dr hab. inż. **Marcin Niemiec**, prof. AGH
Instytut Telekomunikacji
Wydział Informatyki, Elektroniki i Telekomunikacji
Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie
al. Mickiewicza 30
30-059 Kraków
tel. 12 617 48 03
niemiec@agh.edu.pl

Kraków, 28.05.2025

RECENZJA ROZPRAWY DOKTORSKIEJ DLA RADY NAUKOWEJ DYSCYPLINY INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA POLITECHNIKI WARSZAWSKIEJ

Tytuł rozprawy: Development of a Risk-based Security Framework for Mobile Networks Interconnection Applied in Roaming Service Level Agreements within the 5G Context

Autor rozprawy: mgr inż. German Peinado Gomez

1. Jakie zagadnienie naukowe jest rozpatrzone w pracy /teza rozprawy/ i czy zostało dostatecznie jasno sformułowane przez Autora? Jaki charakter ma rozprawa (teoretyczny, doświadczalny, inny)?

Rozprawa doktorska dotyczy problematyki bezpieczeństwa w połączeniach pomiędzy sieciami komórkowymi. Operatorzy sieci zawierają umowy o gwarantowanym poziomie świadczonych usług w celu zapewnienia roamingu. Jednak bezpieczeństwo takich połączeń jest ciągle aktualnym wyzwaniem, bez względu na generację sieci komórkowej (2G/3G, 4G czy 5G). W szczególności istnieje potrzeba opracowania mechanizmów umożliwiających dynamiczną reakcję i adaptację odpowiednich rozwiązań bezpieczeństwa do bieżących warunków w łączu.

W celu zwiększenia bezpieczeństwa połączeń międzyoperatorskich, Autor rozprawy zaproponował podejście bazujące na szacowaniu ryzyka związanego z obsługiwanym ruchem. Postawiono tezę, iż zaufanie między operatorami połączonych sieci komórkowych powinno być oceniane poprzez ciągłą weryfikację poziomu ryzyka w łączach sygnalizacyjnych połączeń międzyoperatorskich, obejmując współistniejące obecnie technologie w sieciach mobilnych, tj. SS7 (2G/3G), Diameter (4G) oraz HTTP/2 (5G). Poza tym, oszacowany poziom ryzyka może posłużyć do dalszych działań w celu zwiększenia efektywności czy bezpieczeństwa. Podejście bazujące na zastosowaniu zdefiniowanych uprzednio profili bezpieczeństwa może spowodować bardziej efektywne ustalanie parametrów bezpieczeństwa charakteryzujące dane łącze, w porównaniu do podejścia z dynamiczną negocjacją takich parametrów. Z kolei wiedza na temat bieżącego poziomu ryzyka w łączu międzyoperatorskim może być wykorzystana do dynamicznego utworzenia i egzekwowania adekwatnej polityki bezpieczeństwa.

Tak przedstawione zagadnienie naukowe zostało dostatecznie jasno sformułowane przez Autora oraz przedstawia ważne i aktualne zagadnienie badawcze we współczesnej telekomunikacji. Rozprawa ma głównie charakter teoretyczny (opis koncepcji), choć praktyczny aspekt badań potwierdzają przeprowadzone przez Autora działania standaryzacyjne.

2. **Czy w rozprawie przeprowadzono w sposób właściwy analizę źródeł / w tym literatury światowej, stanu wiedzy i zastosowań w przemyśle/ świadczący o dostatecznej wiedzy Autora? Czy wnioski z przeglądu źródeł sformułowano w sposób jasny i przekonywujący?**

Wprowadzenie do tematyki bezpieczeństwa połączonych sieci komórkowych znajduje się w drugim rozdziale rozprawy. Ta część szczegółowo opisuje podejścia do ochrony łączy międzyoperatorskich dla kolejnych generacji: sieci 2G/3G (głównie bazujące na zaporach sieciowych), 4G (protokół Diameter) oraz architekturze bezpieczeństwa dla sieci 5G. Rozwiązania te zostały opisane szczegółowo, co potwierdza dużą wiedzę Autora w tematyce rozprawy doktorskiej. Prawdopodobnie dlatego w tekście zdarzają się pewne określenia nieformalne/kolokwialne, stosowane raczej w środowisku firmowym niż akademickim, np. "*firewalling functionalities*", "*down to the bit level*", "*something digestible*" czy "*ZTA lingo*", a także nazewnictwo typu: „*confidentiality and integrity protected*" czy „*end-to-end integrated protected*". Aby dopełnić tą część, warto byłoby dokładnie wyjaśnić schematy na rysunkach przedstawiających architekturę bezpieczeństwa różnych generacji sieci komórkowych, np. rysunek 2.1.2-1 (generacja 4G) czy rysunek 2.3-1 (generacja 5G).

Wspomniany rozdział 2 rozprawy zawiera także istotną część analizy literaturowej bezpośrednio związanej z tematyką rozprawy. Pozostałe części analizy znajdują się w innych miejscach – głownie w rozdziale 4 („*4.2.3.1 Streaming data preprocessing*" czy „*4.2.3.2 Data mining*") oraz w końcowej części opisującej możliwe kierunki dalszych badań. Wprawdzie poruszana tematyka jest obecnie intensywnie rozwijana i można byłoby odwołać się do większej liczby prac, ale przedstawiona analiza źródeł jest wystarczająca. Przeprowadzono ją w sposób właściwy, a wnioski sformułowane na jej podstawie są jasne i przekonywujące. Umiejscawia to rozprawę na tle innych badań w dziedzinie oraz właściwie identyfikuje problem badawczy. Autor w bibliografii zamieścił również 9 własnych prac związanych z tematem swojej rozprawy doktorskiej (prace opublikowane w ciągu ostatnich sześciu lat), w tym uzyskane patenty.

3. **Czy Autor rozwiązał postawione zagadnienia, czy użył właściwej do tego metody i czy przyjęte założenia są właściwe?**

Postawione zagadnienie badawcze zostało rozwiązane przez Autora rozprawy. Zaproponowany został autorski model/struktura bezpieczeństwa dla łączy międzyoperatorskich w sieciach komórkowych. Składa się on z kilku elementów, wśród których kluczowym jest pierwszy – odpowiedzialny za analizę bezpieczeństwa ruchu sygnalizacyjnego w takim łączu i na podstawie szczegółowej weryfikacji poszczególnych wiadomości oraz całych sekwencji danych szacujący poziom ryzyka. Kolejne elementy modelu – na podstawie przeprowadzonej analizy bezpieczeństwa i oszacowanym ryzyku – są w stanie określić poziom zaufania do poszczególnych jednostek w sieci, wybrać adekwatny profil bezpieczeństwa by ułatwić negocjacje parametrów bezpieczeństwa, a także dynamicznie ustalić i egzekwować odpowiednie polityki bezpieczeństwa. Autor założył, że model ma być możliwy do zastosowania w różnych generacjach sieci komórkowych. Metody badawcze wybrano właściwie, a formalny opis modelu oraz analiza przykładowych scenariuszy w większości potwierdzają, że autorski mechanizm stanowi rozwiązanie postawionego zagadnienia. Jednak zarówno formalny opis jak i weryfikacja modelu zawierają pewne nieścisłości, które zostały opisane poniżej.

W rozprawie najlepiej opisany został pierwszy element autorskiego modelu bezpieczeństwa, odpowiedzialny za szacowanie ryzyka. Jednak formalny zapis zawiera pewne niejednoznaczności (np. z opisu na str. 47 wynika, że atrybut może być formalnie reprezentowany zarówno przez $A^{(j)}$ jak i samo j) czy kolizje oznaczeń (np. symbol małej delty został użyty zarówno jako tzw. „*risk factor*" jak i "*desired probability level*". Poza tym, w rozdziale 4 ryzyko jest rozważane dość niekonsekwentnie w poszczególnych fragmentach – od bardzo ogólnego, poprzez zgrubne szacowanie (np. wysokie czy niskie ryzyko), po dokładną liczbową

wartość współczynnika ryzyka. Zaskakuje także niejednorodność opisu poszczególnych elementów modelu bezpieczeństwa. Niektóre zostały zaprezentowane bardzo ogólnikowo, bez formalnego opisu, np. eksploracja danych, gdzie na końcu znajduje się wprost zalecenie: „*Future implementers are kindly invited to test those and other similar algorithms, and accordingly select the most suitable for their environments*". Z drugiej strony, np. na str. 48 znajduje się bardzo dokładny opis trzech różnych model strumieni danych, które w późniejszych rozdziałach nie są wprost używane (a tym bardziej nie wiadomo dlaczego są tam rozpatrywane bardzo specyficzne warunki, jak choćby założenie że $F_t[j'] = F_{t-1}[j']$ dla wszystkich $j' \neq j$). W przypadku weryfikacji zaproponowanego modelu bezpieczeństwa, pewien niedosyt pozostawia brak implementacji modelu (lub jego kluczowych elementów) oraz przeprowadzenie kompleksowej weryfikacji funkcjonalnej. Po części jest to spowodowane brakiem dostępu do rzeczywistego ruchu, ale nawet bazując na posiadanych próbkach ruchu, można byłoby przeprowadzić ocenę działania choćby poszczególnych elementów modelu. Zamiast tego Autor zdecydował się na przedstawienie kilku przykładowych i raczej prostych scenariuszy użycia.

Pomimo wspomnianych niedoskonałości zastosowanych metod badawczych, ostatecznie Autor potwierdził, że można zaprojektować model bezpieczeństwa, dzięki któremu zaufanie między operatorami połączonych sieci komórkowych będzie oceniane poprzez ciągłą weryfikację poziomu ryzyka w łączach międzyoperatorskich. Z kolei podejście bazujące na zastosowaniu zdefiniowanych uprzednio profili bezpieczeństwa może spowodować bardziej efektywne ustalenie parametrów bezpieczeństwa danego połączenia, w porównaniu do podejścia z dynamiczną negocjacją takich parametrów. Ostatecznie wiedza na temat aktualnego poziomu ryzyka może być wykorzystana do dynamicznego utworzenia i egzekwowania adekwatnej polityki bezpieczeństwa dla ruchu w łączu międzyoperatorskim. Dla ścisłości należy wspomnieć, że tezy są postawione dość radykalnie i według recenzenta zamiast określeń „*needs to*" czy „*should*" raczej powinny sugerować, że mechanizmy zaproponowane w rozprawie mogą rozwiązać pewne problemy z bezpieczeństwem czy wydajnością (nie wykazano jednoznacznie, że zaproponowane podejścia są najlepsze). Jednak opracowany model z pewnością pomaga zwiększyć poziom bezpieczeństwa połączeń pomiędzy sieciami komórkowym.

4. Na czym polega oryginalność rozprawy, co stanowi samodzielny i oryginalny dorobek Autora, jaka jest pozycja rozprawy w stosunku do stanu wiedzy czy poziomu techniki reprezentowanych przez literaturę światową?

Oryginalny dorobek opisany w rozprawie doktorskiej dotyczy przede wszystkim opracowania kompletnego modelu/struktury bezpieczeństwa dla łączy międzyoperatorskich w sieciach komórkowych. Oryginalny dorobek bardzo dobrze podsumowuje rozdział 3, a szczególnie rysunek 3.2-1, na którym nie tylko zaprezentowano poszczególne elementy modelu, ale także zwizualizowano w jaki sposób są od siebie zależne (Autor wspomniał o podejściu, gdzie działanie elementów składowych modelu można potraktować jako kompleksowy cykl życia zabezpieczeń). Samodzielny wkład Autora rozprawy jest istotny oraz oryginalny w stosunku do stanu wiedzy i poziomu techniki. Szkoda tylko, że w rozprawie brak informacji jaki jest autorski wkład we wspólne prace z innymi współautorami (np. patenty), na które powołuje się Autor, np. „*Our patented solution [11] provides...*". Recenzent wyodrębnił najważniejsze oryginalne elementów rozprawy, które zostały krótko podsumowane poniżej.

- Autor rozprawy zaproponował formalny schemat analizy poszczególnych wiadomości w łączu międzyoperatorskim, w skład którego wchodzi kilka kryteriów oceny (np. źródło pochodzenia wiadomości, protokół, itd.), a także schemat analizy całych sekwencji wiadomości, gdyż na ich podstawie można uzyskać dodatkową wiedzę, niedostępną w procesie analizy jedynie pojedynczych wiadomości w łączu międzyoperatorskim.

- Na podstawie wyników analizy wiadomości oraz sekwencji wiadomości, zaproponowana została metoda szacowania ryzyka w sposób ilościowy. Sposób określenia

poszczególnych wartości bazuje na podejściu CVSS (*Common Vulnerability Scoring System*). Według recenzenta, szczególnie interesujące są dwa współczynniki: „*Data Sensitivity (DS)*" oraz „*Potential Impacts of the Vulnerability (PIV)*" oraz wyliczony na ich podstawie współczynnik CF_i. Na uwagę zasługuje także sposób wyliczenia współczynnika ryzyka oraz próba skorygowania liczbowej wartości ryzyka dla niektórych zdarzeń/podatności.

- Zaproponowana została koncepcja wykorzystania oszacowanego ryzyka do takich celów jak: określenie poziomu zaufania do poszczególnych jednostek w sieci, wybór adekwatnego profilu bezpieczeństwa w celu ułatwienia negocjacji parametrów bezpieczeństwa dla połączenia czy dynamiczne ustalanie i egzekwowanie odpowiednich polityk bezpieczeństwa.

- Przeanalizowano sposób działania wybranych mechanizmów w przykładowych scenariuszach, przede wszystkim przedstawiono oszacowanie ryzyka w teoretycznym scenariuszu ze śledzeniem lokalizacji oraz bardziej praktycznym, w którym zaprezentowano wyniki badań bazujących na rzeczywistym ruchu międzyoperatorskim. Przedstawiono także przykłady (wysokopoziomowe, bez szczegółów) związane z profilami ochrony danych oraz ustaleniem nowej polityki bezpieczeństwa.

5. Czy Autor wykazał umiejętność poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników /zwięzłość, jasność, poprawność redakcyjna rozprawy/?

Autor wykazał umiejętność poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników, ale poziom językowy i edycyjny rozprawy niestety nie jest najwyższy. W tekście można znaleźć wiele błędów językowych, ale na szczęście w większości nie wpływają one negatywnie na zrozumienie zawartości merytorycznej pracy. Autor niepotrzebnie zapisuje niektóre nazwy stosując dużą literę w środku zdania (np. „*field of Security*"), często robiąc to zupełnie niekonsekwentnie (np. „*in the core network*", „*in the Core Network*", „*of the Core networks*"). Zapis nazwy protokołu bywa różny: „Diameter" oraz „diameter". Niekonsekwentny (a czasami błędny pod względem jezykowym) jest również zapis w przypadku odnośników do rozdziałów (np. „*in Sections 3-7*", „*section 4.2.2*", „*in Chapter 4*", „*in chapter 6*" „*subchapter 6.2*", „*the subchapter 8.2*". Podobnie brak jest konsekwencji w zapisie zmiennych: „the $_t$th item", „the $i-_t h$ signalling message" lub bez kursywy „the ith transaction". Opisując nowe rozwiązania, Autor stosuje czasem formę zdań w pierwszej osobie liczby pojedynczej („*I highlight...*") a czasem mnogiej („*we highlight...*"). W pracy występują jednozdaniowe akapity czy zdania niepoprawne językowo (np. brak orzeczenia w zdaniu „*Diameter message manipulation, Attribute Value Pair (AVP) doubling.*"). Częste są także problemy z interpunkcją, (np. poprzez zastosowanie dwukropka tabela na str. 56 jest potraktowana jak część zdania).

Strona edytorska dokumentu powinna być bardziej staranna. W rozprawie zdarzają się mało czytelne rysunki (np. bardzo mała czcionka na rysunku 4.2.2-1) czy brak opisu poszczególnych kroków na rysunkach 7.2.2-1 oraz 8.2-2. Rysunki i tabele występują w różnych stylach. Niekonsekwentna jest także edycja dokumentu jako całości, np. czasem rozdziały drugiego poziomu są rozpoczynane od nowej strony (np. pusta połowa strony przed rozdziałem 6.3), a czasem nie (np. wcześniejszy podrozdział 6.2). Pewne zamieszanie wprowadzają cytowania rysunków i tabel wraz z oryginalnymi oznaczeniami w rozdziale 8.4. Brak konsekwencji w zapisie tytułów rysunków (czasem wyrazy są pisane małą, a czasem dużą) i w tytułach tabel (np. tabela 8.2-1 ma tytuł pisany dużymi literami). W spisie skrótów niepotrzebnie niektóre skróty są pisane kursywą. Również zapis poszczególnych pozycji w bibliografii powinien być lepiej zredagowany, np. brak daty dostępu w przypadku linków internetowych, niektóre pozycje to tylko link bez żadnych innych informacji (np. [35]), czasem brak dokładnej daty wydania (np. kiedy odbyło się wydarzenie [60] czy na którą wersję publikacji [63] powołuje się Autor).

Wspomniane problemy w pewnym stopniu obniżają jakość pracy, ale należy podkreślić, że tekst nie zawiera poważnych błędów merytorycznych. Nawet podczas uważnego czytania rozprawy można znaleźć jedynie kilka drobnych błędów tego rodzaju, które jednak można potraktować jako niezamierzone literówki, a nie błędy merytoryczne, np. na rysunku 3.1-1 zamiast nazwy „N" powinno być „N32", na rysunku 4.2.2-1 jest literówka „*roamin-in*", na str. 53 zamiast „(0 ... 0 1 1 0 0)" w podanym przykładzie powinien być zapis „(0 0 1 1 0 0)", czy drobny błąd w oznaczeniu "*as indicated in subchapter 3.3*" (prawdopodobnie Autor chciał wskazać na rozdział 4.3). Zatem podsumowując – rozprawa została napisana językiem zrozumiałym, a wspomniane problemy nie zmieniają ogólnej pozytywnej oceny rozprawy.

6. Jakie są słabe strony rozprawy i jej główne wady?

O pewnych słabych stronach rozprawy (np. niejednoznaczności w formalnym opisie, błędy językowe czy niedoskonałości związane ze strukturą rozprawy i stroną edytorską) wspomniano już w poprzednich punktach. Poniżej przedstawione zostały uwagi merytoryczne, które według recenzenta są kluczowe dla ocenianej rozprawy doktorskiej.

- Aby określić poziom ryzyka w sposób ilościowy, Autor używa podejścia bazującego na CVSS. Jednak CVSS określa w sposób liczbowy wagę danej podatności, a nie miarę ryzyka związanego z konkretnym zdarzeniem. Choć ryzyko jest pojęciem trudnym do zdefiniowania w sposób całkowicie jednoznaczny, zwykle szacowane jest na podstawie prawdopodobieństwa wystąpienia oraz wpływu danego zdarzenia na rozpatrywany system. Z tego względu w rozprawie niejasne jest przejście od oszacowania wagi podatności przy użyciu CVSS do wartości współczynnika ryzyka. Również sam formalny opis nie pomaga w określeniu ostatecznego algorytmu ustalania tej wartości, gdyż niejasne jest co się dzieje z wartością R_i (jak wpływa ona na końcową wartość ryzyka czy jaka relacja występuje pomiędzy R_i oraz *Overall Score*), a także dlaczego Autor zakłada akurat proste mnożenie wartości $CVSS_i$ i CF_i.
  Dodatkowo, w rozprawie brakuje także umotywowania decyzji Autora co do wyboru niektórych wartości w tabeli 4.3-1 (przede wszystkim tych w kolumnie *Corrected*) czy co do danych branych pod uwagę w analizie statystycznej sekwencji wiadomości sygnalizacyjnych. Bez wyjaśnienia powodów, podjęte decyzje wydają się mocno arbitralne (jako przykład można zacytować fragment: „*this dissertation considers just what I judge as the most important one in the proposed security analysis*".

- Rozpatrując drugi element zaproponowanego modelu bezpieczeństwa, pewien niedosyt sprawia brak formalnego opisu jak przejść od oszacowanego poziomu ryzyka (pierwszy element modelu) do zaufania do pojedynczej jednostki, które będzie określone w sposób ilościowy (tzw. „*transforming the measurement of the risk into a trust score*").

- Element trzeci modułu bezpieczeństwa zakłada zastosowanie wcześniej zdefiniowanych profili bezpieczeństwa, zawierających określone zestawy parametrów bezpieczeństwa. Zamiast negocjować poszczególne parametry, zakładamy wybór odpowiedniego profilu. Jednak założono, że profile te są odpowiednio uszeregowane, tak aby obie strony transmisji mogły wybrać najbardziej odpowiedni zestaw. Pojawia się zatem pytanie czym się różni takie podejście (a jeśli tak to na ile jest to istotna różnica) od typowej negocjacji parametrów, jaką można spotkać w rozwiązaniach typu IKE (*Internet Key Exchange*) i SA (*Security Association*) czy w protokole TLS (*Transport Layer Security*).

- Słabą stroną rozprawy jest brak obiektywnej oceny zaproponowanego modelu bezpieczeństwa. W zasadzie wyniki zaprezentowane w rozdziale 8 nie są walidacją czy weryfikacją funkcjonalną modelu lub jego poszczególnych elementów, ale stanowią prezentację przykładowych scenariuszy użycia. Jeden scenariusz jest mocno teoretyczny, a jedynie drugi bazuje na danych rzeczywistych. Brak jest prawdziwej

implementacji modelu bezpieczeństwa, a następnie jego weryfikacji funkcjonalnej, badań poszczególnych scenariuszy w różnych środowiskach, dogłębnej analizy czy słusznie wybrano poszczególne wartości ryzyka, badań nad dostosowaniem progów na podstawie danych rzeczywistych, do których miał dostęp Autor, itd. Poza tym niektóre z fragmentów rozdziału 8 nie są związane z testowaniem opracowanych rozwiązań (np. rozdział 8.3 nie tylko nie jest walidacją rozwiązania, ale także nie jest scenariuszem użycia, więc raczej powinien być częścią rozdziału 5).

7. Jaka jest przydatność rozprawy dla nauk technicznych?

Recenzent wysoko ocenia przydatność ocenianej rozprawy doktorskiej dla nauk technicznych. Rozprawa dotyczy aktualnego i ważnego problemu z zakresu telekomunikacji i bezpieczeństwa: jak zapewnić wysoki poziom bezpieczeństwa połączeń pomiędzy sieciami komórkowymi różnych operatorów. Autor zaproponował uniwersalne podejście (z punktu widzenia połączeń sieci komórkowych różnych generacji) bazujące na dynamicznym szacowaniu ryzyka związanego z ruchem międzyoperatorskim – zarówno związanym z pojedynczymi wiadomościami sygnalizacyjnymi jak i strumieniami danych. Co istotne – ryzyko w takim podejściu jest szacowane w sposób ilościowy, co pozwala np. na ustalanie akceptowanych progów ryzyka czy szacowaniu poziomu zaufania do jednostek. Dodatkowo – propozycja ściśle zdefiniowanych i uszeregowanych profili bezpieczeństwa może poprawić efektywność ustalania parametrów bezpieczeństwa danego łącza, a stała kontrola bezpieczeństwa w łączu międzyoperatorskim może być wykorzystana do dynamicznego tworzenia i egzekwowania adekwatnej polityki bezpieczeństwa. Oba te podejścia są przedmiotem prac standaryzacyjnych i patentów przyznanych w ciągu ostatnich kilku miesięcy, co dodatkowo potwierdza użyteczność wyników rozprawy dla nauk technicznych.

8. Konkluzja – do której z następujących kategorii Recenzent zalicza rozprawę:

a) niespełniająca wymagań stawianych rozprawom przez obowiązujące przepisy
b) wymagająca wprowadzenia poprawek i ponownego recenzowania
c) <u>spełniająca wymagania</u>
d) spełniająca wymagania z wyraźnym nadmiarem
e) wybitnie dobra, zasługująca na wyróżnienie

9. Uzasadnienie

Biorąc po uwagę wszystkie wspomniane aspekty rozprawy doktorskiej, moja końcowa konkluzja jest jednoznacznie pozytywna. Autor zaprezentował w rozprawie ogólną wiedzę teoretyczną w dyscyplinie i przedstawił oryginalne rozwiązanie problemu naukowego. Zaproponował nowy model/strukturę bezpieczeństwa, dzięki której możliwe jest oszacowanie ryzyka związanego z ruchem w łączach międzyoperatorskich, a następnie określenie poziomu zaufania do poszczególnych jednostek w sieci, wybór adekwatnego profilu bezpieczeństwa w celu ułatwienia negocjacji parametrów bezpieczeństwa czy dynamiczne ustalanie i egzekwowanie odpowiednich polityk bezpieczeństwa. Tym samym Autor rozprawy potwierdził umiejętność samodzielnego prowadzenia pracy naukowej.

Podsumowując stwierdzam, że rozprawa doktorska spełnia wymagania *Ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce* oraz wnioskuję o dopuszczenie Pana mgr. inż. Germana Peinado Gomeza do dalszych etapów przewodu doktorskiego.