Prof. dr hab. inż. Franciszek Seredyński
Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie
Wydział Matematyczno – Przyrodniczy
Szkoła Nauk Ścisłych
ul. Wóycickiego 1/3, 01-938 Warszawa

Warszawa, 19.10.2013

OPINIA
o dorobku naukowym, dydaktycznym i naukowo-organizacyjnym
dr hab. Janusza Szczepańskiego w związku z postępowaniem
o nadanie tytułu naukowego profesora w dziedzinie nauk technicznych

1. Ogólna charakterystyka Kandydata

Dr hab. Janusz Szczepański jest pracownikiem Instytutu Podstawowych Problemów Techniki PAN w Warszawie, gdzie jest zatrudniony na stanowisku profesora nadzwyczajnego. Jest absolwentem Wydziału Matematyki Uniwersytetu Warszawskiego (1979 r.), stopień doktora nauk technicznych Kandydat uzyskał w IPPT PAN (dyscyplina Mechanika) w 1985 r., a stopień doktora habilitowanego (dyscyplina Informatyka) uzyskał z wyróżnieniem również w IPPT PAN w 2007 r.

Obszar zainteresowań badawczych Kandydata obejmuje szerokie spektrum dziedzin, takich jak informatyka, neuroinformatyka, matematyka, fizyka czy nauki inżynieryjne. Uzyskał w nich znaczące wyniki naukowe potwierdzone pracami publikowanymi w renomowanych czasopismach.

Od wielu lat współpracuje naukowo ze specjalistami krajowymi oraz specjalistami z wiodących zagranicznych ośrodków naukowych w Hiszpanii (Prof. J.M. Amigo, Uniwersytet Miguel Hernandez w Alicante), w USA (Prof. L. Kocarev, Uniwersytet Kalifornijski w San Diego), w W. Brytanii (Prof. M. Slater, University College London). Odbywał staże naukowe jako Visiting Professor na Uniwersytecie Kalifornijskim w San Diego oraz na Uniwersytecie Miguel Hernandez w Alicante.

2. Ocena dorobku naukowo-badawczego

Dorobek naukowy Kandydata jest obszerny i obejmuje ponad 70 publikacji, które pojawiały się w latach 1988 – 2013. Są to artykuły opublikowane w czasopismach, prace o charakterze monograficznym oraz artykuły konferencyjne. Wśród nich 34 prace to artykuły opublikowane w czasopismach naukowych znajdujących się na tzw. liście filadelfijskiej, z tego 11 po złożeniu dokumentów habilitacyjnych.

Publikowane prace to w większości prace wspólne, które powstały bądź w ramach prowadzonych doktoratów, a współautorami są doktoranci realizujący swoje badania pod kierunkiem i przy współpracy Kandydata, bądź są wynikiem współpracy Kandydata z krajowymi oraz zagranicznymi ośrodkami naukowymi.

Kandydat publikował swoje wyniki, między innymi, w takich renomowanych międzynarodowych czasopismach jak:

- **IEEE Transactions on Circuits and Systems I**
- **IEEE Transactions on Circuits and Systems II**
- **Information Sciences**
- **International Journal of Bifurcation and Chaos**
- **Journal of Biological Physics**
- **Journal of Sleep Research**
- **Neurocomputing**
- **Network: Computation in Neural Systems**
- **Physics Letters A**
- **Physica D**
- **Physical Review Letters**
- **Biosystems**
- **Biological Cybernetics**
- **Bulletin of the Polish Academy of Sciences**
- **Computers and Security.**

Główne dziedziny i kierunki prac badawczych Kandydata to:

- Mechanika statystyczna dla układów o nieskończonej przeliczalnej liczbie stopni swobody
- Teoria chaosu i ergodyczności w mechanice
- Problem Nirenberga dla odwzorowań rozciągających
- Zastosowanie układów dynamicznych w kryptografii
- Zastosowanie teorii informacji i teorii układów dynamicznych w układach biologicznych
- Chaos w układach dyskretnych.

Tematyka prac badawczych Kandydata ewoluowała i rozszerzała się z upływem czasu. Swoje badania naukowe rozpoczynał koncentrując się na zagadnieniach **mechaniki statystycznej**, w tym na problemach związanych ze sformułowaniem odpowiedników klasycznej mechaniki statystycznej dla układów o nieskończonej przeliczalnej liczbie stopni swobody modelowanych w przestrzeni Hilberta. Ich finałem była praca doktorska. Badania związane z mechaniką statystyczną były przez niego kontynuowane bezpośrednio po doktoracie i dotyczyły zastosowań **teorii chaosu i układów dynamicznych** w mechanice gazów rozrzedzonych. W okresie tym prowadził również badania czysto matematyczne, zajmując się tzw. **problemem Nirenberga dla odwzorowań rozciągających** w przestrzeniach Hilberta.

W połowie lat 90-tych ubiegłego wieku następuje w jego badaniach zwrot w kierunku tematyki związanej z technologiami informatycznymi, a w szczególności z kryptografią. W sposób twórczy wykorzystuje tu swoje doświadczenia zdobyte w ramach badań nad teorią chaosu. Pierwsze prace z nurtu kryptograficznego związane były z poszukiwaniem modeli systemów kryptograficznych mających genezę w dynamice cząstek oraz tworzenia generatorów liczb losowych bazujących na układach chaotycznych. Kolejne prace z tego nurtu poświęcone były zastosowaniu tzw. periodycznych aproksymacji **układów dynamicznych do projektowania kryptosystemów** o udowadnialnej odporności na standardowe ataki. W związku z gwałtownym rozwojem technologii komunikacji bezprzewodowej jaki można obserwować na przełomie XX i XXI wieku, i który trwa do dzisiaj, Kandydat skupia swoją uwagę na zagadnieniach projektowania optymalnych-dedykowanych algorytmów kryptograficznych zapewniających bezpieczeństwo transmisji danych. Powstaje tu szereg interesujących prac teoretycznych dotyczących, m.in. związków między układami chaotycznymi i dynamiką losową, analizy możliwości zastosowania wprowadzonego przez Kandydata (oraz jego Kolegów) pojęcia dyskretnego wykładnika Lapunowa do badania własności losowych permutacji zbiorów skończonych czy analizy własności cyklicznych i spełniania tzw. kryterium lawinowości. W wyniku prowadzonych prac powstaje, w szczególności, oryginalna metoda konstrukcji permutacji gwarantująca, że permutacje te stosowane do konstrukcji szyfru blokowego zapewniają jego odporność na kryptoanalizę liniową i różnicową. W kontekście prac nurtu kryptograficznego należy również wskazać na prace Kandydata dotyczące praktycznych możliwości stworzenia generatora liczb losowych opartego na zjawiskach biologicznych.

Na początku XXI w. Kandydat włącza się w nowy nurt badań dotyczący zastosowania **teorii informacji i teorii układów dynamicznych w naukach biologicznych**, a w szczególności Neuroscience oraz DNA. Kandydat skupia się na analizie przesyłania informacji wizualnych przez komórki neuronowe w mózgu. Analiza danych eksperymentalnych pod kątem złożoności odpowiedzi neuronów w zależności od zmiany parametrów kodowania wskazała na interesujący fakt istnienia tzw. poziomów nasycenia związanych z typem kodowania. Kandydat zajmował się również analizą własności źródła informacji, celem której było określenie estymatora liczby stanów źródła dla różnych składowych źródła. Uzyskano tu bardzo interesujące wyniki polegające na analizie estymatora entropii opartego na koncepcji złożoności Lempela-Ziva, dzięki której pokazano, że estymator ten jest szybszy od standardowego aktualnie używanego estymatora zaczerpniętego z literatury fizycznej.

Prace te są również kontynuowane po uzyskaniu habilitacji. Przeprowadzono analizę procesu przesyłania informacji przez populacje neuronów pod kątem redundancji transmisji oraz informacji wzajemnej współpracujących neuronów. W kontekście tych prac wprowadzono i udowodniono własności tzw. względnego współczynnika informacji wzajemnej i pokazano, że o ile redundancja podczas transmisji może wykazywać znaczne fluktuacje, o tyle informacja względna zachowuje się stabilnie, a sama współpraca w obrębie grupy neuronów może być bardzo elastyczna. W najnowszych publikowanych pracach przeprowadzono analizę przepływu informacji w korze mózgowej przy zmianie stanów mózgu. Pokazano ilościową symetrię transmisji przy przejściu miedzy

stanami oraz pokazano, że transmisja informacji charakteryzuje się dużymi fluktuacjami, co sugeruje, że komunikacja odbywa się pakietami. Przeprowadzano również analizę efektywności transmisji dla sieci komórek neuronowych w zależności od charakterystyki neuronów. Uzyskano istotne wyniki pokazujące, że w dużym zakresie parametrów transmisja jest wydajniejsza podczas występowania pewnego poziomu szumu oraz większego tłumienia zachowań fluktuacji. Przedmiotem badań, w których uzyskano również interesujące wyniki były badania dotyczące możliwości konstrukcji tzw. potencjałów statystycznych dla łańcuchów DNA.

Obszarem aktualnych zainteresowań Kandydata jest również problematyka **chaosu w układach dyskretnych**, w tym zagadnienia związane z wprowadzeniem klasycznych odpowiedników koncepcji związanych z teorią chaosu układów dynamicznych dla układów o dyskretnej przestrzeni stanów. Uzyskano tu interesujące wyniki dotyczące możliwości zastosowania wprowadzonych koncepcji dyskretnych wykładników Lyapunova do analizy jakości systemów kryptograficznych, w tym oceny odporności kryptosystemu na kryptoanalizę różnicową.

Do najważniejszych osiągnięć naukowych Kandydata potwierdzonych publikacjami chciałbym zaliczyć:

- wyniki prac poświęconych teorii chaosu i ergodyczności w mechanice, w szczególności przedstawione w publikacji **J. Szczepanski, E.Wajnryb, „Long-Time Behaviour of the One-Particle Distribution Function for the Knudsen Gas in a Convex Domain”, *Physical Review A*, v. 44, No. 6, pp. 3615-3621, American Physical Society, 1991**
- wyniki prac poświęconych problemowi Nirenberga dla odwzorowań rozciągających, w szczególności przedstawionych w publikacji **J. Szczepanski, “A New Result on the Nirenberg Problem for Expanding Maps”,** *Nonlinear Analysis: Theory Methods & Applications*, **vol. 43, pp. 91 – 99, Pergamon – Elsevier Publishers, 2001**
- wyniki prac poświęconych zastosowaniu układów dynamicznych w kryptografii, w szczególności przedstawionych w publikacji **J. Szczepanski, J.M. Amigo, T. Michałek, L. Kocarev, „Cryptografically secure substitutions based on the approximation of mixing maps,** *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications,* **52 (2), pp. 443-453, IEEE, 2005**
- wyniki prac poświęconych zastosowaniu teorii informacji i teorii układów dynamicznych w układach biologicznych, w tym praca **B. Paprocki, J. Szczepanski, “Efficiency of neural transmission as a function of synaptic noise, threshold, and source characteristics,** *Biosystems* 105**, pp. 62-72, Elsevier, 2011,** praca **M. M. Arnold, J. Szczepanski, N. Montejo, J.M. Amigo, E. Wajnryb, M.V. Sanchez-Vives, “Information content in cortical spike trains during brain state transitions”,** *Journal of Sleep Research*, **vol. 22, pp. 13 – 21, Wiley, 2013** oraz praca **B. Paprocki, J. Szczepanski, “How do the amplitude fluctuations affect the neuronal transmission efficiency”, *Neurocomputing*, 104, pp. 50-56, Elsevier, 2013**
- wyniki prac poświęconych chaosowi w układach dyskretnych, w tym praca **J. M. Amigo, L. Kocarev, J. Szczepanski, “Discrete Lyapunov exponent and**

resistance to differential cryptanalysis", *IEEE Transactions on Circuits and Systems II,* 54 (10)**, pp. 882-886, IEEE, 2007** oraz praca **J. M. Amigo, L. Kocarev, J. Szczepanski, On some properties of the discrete Lyapunov exponent,** *Physics Letters A***, 372 (41), pp. 6265 – 6268, Elsevier, 2008**

Podsumowując dorobek naukowy Kandydata można stwierdzić, że charakteryzuje się on szerokim spektrum dziedzin, a na szczególne uznanie zasługują jego wyniki naukowe osiągnięte w obszarach związanych z zastosowaniem metod bazujących na teorii układów dynamicznych w kryptografii oraz zastosowaniu metod teorii informacji w badaniu procesów zachodzących w mózgu. Wysoka ranga naukowa osiągnięć Kandydata jest potwierdzana na arenie międzynarodowej i krajowej. Lista cytowań prac Kandydata wg. **ISI Web of Knowledge/Web of Science** wynosi 259, a indeks Hirscha wynosi 11. Sumaryczny Impact Factor wynosi 57.821, w tym po uzyskaniu habilitacji 22.207. Uważam więc, że jego dorobek naukowy, w tym dorobek po uzyskaniu habilitacji, z nadmiarem czyni zadość wymaganiom stawianym przez Kandydata do tytułu naukowego profesora, zarówno pod względem ilościowym jak i przede wszystkim jakościowym.

Na prowadzenie swoich badań uzyskiwał fundusze z NCN-u, KBN-u jak też z ośrodków zagranicznych. Był kierownikiem, głównym wykonawcą bądź wykonawcą szeregu krajowych i międzynarodowych projektów badawczych.

Wysoka pozycja Kandydata na arenie międzynarodowej uzyskana po otrzymaniu stopnia naukowego dr habilitowanego, wynikająca z jego dorobku naukowego znalazła swoje potwierdzenie i odzwierciedlenie w powierzanych mu funkcjach organizacyjnych oraz zaproszeniach do udziału w komitetach programowych konferencji oraz komitetach redakcyjnych czasopism.

Jest od 2007 r. członkiem Komitetu Redakcyjnego czasopisma International Journal of Computational Science wydawanego w Hongkongu przez Global Information Publisher. Przez szereg lat był członkiem Komitetu Programowego konferencji Future Generation Communication and Networking jak też członkiem Komitetu Programowego International Symposium on Applied Computing and Computational Sciences. Jest członkiem American Mathematical Society oraz International Association for Cryptographic Research.

Za swoje osiągniecia był nagradzany i wyróżniany. W 1989 r. otrzymał nagrodę Wydziału IV PAN im. T. Hubera. W latach 2002 – 2004 był konsultantem w zakresie kryptologii w Centrum Certyfikacji Centrast S.A. działającego z ramienia Narodowego Banku Polskiego, a w 2002 r. współuczestniczył w przygotowaniu Ustawy o podpisie elektronicznym. Przez wiele lat był członkiem Komisji oceniającej najlepsze prace magisterskie z zakresu kryptografii prezentowane podczas konferencji ENIGMA poświęconej bezpieczeństwu systemów teleinformatycznych.

Kandydat był recenzentem dwóch rozpraw doktorskich jak też wykonywał recenzje projektów badawczych dla Ministerstwa Nauki i Szkolnictwa Wyższego oraz NCBiR. Ponadto był recenzentem kilkudziesięciu artykułów dla wielu renomowanych czasopism.

3. **Ocena działalności dydaktycznej oraz w zakresie kształcenia kadr**

Działalność dydaktyczna Kandydata związana jest z Uniwersytetem Kazimierza Wielkiego w Bydgoszczy, gdzie pracuje od 2007 r. na stanowisku profesora nadzwyczajnego na Wydziale Matematyki, Fizyki i Techniki. Tematyka prowadzonych przez Niego wykładów to rachunek prawdopodobieństwa z elementami statystyki, teoria informacji, bezpieczeństwo systemów teleinformatycznych oraz kryptografia. Prowadzi też Seminarium dyplomowe poświęcone zagadnieniom transmisji danych w sieciach. W ramach seminarium przygotowywane są pod Jego kierownictwem prace dyplomowe magisterskie oraz inżynierskie. Kandydat był promotorem 5-ciu prac magisterskich oraz 20 prac inżynierskich. Aktualnie jest promotorem kilku prac magisterskich w trakcie finalizacji.

Dr hab. Janusz Szczepański był promotorem jednego zakończonego przewodu doktorskiego - obrony pracy zakończyła się wyróżnieniem. Ponadto pod jego opieką przygotowywana jest kolejna praca doktorska, której obrona planowana jest w br.

4. **Ocena działalności organizacyjnej**

Kandydat ma również liczące się osiągnięcia organizacyjne. Przez trzy kadencje (1991, 1993, 1995) pełnił funkcję Sekretarza konferencji „Polish-Swedish Symposium on Mechanics". Od stycznia 2010 r. jest Zastępcą Przewodniczącego Rady Naukowej IPPT PAN oraz pełni funkcję Przewodniczącego Komisji Koordynacyjnej ds. stopni naukowych w IPPT PAN. Był kierownikiem szeregu projektów badawczych krajowych oraz międzynarodowych. Wielokrotnie działał jako ekspert ds. bezpieczeństwa kryptograficznego w różnych komisjach.

5. **Wniosek końcowy**

Podsumowując, chciałbym stwierdzić, że dr hab. Janusz Szczepański posiada obszerny i znaczący dorobek naukowy, a ocena jego dorobku naukowo-dydaktycznego oraz organizacyjnego jest jednoznacznie pozytywna. Prowadzi to do mojej konkluzji, że dorobek Kandydata spełnia wymagania warunkujące uzyskanie tytułu naukowego profesora wynikające z *Ustawy o stopniach naukowych i tytule naukowym oraz stopniach i tytule w zakresie sztuki* z dnia 14 marca 2003 r. i na tej podstawie odnośny wniosek popieram.