejmuje specyfikację komunikacyjną architektury bezpiecznego systemu cyberfizycznego z wyodrębnionymi, zaufanymi jednostkami Distribution Center (DC) i Authentication Center (AC) oraz kanałami do użytkowników oraz schemat protokołu Amelia do weryfikacji adresów URL z użyciem funkcji haszującej. Protokół został pozytywnie zweryfikowany ze względu na potencjalne ataki z użyciem narzędzi Scyther/ProVerif/Tamarin i narzędzia autorskiego habilitantki. Zaprezentowane wyniki wskazują na przydatność „Amelii" jako warstwy nad HTTPS do weryfikowalności linków w praktycznych scenariuszach (np. spotkania online). Wstępna koncepcja była prezentowana na ETHICOMP 2021 [P13], a pełny opis opublikowany został w uznanym czasopismu *Computer Communications* [P2]. W pracach [P2] oraz [P13] habilitantka jest jedynym autorem i szczególnie prace [P2] uznaję za główne osiągnięcie w przedstawionym cyklu.

Czwarte zagadnienie dotyczy obszaru IoT dla monitoringu zanieczyszczeń powietrza. Rozwiązanie opiera się na prostych sensorach i stosach komunikacyjnych (np. MQTT), w których bezpieczeństwo transmisji bywa często pomijane. Osiągnięcie habilitantki obejmuje specyfikację komunikacyjną architektury systemu oraz dedykowany protokół zabezpieczający, wyprowadzony z Amelii i zintegrowany z MQTT. W ramach badań wykonano analizę, która potwierdziła brak skutecznych ataków, a także wykazała spełnienie własności takich jak anonimowość, wzajemne uwierzytelnienie. Zaproponowane rozwiązanie stanowi adaptację podejścia z [P2], uzupełnioną o modyfikacje wynikające ze specyfiki zastosowania protokołu. Na korzyść

przedstawionego osiągnięcia przemawia fakt, że zostało wykonane nie tylko teoretyczne opracowanie architektury i protokołów, lecz także przeprowadzono eksperymenty, które potwierdzają poprawne działanie systemu. W naukach inżynieryjno-technicznych równie istotne są rezultaty technologiczne, w tym sensie zaprezentowane testy stanowią krok w stronę dojrzałości technologii. Pierwsza koncepcja była prezentowana na BigData 2023 [P11], a pełna wersja została opublikowana w *Sensors* [P8].

Piąte osiągnięcie dotyczy komunikacji D2D w IoT. W literaturze istnieje już bogaty korpus prac nad protokołami uwierzytelniania i dystrybucji kluczy. Na tym tle osiągnięcie proponuje (i) specyfikację architektury z warstwą urządzeń i zaufanym serwerem pełniącym funkcje AAA; (ii) lekki protokół D2D do uzgadniania spotkań, który wiąże tożsamości z kontekstem. Osiągnięcie można więc ująć jako problemowo-specyficzny protokół D2D do uzgadniania spotkań, osadzony w klarownej architekturze z logiką AAA. Uważam, że konstrukcja pozostaje bliska znanym wzorcom (zaufany serwer, etapowa dystrybucja kluczy), co w pewnej mierze ogranicza oryginalność na poziomie architektury ogólnej. Ponadto silne założenie o jednym zaufanym serwerze (generowanie i przechowywanie kluczy) tworzy pojedynczy punkt zaufania/awarii. Dodatkowo, ocena bezpieczeństwa systemu ma charakter wstępny (jeden model intruza, konkretne ustawienia parametrów). Wyniki opublikowano w zbiorczej monografii *Effectiveness of ICT ethics* [P12].

Kolejne wskazane osiągnięcie dotyczy metod komunikacji w ramach rozwiązań w obszarze smart city. Istnieją różne propozycji zabezpieczania komunikacji, lecz często są one kosztowne obliczeniowo lub trudniejsze wdrożeniowo, dlatego zasadne wydaje się tworzenie lekkich, domenowo wyspecjalizowanych metod. W tym kontekście osiągnięcie opisane głównie w [P10] prezentuje architekturę z podziałem ról na urządzenia terenowe, pojazdową stację kontrolną i miejskie centrum powiadamiania, wraz z polityką bezpieczeństwa i założeniami środowiskowymi dla aglomeracji. Opracowano dedykowany protokół o sześciu fazach, w którym konsekwentnie stosuje się proste prymitywy kryptograficzne, które zapewniają poufność, integralność, wzajemne uwierzytelnianie, anonimowość a także odporność na MITM, modyfikację, replay i podszycie. Zabezpieczenia potwierdzono formalnie (BAN) oraz automatycznie w narzędziu autorstwa habilitantki. Dodatkowo, wykonano analizę nieformalną, w której wszystkie cele bezpieczeństwa zostały osiągnięte. W pracy [P3] doprecyzowano przebieg komunikacji wprowadzając dwukierunkowe potwierdzenie znaczników czasu oraz zdefiniowano pełne szyfrowanie symetryczne zdjęć oraz współrzędnych podczas kontaktu urządzenia z serwerem. Z kolei w [P14] zaufany serwer klasyfikuje obrazy metodami CNN dla oceny poziomu zagrożenia, akcentując przy tym wymogi zaufania i etyki w systemach miejskich oraz kierunki rozwoju. Wartym podkreślenia elementem osiągnięcia jest spójne połączenie lekkiej warstwy kryptograficznej z architekturą oraz wielotorową weryfikacją. To co może wpłynąć na trudności wdrożeniowe

proponowanego rozwiązania to wymóg czytnika linii papilarnych i dedykowanej aplikacji klienckiej, co zawęża spektrum obsługiwanych urządzeń. Pewną słabością osiągnięcia jest fakt, że nie zostało porównane z podobnymi rozwiązaniami w tym samym środowisku, bez bezpośrednich porównań z innymi protokołami trudno w pełni ocenić wartość systemu. Osiągnięcie zostało opublikowane w trzech pracach, ale głównie wyniki zostały zaprezentowane w samodzielnej pracy habilitantki w uznanym czasopiśmie *Pervasive and Mobile Computing* [P10].

Siódme osiągnięcie dotyczy rozwiązania IoT dla ochrony zdrowia, w ramach którego habilitantka proponuje specyfikację architektury z wyraźnym podziałem ról i logiką AAA, oraz dedykowany protokół obejmujący pięć faz. Ocena bezpieczeństwa jest wykonana według wcześniej stosowanego schematu, czyli analiza formalna (logika BAN), automatyczna z analizą czasową oraz nieformalna, we wszystkich przypadkach potwierdzono realizację określonych usług bezpieczeństwa. Podobnie jak we wcześniejszych rozwiązaniach habilitantka przyjmuje model z jednym zaufanym serwerem tworzącym pojedynczy punkt zaufania/awarii, co wymaga doprecyzowania procedur rotacji kluczy i wysokiej dostępności. Wyniki zostały opublikowane w samodzielnej pracy habilitanki w czasopiśmie z IF, *Bulletin of the Polish Academy of Sciences Technical Sciences* [P9].

W świetle przedstawionych osiągnięć widać, że kolejne protokoły opierają się na podobnym szkielecie projektowym: centralnej jednostce zaufania, lekkich prymitywach kryptograficznych oraz etapowym przebiegu a różnicę stanowi głównie kontekst domenowy i sposób powiązania tożsamości z usługą. Na plus przemawia spójność i przenośność schematu, niska złożoność wdrożeniowa wynikająca z użycia prostych modułów kryptograficznych i faz „dwupodmiotowych". Warto również podkreślić konsekwentną, metodyczną walidację, co daje porównywalność wyników i wzmacnia gotowość do prototypowania. Z drugiej strony, nowość jest w dużej mierze aplikacyjna, a w tylko w pewnym stopniu dotyczy elementów kryptograficznych. Utrzymuje się ten sam model zaufania z pojedynczym punktem zaufania/awarii, który wymaga zagwarantowania mechanizmów wysokiej dostępności. W niektórych wariantach dochodzą wymogi sprzętowo-użytkowe, które zawężają adopcję.

Myślę, że przedstawione osiągnięcia mają w dużej części charakter projektowo-technologiczny, zawierają obok modelu teoretycznego specyfikację architektury i protokołów gotowych do implementacji. Dodatkowo, zawierają wyniki eksperymentów i symulacji, które potwierdzają wykonalność technologii w warunkach laboratoryjnych (TRL 4), co przekłada się na realny potencjał wdrożeniowy. W mojej ocenie w naukach inżynieryjno-technicznych ważne jest tworzenie rozwiązań o rzeczywistym potencjale wdrożeniowym, czyli takich, które mogą stać się technologiami używanymi społecznie i współtworzyć fundament krajowych technologii.

Biorąc pod uwagę powyższe, uważam, że przedstawione osiągnięcie spełnia wymogi stawiane w procesie habilitacyjnym.

3. Ocena dorobku naukowego

Doktor inżynier Sabina Szymoniak uzyskała w roku 2012 tytuł magistra inżyniera na kierunku Informatyka na Wydziale Inżynierii Mechanicznej i Informatyki, Politechniki Częstochowskiej. W roku 2017 obroniła doktorat w dyscyplinie informatyka techniczna i telekomunikacja na Politechnice Częstochowskiej.

W bazie WoS indeksowanych jest 24 publikacji habilitantki, w Scopus 34, w Goole Scholar 56 prac. Indeks Hirsha wg.: WoS - 6, Scopus – 8, Google Scholar – 10. Liczba cytowań
wg.: WoS – 89 (bez autocytowań – 49), Scopus – 167 (bez autocytowań – 96), Google Scholar – 271 (bez autocytowań – 143).

W dorobku warto szczególnie odnotować publikację w ACM Computing Surveys: „*Key Distribution and Authentication Protocols in Wireless Sensor Networks: A Survey*”. Jest to sygnał rozpoznawalności i jakości, ale należy podkreślić, że jest to artykuł przeglądowy. Takie artykuły są bardzo cenne z punktu widzenia syntezy stanu wiedzy, lecz jest z natury inny niż prace wnoszące oryginalne wyniki badawcze.

Warto zwrócić uwagę na wysoki sumaryczny 5-letni współczynnik wpływu opublikowanych prac habilitantki, który wynosi wg.: WoS – 57,105; Scopus – 58,32; Google Scholar – 58,32. Według mnie jest to poziom bardzo dobry na tym etapie rozwoju naukowego i wskazuje na uznany wkład opublikowanych prac habilitantki do dziedziny.

Habilitantka w dniach 4.09-1.10.2024 odbyła jeden staż naukowy na Uniwersytecie Kardynała Stefana Wyszyńskiego w Warszawie, gdzie prowadziła badania związane z działaniem wybranych protokołów zabezpieczających dedykowanych środowiskom Internetu Rzeczy. Uzyskane wyniki były podstawą do pracy *Defense and Security Mechanisms in the Internet of Things: a Review*, która obecnie została opublikowana w czasopiśmie *Applied Science*. Wartym zauważenia jest współpraca z zespołem badawczym pod kierunkiem prof. Shalini Kesar z Southern Utah University. Efektem tej współpracy są 4 artykuły w obszarze IoT.

Habilitantka uczestniczyła jako wykonawczyni w 2 projektach badawczo-rozwojowych finansowanych w drodze konkursów krajowych lub zagranicznych. Pierwszy dotyczył *prac badawczo-rozwojowych prowadzących do opracowania innowacyjnych algorytmów uczenia maszynowego (machine learning) dostosowanych do specyfiki internetowej platformy handlowej Clemens.pl*. Drugi projekt to Krajowy Magazyn Danych, który dotyczył *uniwersalnej infrastruktury dla składowania i udostępniania*

danych oraz efektywnego przetwarzania dużych wolumenów danych w modelach HPC, BigData i sztucznej inteligencji, który współfinansowany był ze środków Europejskiego Funduszu Rozwoju Regionalnego. Na obecnym etapie kariery liczba projektów, w których habilitantka brała udział, jest niższa od powszechnie spotykanej wartości.

W dorobku konferencyjnym od czasu doktoratu odnotowano 16 referatów (oraz 4 sprzed doktoratu), z przewagą wystąpień na konferencjach międzynarodowych, co potwierdza aktywność i umiędzynarodowienie wyników. Niemniej jednak w zestawieniu brakuje prezentacji na konferencjach z listy CORE klasy A/B, a większość wystąpień przypadła na konferencje kategorii C.

Podsumowując, dorobek naukowy Habilitantki, mimo wskazanych obszarów wymagających dalszego wzmocnienia, oceniam jako wystarczający i spełniający kryteria przewodu habilitacyjnego.

4. Ocena dorobku dydaktycznego i popularyzatorskiego

Doktor inżynier Sabina Szymoniak posiada osiągnięcia w zakresie dydaktycznym, wśród nich można wymienić funkcje opiekuna zakresu Cyberbezpieczeństwo realizowanego w ramach studiów II stopnia na kierunku Informatyka oraz opiekuna Studenckiego Koła naukowego Cyberhydra. Warto dodać, że w latach 2024-2028 pełniła również rolę członka Rady Programowej w dyscyplinie Informatyka techniczna i telekomunikacja.

W latach 2018-2024 prowadziła 7 przedmiotów na studiach I i II stopnia: Bezpieczeństwo systemów komputerowych, Bezpieczeństwo aplikacji internetowych, Techniki pozyskiwania informacji, Wykrywanie i analizowanie zagrożeń oraz reagowanie na incydenty naruszające bezpieczeństwo, Incydenty naruszające bezpieczeństwo, Audyt bezpieczeństwa, Bezpieczeństwo sieci komputerowych.

Istotnym aspektem działalności akademickiej habilitantki jest zaangażowanie w opiekę nad pracami dyplomowymi na poziomie magisterskim i inżynierskim. Doktor inżynier Sabina Szymoniak była promotorką 19 prac magisterskich oraz 22 inżynierskich (lata 2018-2024). Efektem wysokiej jakości współpraca ze studentami jest współautorstwo ośmiu publikacji o zasięgu krajowym i międzynarodowy, które powstały z udziałem studentów i doktorantów.

Habilitantka angażuje się również w popularyzację nauki, przeprowadziła cykl szkoleń dotyczących baz danych na UKSW; prowadziła w latach 2019-2024 zajęcia dotyczące związane z Cyberbezpieczeństwem dla szkół średnich; organizowała w latach 2023-2024 Cybersecurity Day na Politechnice Częstochowskiej.

Doktor inżynier Sabina Szymoniak pełniła również funkcję członka komitetów naukowych (ETHICOMP 2021, 2024, 2025; Informatics 2024; FedCSIS 2024) oraz organizacyjnych ETHICOMP (2022-2025) konferencji naukowych.

Habilitantka przygotowała kilkanaście recenzji dla międzynarodowych czasopism i konferencji naukowych, co potwierdza jej zaangażowanie w prace środowiska. Należy jednak zaznaczyć, że były to w większości tytuły i konferencje nienależące do czołowych miejsc publikacyjnych w danej dziedzinie.

Oceniam działalność dydaktyczną i popularyzatorską habilitantki jako wystarczającą, świadczy ona o udziale w życiu społeczności naukowej oraz o zaangażowaniu we wspieranie młodej kadry akademickiej.

5. Konkluzja końcowa

Biorąc pod uwagę osiągnięcia związane z przedstawionym cyklem publikacji oraz dorobkiem naukowym, stwierdzam, że wymagania określone w art. 219 ust. 1 pkt. 2 i 3 ustawy „Prawo o szkolnictwie wyższym i nauce" zostały spełnione i wnioskuję o dopuszczenie doktora inżyniera Sabiny Szymoniak do dalszych etapów postępowania habilitacyjnego w dyscyplinie informatyka techniczna i telekomunikacja w dziedzinie nauk inżynieryjno-technicznych.

dr hab. Bogdan Księżopolski