Dr hab. inż. Grzegorz Borowik Warszawa, dnia 17 listopada 2025 r.

Recenzja rozprawy doktorskiej

pt. *Pakiet testów losowości do badania prymitywów kryptograficznych*

w dziedzinie nauk inżynieryjno-technicznych,
w dyscyplinie **informatyka techniczna i telekomunikacja**

Autor rozprawy: mgr inż. Krzysztof Mańk
Promotor: dr hab. Marek Kojdecki, prof. WAT
Promotor pomocniczy: dr inż. Michał Wroński

Niniejsza recenzja pracy doktorskiej została sporządzona w odpowiedzi na pismo z dnia 13 maja 2025 r., otrzymane od dr. hab. inż. Zbigniewa Tarapaty, prof. WAT, Przewodniczącego Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja przy Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego w Warszawie. Przedmiotowa rozprawa doktorska została przygotowana pod kierunkiem dr. hab. Marka Kojdeckiego, prof. WAT. Praca została przedłożona Radzie Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja Wojskowej Akademii Technicznej. Na podstawie art. 192 ust. 1 ustawy z dnia 20 lipca 2018 r. *Prawo o szkolnictwie wyższym i nauce* (Dz. U. z 2023 r. poz. 742 z późn. zm.), § 25 ust. 1 pkt 1 Statutu WAT (załącznik do uchwały Senatu WAT nr 16/WAT/2019 z dnia 25 kwietnia 2019 r.) oraz § 6 ust. 3–5 *Sposobu postępowania w sprawie nadania stopnia naukowego w Wojskowej Akademii Technicznej* (załącznik do uchwały Senatu WAT nr 99/WAT/2021 z dnia 21 grudnia 2021 r. z późn. zm.), Rada Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja WAT podjęła uchwałę nr 65/RDN ITiT/2025 o delegowaniu mi zadania wykonania recenzji tej pracy, w dziedzinie nauk inżynieryjno-technicznych, dyscyplinie informatyka techniczna i telekomunikacja.

Dokonując oceny rozprawy doktorskiej mgr. inż. Krzysztofa Mańka, uwzględniłem obligatoryjne wymogi formalnoprawne determinowane przepisami ustawy *Prawo o szkolnictwie wyższym i nauce*. Zgodnie z art. 187 tej ustawy rozprawa doktorska powinna prezentować ogólną wiedzę teoretyczną kandydata w dyscyplinie albo dyscyplinach oraz umiejętność samodzielnego prowadzenia pracy naukowej lub artystycznej. Natomiast przedmiotem rozprawy doktorskiej powinno być oryginalne rozwiązanie problemu naukowego, oryginalne rozwiązanie w zakresie zastosowania wyników własnych badań naukowych w sferze gospodarczej lub społecznej albo oryginalne dokonanie artystyczne.

W trakcie recenzji, weryfikując spełnienie wymagań formalnych i merytorycznych, dokonałem szczegółowej oceny następujących aspektów: doboru problematyki badawczej i tematu rozprawy, sformułowania celu i hipotez badawczych, poprawności i adekwatności zastosowanych metod, kompletności oraz przejrzystości treści i struktury pracy (w tym zgodności z kanonem prac doktorskich w dyscyplinie), jak również zakresu oryginalności i znaczenia uzyskanych wyników. Ocena merytoryczna oraz formalna została przeprowadzona na podstawie wiedzy specjalistycznej oraz dostępnych publikacji, a także analizy samej rozprawy wraz z materiałami uzupełniającymi.

Jaki jest problem naukowy (teza) rozprawy i czy został on trafnie i jasno sformułowany?

W rozprawie doktorskiej mgr. inż. Krzysztofa Mańka pt. *„Pakiet testów losowości do badania prymitywów kryptograficznych"* autor podejmuje tematykę oceny jakości losowości generowanej przez prymitywy kryptograficzne, w szczególności przez generatory liczb pseudolosowych. We wprowadzeniu (s. 19) autor podkreśla, że *„testy statystyczne są zwykle pierwszym narzędziem w rękach kryptoanalityka, wskazującym mu ewentualne błędy popełnione w trakcie projektowania algorytmu"*, co jednoznacznie wpisuje problem w obszar praktycznej weryfikacji bezpieczeństwa konstrukcji kryptograficznych.

Chociaż autor nie formułuje wprost hipotezy badawczej, z całości rozprawy wynika, że zasadniczym celem jest opracowanie i empiryczna weryfikacja pakietu testów pozwalającego na ocenę jakości losowości ciągów generowanych przez różne źródła kryptograficzne. W rozdziale I pkt. 4 autor pisze: *„W pracy tej chcemy zwrócić uwagę na dwa aspekty użytkowania pakietu testów losowości, którym naszym zdaniem nie poświęcono dotychczas należytej uwagi. [...] (Pierwszy) to kwestia poprawności wyników otrzymywanych na podstawie pojedynczego testu. [...] Drugą, jest skorelowanie statystyk procedur testowych; dające się empirycznie mierzyć skorelowanie wartości p_{val} otrzymywanych dla tych samych ciągów"* (s. 23). Cytowany fragment wskazuje, że przedmiotem badań jest zarówno poprawność metodologiczna, jak i analiza wzajemnych zależności między wynikami testów.

W części opisującej wybrane istniejące pakiety testów losowości (rozdział III) autor omawia m.in. opracowania i pakiety: rozdział 3.3.2 w tomie II książki D. E. Knutha, *DIEHARD*, *FIPS PUB 140*, *AIS-31*, *NIST SP 800-22 Statistical Test Suite*, *TestU01*, *Dieharder* oraz *Crypt-X*, przedstawiając ich strukturę, zakres zastosowań i przykłady testów (s. 85–120). W tym rozdziale autor dokonuje szczegółowej analizy poprawności wybranych procedur, formułując krytyczne uwagi wobec poszczególnych implementacji, np. pakietu NIST, w którym *„... poważnym uchybieniem jest nierozróżnianie przez implementację testu obu powodów przerwania procedury testowej"* (s. 106), czy pakietu Dieharder, którego implementacja *„zawiera błąd związany z odrzucaniem klas o zbyt małej wartości oczekiwanej liczby obserwacji"* (s. 119). Tego rodzaju obserwacje stanowią empiryczne uzasadnienie dla podjęcia przez autora dalszych prac nad własnym zestawem testów i jego implementacją, rozwiniętych w kolejnych rozdziałach rozprawy.

Problem badawczy został więc sformułowany pośrednio, lecz jasno: autor dąży do weryfikacji, czy możliwe jest opracowanie i zastosowanie własnego pakietu testów pozwalającego rzetelnie oceniać losowość generatorów kryptograficznych. W tym znaczeniu teza pracy ma zarazem charakter aplikacyjny i metodologiczny. Opracowanie autorskiego pakietu testów i jego empiryczna walidacja stanowią logiczną odpowiedź na zidentyfikowaną lukę badawczą, co czyni problem naukowy trafnie dobranym i spójnie rozwiniętym w strukturze rozprawy.

Jaka jest konstrukcja rozprawy?

Rozprawa doktorska mgr. inż. Krzysztofa Mańka liczy 303 strony tekstu zasadniczego i posiada klasyczną strukturę, uzupełnioną dwoma załącznikami: **Załącznikiem A** – *„Zestawy procedur dla ciągów długości 1 kiB"* i **Załącznikiem B** – *„Zestawy procedur dla ciągów długości 1 Mb"*. **Praca jest nad wyraz obszerna jak na rozprawę doktorską tego typu**, co świadczy o rozległości

przeprowadzonych analiz, kompletności badań oraz dużym nakładzie pracy autora. Całość jest logicznie uporządkowana i spójna tematycznie, a układ rozdziałów odzwierciedla naturalny tok badań: od wprowadzenia teoretycznego i analizy istniejących metod po opracowanie własnego pakietu testowego, jego walidację i analizę korelacji między procedurami.

We **Wstępie** autor określa motywację badań, wskazując na potrzebę opracowania zestawu testów spełniającego wymogi poprawności matematycznej, jednoznaczności i powtarzalności wyników. Wskazuje niedoskonałości istniejących pakietów oraz uzasadnia potrzebę stworzenia własnego, zintegrowanego środowiska testowego. W końcowej części wstępu przedstawia ogólny plan pracy – sześć rozdziałów, z których każdy obejmuje kolejny etap badań.

Rozdział I (*„Losowość, generatory i testy statystyczne”*) wprowadza podstawowe pojęcia teoretyczne związane z losowością, generatorami liczb pseudolosowych i testami statystycznymi. Omawia definicje, relacje między generatorami fizycznymi a pseudolosowymi oraz formalne ujęcia pojęcia losowości, w tym definicje funkcji zaniedbywalnej i algorytmów obliczalnych. Zdefiniowano w nim także pojęcie procedury testowej oraz przedstawiono podstawowe założenia testów drugiego i trzeciego poziomu, a na końcu zaprezentowano cel pracy.

Rozdział II stanowi szerokie kompendium opisujące metody i algorytmy testowania losowości. Zawiera szczegółowe omówienie kilkudziesięciu testów statystycznych, obejmujących zarówno procedury ogólne, jak i liczne testy dedykowane dla ciągów bitowych, czy ciągów bloków bitów. Autor systematyzuje je według sposobu interpretacji danych, opisując założenia, statystyki testowe, rozkłady teoretyczne oraz ograniczenia poszczególnych metod. Ta część pracy stanowi podstawę merytoryczną wykorzystywaną w kolejnych etapach analizy pakietów testowych.

Rozdział III (*„Wybrane pakiety testów losowości”*) prezentuje przegląd i analizę istniejących zestawów testów stosowanych w kryptografii: opracowania Knutha, *DIEHARD*, *FIPS PUB 140*, *AIS-31*, *NIST SP 800-22*, *TestU01*, *Dieharder* i *Crypt-X*. Autor omawia ich strukturę, zakres oraz wskazuje błędy i ograniczenia implementacyjne. Rozdział ten uzasadnia potrzebę opracowania własnego, poprawnie zweryfikowanego środowiska testowego.

Rozdział IV opisuje trójpoziomową procedurę służącą do oceny jakości testów losowości poprzez porównywanie wyników uzyskiwanych dla kilku zróżnicowanych generatorów pseudolosowych, traktowanych jako praktyczne przybliżenie idealnego źródła. Analiza pokazuje, że żaden z testów zgodności nie wykazuje zdolności rozróżniania zastosowanych generatorów, natomiast same testy, po dodatkowej wielopoziomowej weryfikacji, okazują się stabilne i nadają się do wykorzystania jako testy wyższych poziomów. Autor ostatecznie rekomenduje test Andersona-Darlinga jako najdokładniejszy i użyteczny w dalszych etapach badań.

Rozdział V podsumowuje praktyczną ocenę procedur testowych dla ciągów 1 kiB i 1 Mb, weryfikując ich zdolność do badania generatorów przy różnej liczbie powtórzeń. Autor pokazuje, że większość procedur, mimo obecności w literaturze i pakietach takich jak NIST STS, nie spełnia kryteriów poprawności ani stabilności, co prowadzi do eliminacji testów na kolejnych poziomach walidacji. W efekcie pozostaje podzbiór procedur, które mogą być uznane za rzeczywiście przydatne w badaniu prymitywów kryptograficznych.

Rozdział VI poświęcony jest analizie współzależności między testami. Autor bada korelacje liniowe, nieliniowe i wielowymiarowe między wartościami p_{val}, stosując regresję dwu- i wielowymiarową oraz analizę grup skorelowanych procedur. Celem jest dalsze ograniczenie liczby testów

poprzez eliminację nadmiarowych i silnie skorelowanych procedur, z zachowaniem maksymalnej skuteczności pakietu.

Podsumowanie syntetyzuje rezultaty budowy pakietu *TeStat*, obejmującego zestaw zweryfikowanych procedur testowych oraz kluczowe wyniki teoretyczne i implementacyjne. Autor podkreśla redukcję nadmiarowości i korelacji testów oraz wskazuje kierunki dalszego rozwoju pakietu, w tym rozszerzenia dla dłuższych ciągów i wariantów on-line. **Załączniki A i B** zawierają proponowane zestawy procedur oraz rekomendacje.

Na podkreślenie zasługuje bardzo dobre rozeznanie doktoranta w literaturze przedmiotu. Wykaz bibliograficzny obejmuje 112 pozycji, w tym zarówno klasyczne publikacje z XX wieku, jak i liczne prace z ostatnich lat. Najmłodsza pozycja spoza dorobku autora pochodzi z 2022 r., co pozwala uznać zestawienie literatury za dość aktualne i odpowiednio osadzające rozprawę w kontekście współczesnych badań. Autor w sposób właściwy odnosi się do dotychczasowego dorobku, wykorzystując zarówno prace poświęcone teoretycznym podstawom losowości i generatorów, jak i opracowania dotyczące praktycznych pakietów testów oraz ich walidacji. Warto podkreślić, że część cytowanej literatury stanowią współautorskie publikacje mgr. inż. Krzysztofa Mańka, które zostały wcześniej pozytywnie ocenione w procesie recenzyjnym przez innych recenzentów, co dodatkowo potwierdza zasadność obranej problematyki oraz dojrzałość naukową doktoranta. Wnioski z przeglądu stanu wiedzy oraz aktualnych badań w uznanych ośrodkach naukowych zostały przedstawione w sposób jasny i przekonujący, a dobór źródeł należy uznać za adekwatny do zakresu i ambicji rozprawy.

Struktura rozprawy jest przejrzysta, spójna i dobrze uzasadniona merytorycznie. Poszczególne rozdziały tworzą logiczny ciąg prowadzący od podstaw teoretycznych i analizy literaturowej po autorskie rozwiązania i ich empiryczną walidację, co zapewnia wysoką czytelność i klarowność argumentacji badawczej.

Czy tematyka rozprawy jest aktualna lub dostatecznie ważna?

Tematyka rozprawy doktorskiej jest bez wątpienia aktualna, naukowo uzasadniona i posiada istotne znaczenie zarówno z perspektywy współczesnej kryptografii, jak i praktycznych zastosowań w bezpieczeństwie informacji. Jakość losowości generowanej przez prymitywy kryptograficzne stanowi fundament wielu systemów bezpieczeństwa, począwszy od generatorów liczb pseudolosowych, przez protokoły wymiany kluczy i podpisy cyfrowe, po funkcje skrótu i szyfry blokowe. W dobie rosnących wymagań dotyczących ochrony danych, certyfikacji urządzeń kryptograficznych oraz rozwoju kryptografii postkwantowej, problem poprawnej i powtarzalnej oceny losowości nabiera szczególnej wagi. W literaturze i praktyce funkcjonuje kilka konkurencyjnych pakietów testów losowości, które według autora cechują się niejednoznacznością wyników, problemami analitycznymi i implementacyjnymi oraz brakiem pełnej weryfikacji statystycznej. W takiej sytuacji podjęcie tematu konstrukcji i oceny zestawu poprawnych oraz stabilnych procedur testowych staje się zagadnieniem szczególnie istotnym.

Aktualność tematyki wynika również z dynamicznego rozwoju generatorów losowych, w tym sprzętowych generatorów opartych na zjawiskach fizycznych, generatorów kwantowych oraz konstrukcji hybrydowych. Dla wielu z nich tradycyjne testy losowości okazują się niewystarczające, co znajduje odzwierciedlenie w najnowszych publikacjach poświęconych korelacji pomiędzy testami, powtarzalności wyników i odporności procedur statystycznych na błędy estymacji. W tym

kontekście opracowana w rozprawie autorska trójpoziomowa procedura testowa, mająca na celu rzetelną weryfikację poprawności i przydatności poszczególnych testów, wpisuje się w nurt aktualnych badań dotyczących metod oceny jakości generatorów losowych.

Znaczenie podjętego tematu wykracza poza obszar badań teoretycznych. Problematyka testowania generatorów jest ściśle powiązana z wymaganiami certyfikacyjnymi i regulacyjnymi stosowanymi w systemach bezpieczeństwa telekomunikacyjnych, bankowych, przemysłowych oraz w infrastrukturze krytycznej. Wymagania te znajdują odzwierciedlenie w standardach takich jak Common Criteria, FIPS 140-3 czy wytyczne ENISA, które kładą nacisk na niezależną i statystycznie poprawną ocenę źródeł losowości. W tym świetle praca autora posiada realny potencjał aplikacyjny, gdyż przedstawiona metodologia może stanowić podstawę do oceny jakości prymitywów kryptograficznych stosowanych w praktyce.

Należy również zauważyć, że zagadnienia opisane w rozprawie pozostają istotne w kontekście rozwoju kryptografii postkwantowej i zaufanych systemów obliczeniowych. Wraz z pojawieniem się nowych klas zagrożeń, takich jak manipulacje generatorami na poziomie sprzętowym czy analizy statystyczne prowadzone z wykorzystaniem algorytmów kwantowych, wzrasta potrzeba opracowywania wiarygodnych i odpornych na błędy procedur testowania losowości. Podjęta w rozprawie próba uporządkowania i matematycznego zweryfikowania metod badania losowości odpowiada na te współczesne wyzwania.

Opracowana w rozprawie spójna, zarówno metodologicznie, jak i empirycznie zweryfikowana procedura testowa stanowi odpowiedź na realne potrzeby współczesnej kryptologii i bezpieczeństwa cyfrowego. Przedstawiona analiza istniejących rozwiązań, połączona z budową własnego, poprawnego statystycznie zestawu testów, wpisuje się w bieżące prace nad doskonaleniem metod oceny generatorów losowych w kontekście certyfikacji, standaryzacji oraz praktycznych zastosowań komercyjnych i instytucjonalnych. Tematyka rozprawy mieści się więc w centrum aktualnych badań nad jakością losowości i bezpieczeństwem prymitywów kryptograficznych, a jednocześnie posiada wyraźny potencjał aplikacyjny, istotny dla dalszego rozwoju nowoczesnych systemów ochrony informacji.

Czy rozprawa prezentuje ogólną wiedzę teoretyczną doktoranta?

Rozprawa w sposób wyraźny potwierdza, że autor posiada szeroką i solidną wiedzę teoretyczną obejmującą zarówno podstawy matematyczne testów losowości, jak i zagadnienia związane z konstrukcją oraz analizą prymitywów kryptograficznych. W pierwszych rozdziałach pracy doktorant przedstawia spójny przegląd pojęć niezbędnych do zrozumienia dalszej części rozprawy, obejmujący m.in. formalne definicje losowości, właściwości generatorów liczb pseudolosowych, klasyczne testy statystyczne oraz ich interpretację. Zestawienie to ma charakter uporządkowanego kompendium i świadczy o bardzo dobrej orientacji autora w literaturze przedmiotu.

W kolejnych rozdziałach doktorant adekwatnie wykorzystuje tę wiedzę, przechodząc od prezentacji podstaw teoretycznych do krytycznej analizy istniejących pakietów testów oraz zaprojektowania i uzasadnienia własnej procedury badawczej. Trafność doboru narzędzi statystycznych, poprawność metodologiczna oraz umiejętność interpretacji wyników potwierdzają, że autor nie tylko zna stosowane koncepcje teoretyczne, lecz także potrafi je właściwie zastosować w praktyce badawczej. Całość świadczy o wszechstronnej znajomości zagadnień z obszaru kryptografii stosowanej, statystyki i analizy danych.

Czy rozprawa wykazuje umiejętność samodzielnego prowadzenia pracy naukowej?

Rozprawa jednoznacznie potwierdza umiejętność samodzielnego prowadzenia pracy naukowej przez doktoranta. Autor podejmuje złożone zadania badawcze obejmujące krytyczną analizę istniejących pakietów testów losowości, identyfikację ich ograniczeń oraz opracowanie własnych procedur weryfikacyjnych. Samodzielność przejawia się w świadomym i uzasadnionym wyborze metod, w konstrukcji trójpoziomowej procedury testowej oraz w przygotowaniu narzędzi eksperymentalnych pozwalających na przeprowadzenie szerokiego zakresu badań porównawczych.

Autor konsekwentnie realizuje zaplanowany program badawczy, formułuje własne kryteria eliminacji procedur testowych, interpretuje wyniki eksperymentów oraz buduje końcowe rekomendacje. Całość wskazuje na dojrzałość metodologiczną, umiejętność projektowania oraz prowadzenia badań empirycznych, a także zdolność do wyciągania trafnych i logicznych wniosków na podstawie dużych zbiorów danych. Rozprawa w pełni potwierdza, że doktorant jest przygotowany do samodzielnej działalności naukowej.

Czy rozprawa stanowi oryginalne rozwiązanie problemu naukowego albo oryginalne rozwiązanie w zakresie zastosowania wyników własnych badań naukowych w sferze gospodarczej lub społecznej?

Rozprawa przedstawia oryginalne rozwiązanie problemu naukowego w obszarze oceny losowości prymitywów kryptograficznych. Autor nie ogranicza się do analizy istniejących pakietów testów, lecz identyfikuje ich braki metodologiczne oraz niejednoznaczności interpretacyjne, co prowadzi do sformułowania własnego podejścia badawczego. Najbardziej wyrazistym elementem oryginalności jest zaprojektowanie i uzasadnienie trójpoziomowej procedury testowej, opisanej przez doktoranta jako podstawowe narzędzie wykorzystane w pracy. Procedura ta pełni kluczową rolę w ocenie poprawności i przydatności poszczególnych testów losowości oraz stanowi autorskie rozwiązanie konstrukcyjne, niewystępujące w takiej postaci w literaturze.

Oryginalny charakter mają również opracowane kryteria eliminacji procedur testowych oraz sposób selekcji zestawów testów o największej zdolności rozróżniania generatorów. Wyniki te prowadzą do stworzenia rekomendowanych pakietów procedur dla różnych długości ciągów i parametrów badawczych, co nadaje pracy wymiar praktyczny. Choć celem rozprawy nie jest bezpośrednie opracowanie rozwiązania wdrożeniowego, przedstawione narzędzia i metodologia mogą znaleźć zastosowanie w procesach certyfikacji, standaryzacji i ocenie jakości generatorów losowych stosowanych w systemach bezpieczeństwa, co podkreśla ich potencjalną użyteczność w sferze gospodarczej i instytucjonalnej.

Jakie są słabe strony rozprawy i jej główne wady?

Pomimo dużej wartości merytorycznej rozprawy, dostrzegalne są pewne słabe strony, które wpływają na jej klarowność oraz odbiór. Najistotniejszą z nich jest bardzo duża objętość pracy oraz rozbudowany zakres materiału, który miejscami utrudnia szybkie uchwycenie głównej myśli badawczej. Obszerny, encyklopedyczny charakter rozdziałów dotyczących testów losowości i pakietów testowych sprawia, że zasadniczy wątek własnych badań autora zostaje przesunięty do

dalszych rozdziałów. Momentami pojawia się również powtórzenie tych samych objaśnień lub ujęć definicyjnych, co niepotrzebnie zwiększa objętość tekstu.

Pewnym ograniczeniem jest także stosunkowo skromne odniesienie wyników do najnowszych prac dotyczących walidacji pakietów testowych czy badań nad korelacją procedur statystycznych, co mogłoby dodatkowo wzmocnić kontekst literaturowy. Brakuje również bardziej rozbudowanej dyskusji dotyczącej praktycznych scenariuszy zastosowania opracowanego zestawu testów w narzędziach certyfikacyjnych lub w środowiskach produkcyjnych. Choć autor przedstawia uzasadnione kryteria eliminacji procedur testowych i klarownie prezentuje wyniki, miejscami przydałoby się głębsze omówienie konsekwencji niektórych obserwacji, zwłaszcza w kontekście ograniczeń metod statystycznych dla krótkich próbek.

Wskazane słabości nie podważają jakości całościowego dorobku zawartego w rozprawie, jednak stanowią elementy, które mogłyby zostać dopracowane w przyszłych rozszerzeniach lub publikacjach wynikających z tej pracy.

Analiza językowa i strukturalna: błędy gramatyczne, typograficzne i inne problemy w tekście

Język i styl rozprawy świadczą o wysokiej świadomości językowej i redakcyjnej autora. Tekst jest precyzyjny, spójny, logicznie uporządkowany i poprawny gramatycznie. Mimo ogólnie bardzo dobrej jakości językowej, w pracy można wskazać nieliczne błędy i uchybienia, głównie natury stylistycznej i typograficznej. Nie mają one jednak wpływu na zrozumiałość tekstu ani na jego wartość merytoryczną. Poniżej przedstawiam ich charakterystykę.

Pod względem gramatycznym tekst jest w zasadzie poprawny. Nieliczne błędy dotyczą głównie zgody liczby i rodzaju oraz nadmiernej długości zdań złożonych.

W zdaniu „Ogromna moc obliczeniowa i pojemność pamięci współczesnych komputerów jest jednak ograniczona...” występuje niezgodność liczby. Poprawnie powinno być: „...są jednak ograniczone...”.

Część zdań jest zbyt rozbudowana, co utrudnia ich odbiór. Przykładem może być: „Jeśli więc realnie dostępne są tylko rozwiązania działające w czasie wielomianowym oraz rzeczona tolerancja jest asymptotycznie ograniczona przez odwrotność dowolnego wielomianu, to szansa na odróżnienie dwóch obiektów mieszczących się w zakresie rzeczonej tolerancji, jest zaniedbywalnie mała.” Zdanie to można uprościć i rozdzielić dla większej czytelności, nie tracąc treści merytorycznej.

W większości rozdziałów autor używa pierwszej osoby liczby mnogiej, co jest w pełni akceptowalne w polskiej i międzynarodowej praktyce akademickiej. Sporadycznie pojawia się niekonsekwencja osobowa, np. „Wiarygodność rozumiemy jako...” w kontekście, w którym autor częściej używa konstrukcji bezosobowych. Z punktu widzenia stylistycznej spójności zaleca się ujednolicenie narracji przez zachowanie konsekwentnie pierwszej osoby liczby mnogiej (która w pracy dominuje) lub całkowite przejście na styl bezosobowy, np. „Wiarygodność należy rozumieć jako matematyczną poprawność oceny każdego z testów z osobna oraz oceny końcowej.”

W pracy występuje kilka drobnych błędów interpunkcyjnych, np. „W szczególności, jest ona jednym z narzędzi...”, podczas gdy poprawnie powinno być: „W szczególności jest ona jednym z narzędzi...”. Zauważalna jest również niekonsekwencja w stawianiu przecinków przed spójni-

kami „że", „który", „gdy", np. w zdaniu „. . . to szansa na odróżnienie dwóch obiektów mieszczących się w zakresie rzeczonej tolerancji, jest zaniedbywalnie mała." przecinek przed „jest" jest zbędny.

W tekście pojawiają się również sformułowania typu „Uzmysławia nieoczywiste na pierwszy rzut oka relacje pomiędzy różnymi testami.", które mają charakter potoczny. Bardziej precyzyjną i neutralną wersją byłoby: „Ujawnia nieoczywiste zależności pomiędzy różnymi testami."

Całość rozprawy została napisana poprawnym i dojrzałym językiem naukowym, zgodnym z konwencjami obowiązującymi w naukach inżynieryjno-technicznych. Tekst charakteryzuje się dużą spójnością terminologiczną, logiczną strukturą oraz wysokim poziomem precyzji w operowaniu językiem matematycznym. Zidentyfikowane błędy mają charakter drobnych potknięć techniczno-redakcyjnych, a nie merytorycznych i nie mają żadnego wpływu na jakość naukową pracy ani na odbiór przedstawionych wyników. Tym samym zauważone problemy można traktować jako naturalne w pracy o tak dużej objętości i skomplikowanej tematyce.

Wniosek końcowy

Na podstawie przeprowadzonej analizy rozprawy doktorskiej mgr. inż. Krzysztofa Mańka pt. *„Pakiet testów losowości do badania prymitywów kryptograficznych"* stwierdzam, że:

- rozprawa stanowi oryginalne rozwiązanie problemu naukowego;
- treść rozprawy świadczy o ogólnej i ugruntowanej wiedzy Doktoranta w dyscyplinie naukowej informatyka techniczna i telekomunikacja;
- rozprawa jednoznacznie potwierdza umiejętność samodzielnego prowadzenia pracy naukowej przez Doktoranta.

Powyższe oznacza, że praca spełnia wymagania określone w art. 187 ustawy z dnia 20 lipca 2018 r. *Prawo o szkolnictwie wyższym i nauce* (Dz. U. z 2023 r. poz. 742 z późn. zm.) w odniesieniu do rozprawy doktorskiej w dziedzinie nauk inżynieryjno-technicznych, w dyscyplinie informatyka techniczna i telekomunikacja.

Uwzględniając przedstawione oceny merytoryczne, oryginalność wyników oraz bardzo duży nakład pracy związany z przygotowaniem rozprawy, w szczególności rozległy zakres przeprowadzonych badań eksperymentalnych, skalę analiz oraz staranność opracowania pakietu testów i materiałów uzupełniających, **wnioskuję** do Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja przy Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego w Warszawie **o przyjęcie recenzowanej rozprawy doktorskiej** mgr. inż. Krzysztofa Mańka, dopuszczenie jej do publicznej obrony oraz nadanie Autorowi stopnia doktora nauk inżynieryjno-technicznych w dyscyplinie informatyka techniczna i telekomunikacja.

Ponadto, biorąc pod uwagę wysoki poziom merytoryczny pracy, jej oryginalny charakter oraz wyjątkowo dużą pracochłonność i skalę przeprowadzonych badań, **wnoszę o wyróżnienie rozprawy** zgodnie z obowiązującymi w Wojskowej Akademii Technicznej zasadami.

PODPIS ZAUFANY
GRZEGORZ ANDRZEJ
BOROWIK
17.11.2025 13:32:48 GMT+1
Dokument podpisany elektronicznie
podpisem zaufanym