Образац 3.

Факултет Машински

УНИВЕРЗИТЕТ У БЕОГРАДУ

663/5
(Број захтева)

Веће научних области техничких наука
(Назив већа научне области коме се захтев упућује)

23.6.2022.
(Датум)

З А Х Т Е В

за давање сагласности на одлуку о прихватању теме докторске дисертације и о одређивању ментора

Молимо да, сходно члану 47. ст. 5. тач. 3. Статута Универзитета у Београду ("Гласник Универзитета", број 186/15-пречишћени текст и 189/16), дате сагласност на одлуку о прихватању теме докторске дисертације:

„ДЕТЕКЦИЈА КИБЕРНЕТСКИХ НАПАДА НА СИСТЕМЕ ЗА УПРАВЉАЊЕ ПРОИЗВОДНИМ РЕСУРСИМА“
(пун назив предложене теме докторске дисертације)

НАУЧНА ОБЛАСТ Машинство

ПОДАЦИ О КАНДИДАТУ:

1. Име, име једног од родитеља и презиме кандидата:
   ДУШАН (МОМИР) НЕДЕЉКОВИЋ
2. Претходно образовање (назив и седиште факултета, студијски програм):
   Машински факултет Београд
3. Година завршетка претходног нивоа студија: 2016.
4. Година уписа на докторске студије: 2017.
5. Назив студијског програма докторских студија: Машинско инжењерство

ПОДАЦИ О МЕНТОРУ:

Име и презиме ментора:_____Живана Јаковљевић_____

Звање:____ редовни професор_____

Списак радова који квалификују ментора за вођење докторске дисертације:

1. Jakovljevic, Z., Lesi, V., Pajic, M., Attacks on Distributed Sequential Control in Manufacturing Automation, IEEE Transactions on Industrial Informatics, Vol. 17, No. 2 , pp 775-786, 2021, ISSN: 1551-3203, DOI: 10.1109/TII.2020.2987629. (M21a, IF(2020): 10.215, 1/49)
2. Jakovljevic, Z., Puzovic, R., Pajic, M., Recognition of Planar Segments in Point Cloud based on Wavelet Transform, IEEE Transactions on Industrial Informatics, Vol. 11, No. 2 , pp 342-352, 2015, ISSN: 1551-3203, DOI: 10.1109/TII.2015.2389195, (M21a, IF(2015): 4.880, 3/59)
3. Nedeljkovic, D., Jakovljevic, Z., CNN based method for the development of cyber-attacks detection algorithms in industrial control systems. Computers and Security, 114, paper no. 102585, 2022, ISSN: 0167-4048, DOI:10.1016/j.cose.2021.102585. (M21, IF(2020): 4.438, 40/162)
4. Lesi, V., Jakovljevic, Z., Pajic, M., Security analysis for distributed IoT-based industrial automation, IEEE Transactions on Automation Science and Engineering, 2021, ISSN: 1545-5955, DOI:10.1109/TASE.2021.3106335. (M21, IF(2020): 5.083, 16/62)
5. Jakovljevic, Z., Lesi, V., Mitrovic, S., Pajic, M., Distributing Sequential Control for Manufacturing Automation Systems, IEEE Transactions on Control Systems Technology, vol. 28, no. 4, pp. 1586-1594, 2020, ISSN: 1063-6536, DOI: 10.1109/TCST.2019.2912776, (M21, IF(2018): 5.312, 10/63)
6. Sokac, M., Budak, I., Katic, M., Jakovljevic, Z., Santosi, Z., Vukelic, Dj., Improved surface extraction of multi-material components for single-source industrial X-ray computed tomography, Measurement, Vol. 153, Article 107438, 2020, ISSN 0263-2241, DOI: 10.1016/j.measurement.2019.107438, (M21, IF(2019): 3.364, 22/91)
7. Jakovljevic, Z., Petrovic, P., B., Mikovic, V., Dj., Pajic, M., Fuzzy inference mechanism for recognition of contact states in intelligent robotic assembly, Journal of Intelligent Manufacturing, Vol. 25, No. 3, pp 571-587, 2014, ISSN: 0956-5515 DOI 10.1007/s10845-012-0706-x, (M21, IF(2014): 1.731, 10/40)
8. Milkovic D., Simic G., Jakovljevic Z., Tanaskovic J., Lucanin V., Wayside system for wheel-rail contact forces measurements, Measurement, Vol. 46 No. 9, pp. 3308-3318, 2013, ISSN: 0263-2241, doi: 10.1016/j.measurement.2013.06.017, (M21, IF(2013): 1.526, 19/87)
9. Markovic, V., Jakovljevic, Z., Budak, I., Automatic recognition of cylinders and planes from unstructured point clouds, Visual Computer, 2021, ISSN: 0178-2789 doi:10.1007/s00371-021-02299-9. (M22, IF(2020): 2.601, 39/108)
10. Jakovljevic Z., Petrovic P., B., Milkovic D. D., Pajic M., Diagnosis of irregularities in the robotized part mating process based on contextual recognition of contact states transitions, Assembly Automation, Vol. 35 No. 2, pp. 190-199, 2015, ISSN: 0144-5154, DOI: 10.1108/AA-10-2014-077 (M22, IF(2015): 1.225, 34/59)

Обавештавамо вас да је Наставно – научно веће на седници одржаној 23.06.2022. године размотрил предложену тему и закључило да је тема подобна за израду докторске дисертације јер садржи оригиналну идеју и да је од значаја за развој науке, примену њених резултата, односно развој научн мисли уопште.

ДЕКАН ФАКУЛТЕТА

_____

Прилог:

1. Одлука Наставно-научног већа о прихватању теме и одређивању ментора.
2. Извештај Комисије о оцени научне заснованости теме докторске дисертације

Напомена: Факултет доставља Универзитету захтев са прилозима у електронској форми и једном писаном примерку за архиву Универзитета

УНИВЕРЗИТЕТ У БЕОГРАДУ
- МАШИНСКИ ФАКУЛТЕТ -
Број: 663/6
Датум: 23.06.2022. године
Београд, Краљице Марије 16

На основу захтева студента **Душана Недељковића,** маст. инж. маш., бр. 663/1 од 27.04.2022. године да му се одобри израда докторске дисертације, реферата Комисије у саставу: др Бојан Бабић, ред. проф., др Зоран Миљковић, ред. проф., др Никола Славковић, ванр. проф., др Милица Петровић, ванр. проф. и др Младен Николић, ванр. проф., Универзитет у Београду, Математички факултет број 663/5 од 17.06.2022. године, а на основу члана 30. Закона о високом образовању („Службени гласник РС“, број 76/2005, 100/2007 – аутентично тумачење, 97/2008, 93/2012 и 89/2013), члана 64. Статута Машинског факултета – пречишћени текст (број 1136/4 од 28.06.2021. године) и члана 30. Правилника о докторским студијама Машинског факултета, Наставно-научно веће Машинског факултета на седници од 23.06.2022. године, донело је следећу

О Д Л У К У

Прихвата се научна заснованост теме докторске дисертације и констатује да студент **ДУШАН НЕДЕЉКОВИЋ,** маст. инж. маш. испуњава услове за израду докторске дисертације **«ДЕТЕКЦИЈА КИБЕРНЕТСКИХ НАПАДА НА СИСТЕМЕ ЗА УПРАВЉАЊЕ ПРОИЗВОДНИМ РЕСУРСИМА»**.

Одлуком ННВ број 663/4, од 02.06.2022. године за ментора докторске дисертације **ДУШАНА НЕДЕЉКОВИЋА**, маст. инж. маш. именована је др Живана Јаковљевић, ред. проф.

Одлуку доставити: Већу научних области техничких наука Универзитета у Београду, ментору и архиви Факултета.

ДЕКАН
МАШИНСКОГ ФАКУЛТЕТА

проф. др Владимир Поповић

УНИВЕРЗИТЕТ У БЕОГРАДУ
МАШИНСКИ ФАКУЛТЕТ

ВЕЋУ ДОКТОРСКИХ СТУДИЈА

Овде

Предмет: Реферат Комисије за оцену научне заснованости теме докторске дисертације **Душана Недељковића, маст.инж.маш.** по одлуци Наставно-научног већа број 663/3 од 02.06.2022. године.

На основу поднете пријаве за израду докторске дисертације кандидата Душана Недељковића, маст.инж.маш, број 663/1 од 27.04.2022. године, дате сагласности Колегијума наставника Катедре за производно машинство број 663/2 од 11.05.2022. године и Одлуке Наставно-научног већа Машинског факултета Универзитета у Београду број 663/3 од 02.06.2022. године именовани смо за чланове Комисије за подношење реферата о теми докторске дисертације кандидата **Душана Недељковића, маст.инж.маш.**

Увидом у документацију, коју је докторанд Душан Недељковић, маст.инж.маш. приложио уз свој захтев за израду докторске дисертације, после разматрања, Комисија подноси следећи

Р Е Ф Е Р А Т

о теми докторске дисертације
под насловом

Детекција кибернетских напада на системе за управљање производним ресурсима

1. ПОДАЦИ О КАНДИДАТУ

1.1 Општи биографски подаци

Душан (Момир) Недељковић, маст.инж.маш. рођен је 03. децембра 1992. године у Аранђеловцу, Република Србија. Основну школу „Светолик Ранковић“ и средњу школу „Техничка школа – Милета Николић“ завршио је у Аранђеловцу као одличан ђак.

На Машински факултет Универзитета у Београду уписао се школске 2011/2012. године. Основне академске студије Машинско инжењерство завршио је 2014. године одбранивши завршни рад (B.Sc.) са оценом 10 (десет) из предмета CAD/CAM системи и просечном оценом током Основних академских студија 8,48 (осам и 48/100). Школске 2014/2015. године уписао је Мастер академске студије Машинско инжењерство на Модулу за производно машинство, а завршио их је 2016. године са просечном оценом 9,75 (девет и 75/100) одбранивши мастер рад (MSc) на тему „Интерфејс човек-машина за одабране производне ресурсе" из предмета Аутоматизација производње, под менторством проф. др Живане Јаковљевић са оценом 10 (десет).

Након дипломирања кандидат започиње радни однос у компанији Сервотех д.о.о. као машински инжењер – пројектант. Школске 2017/2018. године, уписао је Докторске студије на Машинском факултету Универзитета у Београду (број индекса Д13/17). Током првог семестра Докторских студија утврђени су његови правци научноистраживачког рада на Катедри за производно машинство, да би Одлуком број 271/1 од 31.01.2018. године био озваничен и Програм усавршавања, који се реализује под руководством потенцијалног ментора проф. др Живане Јаковљевић. Кандидат је положио све испите на Докторским студијама и тренутно је студент VI семестра.

Од 19. јануара 2018. године запослен је на Машинском факултету у Београду у звању асистента на Катедри за производно машинство. Кандидат је од 1. фебруара 2018. ангажован на пројекту Технолошког развоја под називом „Иновативни приступ у примени интелигентних технолошких система за производњу делова од лима заснован на еколошким принципима“ који финансира Министарство просвете, науке и технолошког развоја Републике Србије (ев. бр. ТР-35004, руководилац пројекта проф. др Бојан Бабић), закључно са 31. децембром 2019. године. Након тога, кандидат је од 1. јануара 2020. ангажован на пројекту под називом „Интегрисана истраживања у области макро, микро и нано машинског инжењерства – Дубоко машинско учење интелигентних технолошких система у производном машинству“, који је финансиран од стране Министарства просвете, науке и технолошког развоја Владе Републике Србије према уговору о реализацији и финансирању научноистраживачког рада НИО у 2020. години (ев. бр. 451-03-68/2020-14/200105, руководилац пројекта проф. др. Радивоје Митровић), у 2021. години (ев. бр. 451-03-9/2021-14/200105, руководилац пројекта проф. др. Радивоје Митровић) и у 2022. години (ев. бр. 451-03-68/2022-14/200105, руководилац пројекта проф. др. Владимир Поповић). Поред тога, кандидат је од 1. септембра 2020. године ангажован и на пројекту под називом „*Deep Machine Learning and Swarm Intelligence-based Optimization Algorithms for Control and Scheduling of Cyber-Physical Systems in Industry 4.0*“ (акроним - MISSION4.0, ев. бр. 6523109, руководилац пројекта проф. др Зоран Миљковић), који финансира Фонд за науку Републике Србије у оквиру позива „Програм за развој пројеката из области вештачке интелигенције“. Кандидат је у периоду од 15.12.2021-15.03.2022. године боравио на Дјук Универзитету (енгл. *Duke University*) из Дурхама, САД у оквиру Erasmus+ КА107 пројекта размене студената. У том периоду, кандидат је био укључен у активности Лабораторије за кибернетско-физичке системе (енгл. *Cyber-Physical Systems Lab*) чији је руководилац проф. др Мирослав Пајић.

За постигнуте резултате, током похађања основних и мастер академских студија, добио је следеће похвале:

2016-2017. Похвала поводом Дана Машинског факултета у Београду за одличан успех постигнут на трећој години Основних академских студија и првој години Мастер академских студија (школска 2013/14. и 2014/15. година).

Од пролећног семестра школске 2017/2018. године, кандидат је активно укључен у наставни процес Катедре за производно машинство Машинског факултета Универзитета у Београду. Кандидат реализује лабораторијске вежбе, преглед самосталних задатака и преглед пројеката на следећим наставним предметима Катедре:

- Компјутерска графика (ОАС Машинско инжењерство): 2018-...
- Технологија машинске обраде (ОАС Машинско инжењерство): 2018-...
- CAD/CAM системи (ОАС Машинско инжењерство): 2018-2020.
- Аутоматизација производње (МАС Машинско инжењерство): 2018-...
- Рачунарски интегрисани системи и технологије (МАС Машинско инжењерство): 2018-...

- Компјутерска симулација у аутоматизацији производње (МАС Машинско инжењерство): 2018-...
- Програмабилни системи управљања (МАС Машинско инжењерство): 2018-2021.
- Кибернетско физички системи (МАС Индустрија 4.0): 2020-...
- Индустријски интернет ствари и сајбер безбедност (МАС Индустрија 4.0): 2021-...

Познавање страних језика

- Енглески језик – говори, чита и пише.

Познавање рада на рачунару

- Напредно коришћење програма: Python, Matlab, C/C++, Creo Parametric, AnyLogic, Arena, CorelDRAW, LaTeX, Microsoft Office (Word, Excel, PowerPoint, Visio)

Истраживачке области

- Аутоматизација производње, Дистрибуирани ситеми управљања, Кибернетско физички системи, Сајбер безбедност, Машинско учење

Остало

- Поседује возачку дозволу Б категорије

1.2 Активности на Докторским студијама

Кандидат Душан Недељковић, маст.инж.маш. уписао је Докторске студије на Машинском факултету у Београду школске 2017/2018. године. У циљу реализације Програма усавршавања, положио је следеће обавезне и изборне предмете:

Први семестар Докторских академских студија

Назив предмета	**Предметни наставник**	**ЕСПБ**	**Оцена**
Виши курс математике (о)*	Проф. др Слободан Радојевић	5	10 (десет)
Нумеричке методе (о)*	Проф. др Миодраг Спалевић	5	10 (десет)
ОМНИР (организација и методе научно - истраживачког рада) и комуникација (о)*	Проф. др Милош Недељковић	5	9 (девет)
Аквизиција и обрада експерименталних података (и)*	Проф. др Живана Јаковљевић	5	10 (десет)
Истраживање и публиковање - I	Проф. др Живана Јаковљевић	10	10 (десет)

Други семестар Докторских академских студија

Назив предмета	Предметни наставник	ЕСПБ	Оцена
Одабрана поглавља из механике (о)*	Проф. др Зоран Митровић	5	9 (девет)
Аутономни системи и машинско учење (и)*	Проф. др Зоран Миљковић	5	10 (десет)
Биолошки инспирисани алгоритми оптимизације (и)*	Проф. др Милица Петровић	5	10 (десет)
Истраживање и публиковање - II	Проф. др Живана Јаковљевић	15	10 (десет)

Трећи семестар Докторских академских студија

Назив предмета	Предметни наставник	ЕСПБ	Оцена
Дигитална обрада нестационарних сигнала (и)*	Проф. др Живана Јаковљевић	5	10 (десет)
Когнитивна роботика (и)*	Проф. др Зоран Миљковић	5	10 (десет)
Истраживање и публиковање - III	Проф. др Живана Јаковљевић	20	10 (десет)

Четврти семестар Докторских академских студија

Назив предмета	Предметни наставник	ЕСПБ	Оцена
Истраживање и публиковање - IV	Проф. др Живана Јаковљевић	8	10 (десет)
Пројекат идеје докторске дисертације	Проф. др Живана Јаковљевић Проф. др Зоран Миљковић Проф. др Радован Пузовић	22	10 (десет)

Напомена: *о** - обавезни предмет; *и** - изборни предмет.

Душан Недељковић је на Докторским студијама положио 4 (четири) обавезна и 5 (пет) изборних предмета (сваки вреди по 5 ЕСПБ бодова) чиме је остварио укупно 45 ЕСПБ бодова. Кроз Истраживање и публиковање I-IV остварио је 53 ЕСПБ бодова. Ови предмети (Истраживање и публиковање I-IV) су обухватили интензивна истраживања и експериментални рад у области дистрибуираног управљања производним ресурсима и сајбер безбедности, чији резултати су верификовани објављивањем низа радова. Уз то, кандидат је учествовао у извођењу наставе на предметима Катедре за производно машинство. Душан Недељковић је успешно написао и одбранио Пројекат идеје докторске дисертације, што је Комисија у саставу проф. др Живана Јаковљевић, проф. др Зоран Миљковић и проф. др Радован Пузовић потврдила оценом 10 (десет), а тиме је кандидат стекао још 22 ЕСПБ бода. Дакле, у складу са чланом 25. Правилника о Докторским студијама

Машинског факултета у Београду, кандидат је остварио укупно 120 ЕСПБ бодова, чиме је испунио основни услов да пријави докторску дисертацију.

1.3 Списак објављених научних радова и других релевантних резултата и активности које опредељују афинитет кандидата за рад на предложеној теми

Као резултат истраживања кандидат је објавио 15 радова у часописима и на скуповима међународног и националног значаја:

1. Радови објављени у тематском зборнику водећег међународног значаја

[1] Jakovljević, Ž., **Nedeljković, D.**, *Cyber Physical Systems in Manufacturing Engineers Education*, 11th International Conference on Machine and Industrial Design in Mechanical Engineering, Scopus indexed book of the Springer Series Mechanisms and Machine Science, with the title Machine and Industrial Design in Mechanical Engineering – Proceedings of KOD 2021, (eISBN: 978-3-030-88465-9), DOI: 10.1007/978-3-030-88465-9, https://www.springer.com/gp/book/9783030884642, 2021 → **M13**

2. Радови објављени у научним часописима међународног значаја

[2] **Nedeljkovic, D.**, Jakovljevic, Z., *CNN based method for the development of cyber-attacks detection algorithms in industrial control systems*, Computers & Security, Vol. 114, Article 102585, 2022, ISSN 0167-4048, DOI: https://doi.org/10.1016/j.cose.2021.102585 → **M21**, IF(2020)=4.438

3. Рад у часопису међународног значаја верификованом посебном одлуком

[3] **Nedeljković, D.**, Jakovljević, Ž., Miljković, Z., *The detection of sensor signal attacks in industrial control systems*, FME Transactions, Vol. 48, No. 1, pp. 7-12, 2020. → **M24**

4. Радови саопштени на скуповима међународног значаја, штампани у целини

[4] **Nedeljković, D.**, Jakovljević, Ž., *Implementation of CNN based algorithm for cyber-attacks detection on a real-world control system*, in 14th International Scientific Conference MMA 2021 – Flexible Technologies, pp. 119-122 (ISBN 978-86-6022-364-9), Novi Sad, Serbia, 2021. → **M33**

[5] Jakovljevic, Z., **Nedeljkovic, D.**, *Distribution of Control Tasks to Smart Devices in Industrial Control Systems: a Case Study*, in 8th International Conference on Electrical, Electronics and Computing Engineering (IcETRAN 2021), pp. 585-590 (ISBN: 978-86-7466-894-8), Bijeljina, B&H, 2021. → **M33**

[6] **Nedeljković, D.**, Jakovljević, Ž., *Integration of Smart Vision Sensor into Manipulator Control System using OPC-UA*, in 28th Telecommunications Forum (TELFOR 2020), art. 4734, (ISBN: 978-0-7381-4244-9, eISBN: 978-0-7381-4243-2), Belgrade, Serbia, 2020. → **M33**

[7] **Nedeljković, D.**, Jakovljević, Ž., *Integration of Smart Vision Sensor into Manipulator Control System using OPC-UA*, in 28th Telecommunications Forum (TELFOR 2020), art. 4734, (ISBN: 978-0-7381-4244-9, eISBN: 978-0-7381-4243-2), Belgrade, Serbia, 2020. → **M33**

[8] **Nedeljković, D.**, Jakovljević, Ž., Miljković, Z., Pajić, M., *Detection of cyber-attacks in electro-pneumatic positioning system with distributed control*, in Proceedings of 27th Telecommunications forum (TELFOR 2019), art. 0525 (ISBN: 978-1-7281-4789-5), Belgrade, Serbia, 2019. → **M33**

[9] **Nedeljković, D.**, Kokotović, B., Jakovljević, Ž., *Comparative analysis of Discrete Wavelet Transform and Singular Spectrum Analysis in signal trend identification*, in Proceedings of International

Conference on Innovative Technologies (IN-TECH 2019), pp. 48-51 (ISSN 0184-9069), Belgrade, Serbia, 2019. → **M33**

5. Рад објављен у часопису националног значаја

[10] **Nedeljković, D. M.**, Jakovljević, Ž. B., Miljković, Z. Đ., Pajić, M., *Detection of cyber-attacks in systems with distributed control based on support vector regression*, Telfor Journal, Vol. 12, No. 2, pp. 104-109, 2020 → **M53**

6. Радови саопштени на скуповима националног значаја, штампани у целини

[11] **Недељковић, Д.**, Станојевић, С., Пузовић, Р., Јаковљевић, Ж., *Интеграција производних ресурса у систем за извршавање производње коришћењем OPC-UA*, 13. ЕТИКУМ конференција, стр. 65-68 (ИСБН 978-86-6022-387-8), Нови Сад, Србија, 2021. → **M63**

[12] **Недељковић, Д.**, Јаковљевић, Ж., Миљковић, З., *Класификација слике заснована на примени конволуционих неуронских мрежа*, 42. ЈУПИТЕР конференција, стр. 4.13-4.23, (ИСБН: 978-86-6060-055-6), Београд, Србија, 2020. → **M63**

[13] Јаковљевић, Ж., **Недељковић, Д.**, Шеварлић, Ф., Пузовић, Р., *Комуникација између производних ресурса коришћењем OPC-UA стандарда*, 42. ЈУПИТЕР конференција, стр. 4.1-4.12 (ИСБН: 978-86-6060-055-6), Београд, Србија, 2020. → **M63**

[14] **Nedeljković, D.**, Petrović, M., Jakovljević, Ž., *Comparison of Particle Swarm and Ant Colony Optimization in wireless sensor network routing*, International Scientific Conference ETIKUM 2018, pp. 33-36 (ISBN: 978-86-6022-123-2), Novi Sad, Serbia, 2018. → **M63**

[15] **Недељковић, Д.**, Миловановић, М., Јаковљевић, Ж., *Прототип електропнеуматског система за позиционирање*, 41. ЈУПИТЕР конференција, стр. 4.19-4.24 (ИСБН: 978-86-7083-978-6), Београд, Србија, 2018. → **M63**

7. Техничка и развојна решења – алгоритми, методе и софтвери

1) **Недељковић, Д.**, Јаковљевић, Ж., *Алгоритам за детекцију сајбер напада код енергетски ограничених кибернетско физичких система базиран на дубоком машинском учењу* (нова метода: се односи на решавање проблема детекције сајбер напада на бази сигнала добијених са сензора распоређених унутар постројења. Систем детекције заснован је на моделу који је добијен дубоким машинским учењем). → **M85**

8. Учешће у научно-истраживачким, стручним и образовно-развојним пројектима

1) „*Иновациони приступ у примени интелигентних технолошких система за производњу делова од лима заснован на еколошким принципима*“, Пројекат технолошког развоја који финансира Министарство просвете, науке и технолошког развоја Владе Републике Србије: ТР-35004, руководилац пројекта проф. др Бојан Бабић, Београд, 2011–2021.

2) „*Интегрисана истраживања у области макро, микро и нано машинског инжењерства – Дубоко машинско учење интелигентних технолошких система у производном машинству*“, који је финансиран од стране Министарства просвете, науке и технолошког развоја Владе Републике Србије према уговору о реализацији и финансирању научноистраживачког рада НИО у 2020. години (ев. бр. 451-03-68/2020-14/200105, руководилац пројекта проф. др Радивоје Митровић), у 2021. години (ев. бр. 451-03-9/2021-14/200105, руководилац пројекта проф. др Радивоје

Митровић) и у 2022. години (ев. бр. 451-03-68/2022-14/200105, руководилац пројекта проф. др Владимир Поповић).

3) „*Deep Machine Learning and Swarm Intelligence-based Optimization Algorithms for Control and Scheduling of Cyber-Physical Systems in Industry 4.0*“ (акроним - MISSION4.0), Пројекат финансиран од стране Фонда за науку Републике Србије у оквиру позива „Програм за развој пројеката из области вештачке интелигенције“, ев. бр. 6523109, руководилац пројекта проф. др Зоран Миљковић, Београд, 2020–2022.

1.4. Оцена подобности кандидата за рад на предложеној теми

Кандидат Душан Недељковић, маст.инж.маш. својим досадашњим истраживачким активностима показао је посебну заинтересованост, квалитет и изражену способност за научноистраживачки рад.

Публиковани научни радови у врхунском међународном часопису, часопису међународног значаја верификованог посебном одлуком и у зборницима радова скупова међународног и националног значаја, као и верификовано техничко решење, указују на изразит смисао кандидата да се бави комплексним мултидисциплинарним теоријским и експерименталним научним истраживањима.

Досадашња истраживања и објављени радови кандидата у потпуности припадају ужој научној области производно машинство и то области дистрибуираног управљања производним ресурсима и системима заштите од кибернетских напада и у потпуности су повезани са научном облашћу којој припада предложена тема докторске дисертацијa.

Биографски подаци, објављени научни радови, експериментална истраживања кроз ангажовање на пројектима технолошког развоја (ев. бр. ТР-35004, ев. бр. 451-03-68/2020-14/200105, ев. бр 451-03-9/2021-14/200105 и ев. бр. 451-03-68/2022-14/200105) и пројекту Фонда за науку (ев. бр. 6523109), као и други набројани резултати, према мишљењу Комисије, недвосмислено квалификују Душана Недељковића за самосталан, успешан и ефикасан теоријски и експериментални научноистраживачки рад на предложеној докторској дисертацији.

2. ПРЕДМЕТ, НАУЧНА ОБЛАСТ И ЦИЉ ИСТРАЖИВАЊА

Развој кибернетско-физичких система (енгл. *Cyber-Physical Systems* - CPS) у оквиру којих су физички процеси и прорачунске способности интегрисани кроз интеракцију у реалном времену и њихова имплементација у индустрији доводе до значајних промена у производњи. Механички уређаји се проширују локалним контролерима (енгл. *Local Controller* - LC) који садрже прорачунске и комуникационе модуле и представљају паметне уређаје спремне за интеграцију у индустријски интернет ствари (енгл. *Industrial Internet of Things* - IIoT). Уз примену ових технологија, производни системи и ресурси у оквиру њих представљају CPS који се конфигуришу у облику система система (енгл. *Systems-of-Systems*), где системи мање комплексности (нпр. паметни сензори и актуатори са интегрисаним прорачунским и комуникационим способностима) креирају системе веће комплексности, а функционалност система се остварује кроз њихову интензивну комуникацију. Поред омогућавања једноставне реконфигурације производних система и ресурса и њиховог брзог прилагођавања различитим врстама производа у складу са захтевима тржишта, CPS и на њима заснован IIoT представљају основу за дигитализацију производних процеса.

Уз примену CPS, традиционални централизовани системи управљања репрезентовани кроз пирамиду аутоматизације замењују се дистрибуираним системима управљања у оквиру којих се поједини управљачки задаци расподељују на различите уређаје, а целокупан задатак управљања реализује кроз њихов синхронизовани рад и сталну размену информација коришћењем различитих (ожичених и

бежичних) комуникационих веза. Поред тога, како би се што брже одговорило на захтеве тржишта, поједини подаци се директно из погона коришћењем глобалне мреже у реалном времену стављају на располагање кооперантима тако да ICS више не представљају изолована острва инхерентно отпорна на различите врсте упада. Свеприсутна комуникација између елемената ICS као и њихово повезивање на глобалну мрежу доводи до опасности везаних за кибернетске нападе од стране различитих противника. Потребно је нагласити да кибернетски напади на ICS поред економских последица и катастрофалних оштећења опреме могу за последицу имати негативне утицаје на животну средину као и последице везане за безбедност на раду, које чак могу бити фаталне по живот човека. Имајући у виду наведено, као и неопходност функционисања ICS у реалном времену, захтеви који се постављају пред системе заштите од кибернетских напада у оквиру ICS се значајно разликују у односу на системе у оквиру општих информационих технологија. За разлику од општих информационих технологија у оквиру којих је најзначајнија поверљивост података, код ICS њихова расположивост и интегритет су круцијални. У складу са наведеним, у оквиру ICS неопходно је увођење посебних система заштите познатих под називом дубинска одбрана (енгл. *Defense-in-Depth*). Концепт дубинске одбране подразумева да се поред вишеслојних заштитних механизама кроз сегментацију и сегрегацију мреже уводе и системи за детекцију напада (енгл. *Intrusion Detection Systems* - IDS) који се имплементирају на самом уређају који прима податке коришћењем комуникационих веза. Улога IDS је да препознају напад ако он заобиђе претходне линије одбране и то пре него што напад постигне жељене ефекте.

Предмет истраживања ове дисертације представљају системи за детекцију кибернетских напада у оквиру индустријских система управљања. У фокусу истраживања биће методе за креирање IDS за системе са континуалним управљањем. Имајући у виду специфичности система са централизованим и дистрибуираним управљањем, а које се пре свега односе на прорачунске способности уређаја који се користе у овим системима као и начин њиховог напајања (мрежно или батеријско), ове две врсте система управљања ће бити посебно разматране. При том ће један од кључних циљева бити очување потпуне функционалности индустријских система управљања пре свега узимајући у обзир неопходност њиховог рада у реалном времену и кашњења која имплементација IDS инхерентно узрокује.

Научни циљ дисертације је развој методологије за креирање алгоритама који представљају основе система за детекцију кибернетских напада у оквиру индустријских система управљања. Методологија треба да обухвати системе са континуалним управљањем и то са централизованом и дистрибуираном архитектуром.

Основни циљеви истраживања јесу:

1. Развој метода за генерисање модела података који се размењују између уређаја у нормалним условима рада (без напада) и то како за системе из којих је могуће прикупити довољну количину података, тако и за системе из којих је количина података која се може прикупити ограничена;
2. Развој метода заснованих на принципима полу-надгледаног учења за креирање система за детекцију напада на комуникационе везе између CPS у оквиру система за континуално управљање производним ресурсима узимајући у обзир архитектуру система управљања и могућност имплементације алгоритма за детекцију напада на неком од уређаја у оквиру система;
3. Развој методе за аутоматски избор алгоритма (укључујући и све његове параметре) за детекцију напада на комуникационе везе између CPS који ће се ефикасно користити у процесу детекције напада у реалном систему;
4. Верификација развијених метода на јавно доступним скуповима података и скуповима података добијених са експерименталне инсталације;

5. Имплементација и експериментална верификација система за детекцију напада генерисаних коришћењем развијених метода на креираној лабораторијској инсталацији.

Сајбер безбедност у оквиру индустријских система управљања представља релативно нову истраживачку област која је замах добила од 2010. године након *Stuxnet* напада на иранско нуклеарно постројење [1]. Последњих година извршена су иницијална истраживања у области и публикован је одређен број запажених научних радова који са разних становишта третирају развој система за детекцију кибернетских напада и базирани су на различитим техникама и принципима. Садржај ових радова се анализира у наставку. Поред литературних извора који се односе на креирање IDS, неопходан основ за развој нових метода у оквиру ове дисертације представљају и напредне технике за обраду сигнала, статистичке методе и технике машинског учења и вештачке интелигенције. Неки од литературних извора на које се ослања ова докторска дисертација су:

[1] Bakić, B., Milić, M., Antović, I., Savić, D., Stojanović, T., *10 years since Stuxnet: What have we learned from this mysterious computer software worm?*, In 2021 25th International Conference on Information Technology (IT), pp. 1-4, IEEE, February, 2021.

[2] Sánchez, H.S., Rotondo, D., Escobet, T., Puig, V., Quevedo, J., *Bibliographical review on cyber attacks from a control oriented perspective*, Annual Reviews in Control, Vol. 48, pp.103-128, 2019.

[3] Tantawy, A., Abdelwahed, S., Erradi, A., Shaban, K., *Model-based risk assessment for cyber physical systems security*, Computers & Security, Vol. 96, Article 101864, 2020.

[4] Jakovljevic, Z., Lesi, V., Pajic, M., *Attacks on distributed sequential control in manufacturing automation*, IEEE Transactions on Industrial Informatics, Vol. 17, No. 2, pp. 775-786, 2020.

[5] Wang, Y., Li, Y., Yu, Z., Wu, N., Li, Z., *Supervisory control of discrete-event systems under external attacks*, Information Sciences, Vol. 562, pp. 398-413, 2021.

[6] Pasqualetti, F., Dörfler, F., Bullo, F., *Attack detection and identification in cyber-physical systems*, IEEE transactions on automatic control, Vol. 58, No. 11, pp. 2715-2729, 2013.

[7] Teixeira, A., Shames, I., Sandberg, H., Johansson, K., *A secure control framework for resource-limited adversaries*, Automatica, Vol. 51, pp.135-148, 2015.

[8] Smola, A. J., Schölkopf, B., *A tutorial on support vector regression*, Statistics and Computing, Vol. 14, No. 3, pp. 199–222, 2004.

[9] Goodfellow, I., Bengio, Y., Courville, A., *Deep learning*. MIT press, 2016.

[10] Elman, J., *Finding Structure in Time*, Cognitive Science, Vol. 14, No. 2, pp. 179-211, 1990.

[11] Hochreiter, S., Schmidhuber, J., *Long short-term memory*, Neural Computation, Vol. 9, No. 8, pp. 1735–1780, 1997.

[12] Chung, J., Gulcehre, C., Cho, K., Bengio, Y., *Empirical evaluation of gated recurrent neural networks on sequence modeling*, arXiv preprint, 2014, doi: https://doi.org/10.48550/arXiv.1412.3555

[13] Elnour, M., Meskin, N., Khan, K., Jain, R., *A dual-isolation-forests-based attack detection framework for industrial control systems*, IEEE Access, Vol. *8*, pp. 36639-36651, 2020.

[14] Mishra, P., Varadharajan, V., Tupakula, U., Pilli, E.S., *A detailed investigation and analysis of using machine learning techniques for intrusion detection*, IEEE Communications Surveys & Tutorials, Vol. 21, No. 1, pp. 686-728, 2018.

[15] Priyanga, S., Krithivasan, K., Pravinraj, S., Shankar, S., *Detection of Cyberattacks in Industrial Control Systems Using Enhanced Principal Component Analysis and Hypergraph-Based Convolution Neural Network (EPCA-HG-CNN)*, IEEE Transactions on Industry Applications, Vol. 56, pp. 4394-4404, 2020.

[16] Sapkota, S., Mehdy, A., Reese, S., Mehrpouyan, H., *Falcon: Framework for anomaly detection in industrial control systems*, Electronics, Vol. *9, No.* 8, pp. 1-20, 2020.

[17] Das, T., Adepu, S., Zhou, J., *Anomaly detection in industrial control systems using logical analysis of data*, Computers & Security, Vol. *96*, Article 101935, 2020.

[18] Al-Abassi, A., Karimipour, H., Dehghantanha, A., Parizi, R.M., *An ensemble deep learning-based*

cyber-attack detection in industrial control system, IEEE Access, Vol. *8*, pp. 83965-83973, 2020.

[19] Goh, J., Adepu, S., Tan, M., Lee, Z. S., *Anomaly detection in cyber physical systems using recurrent neural networks*, In 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), pp. 140-145, IEEE, January, 2017.

[20] Inoue, J., Yamagata, Y., Chen, Y., Poskitt, C. M., Sun, J., *Anomaly detection for a water treatment system using unsupervised machine learning*, In 2017 IEEE International Conference on Data Mining Workshops (ICDMW), pp. 1058-1065, IEEE, November, 2017.

[21] Kravchik, M., Shabtai, A., *Detecting cyber attacks in industrial control systems using convolutional neural networks*, In Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy, pp. 72-83, January, 2018.

[22] Kravchik, M., Shabtai, A., *Efficient cyber attack detection in industrial control systems using lightweight neural networks and pca*, IEEE Transactions on Dependable and Secure Computing, 2021, doi: 10.1109/TDSC.2021.3050101

[23] Raman MR, G., Somu, N., Mathur, A., *A multilayer perceptron model for anomaly detection in water treatment plants*, International Journal of Critical Infrastructure Protection, Vol. 31, Article 100393, 2020.

[24] Lin, Q., Adepu, S., Verwer, S., Mathur, A., *TABOR: A graphical model-based approach for anomaly detection in industrial control systems*, In Proceedings of the 2018 on asia conference on computer and communications security, pp. 525-536, May, 2018.

[25] Aoudi, W., Iturbe, M., Almgren, M., *Truth will out: Departure-based process-level detection of stealthy attacks on control systems*, In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 817-831, October, 2018.

[26] Luo, Y., Xiao, Y., Cheng, L., Peng, G., Yao, D., *Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities*, ACM Computing Surveys, Vol. 54, No. 5, pp. 1-36, 2021.

[27] Erhan, L., Ndubuaku, M., Di Mauro, M., Song, W., Chen, M., Fortino, G., Bagdasar, O., Liotta, A., *Smart anomaly detection in sensor systems: A multi-perspective review*, Information Fusion, Vol. 67, pp. 64-79, 2021.

Методе за детекцију напада у оквиру ICS засноване су на одступању података примљених комуникационом везом од података добијених на основу модела рада система у нормалним условима (без напада) и у зависности од приступа генерисању модела рада система могу се сврстати у методе засноване на дизајну система управљања и методе засноване на подацима [2].

У приступу заснованом на дизајну, за генерисање модела система са дискретним догађајима коришћени су различити алати, као што су формалне методе попут коначних аутомата [3], теорија надзорног управљања [4] и Петријевих мрежа [5] са више или мање успеха. Код система са континуалним управљањем, с друге стране, истраживана је употреба аналитичких модела [6, 7], али је, због ограничења везаних за аналитички опис, примена оваквих метода ограничена на системе мале комплексности.

С друге стране, приступи засновани на подацима били су у фокусу бројних истраживачких радова који су за развој IDS-а користили различите технике машинског учења [8, 9, 10, 11, 12] пре свега код система са континуалним управљањем. Ови приступи се могу класификовати у три главне категорије у зависности од података и начина на који се они користе током обучавања модела: надгледани (користе се подаци прикупљени током нормалног рада система и подаци прикупљени током напада са назнаком којој групи подаци припадају), полу-надгледани (користе се само подаци прикупљени током нормалног рада система) и ненадгледани (користе се подаци прикупљени током нормалног рада система и подаци прикупљени током напада, без назнаке којој групи припадају) [13, 14].

У референтним радовима који се баве надгледаним учењем, за креирање модела система коришћене су различите технике: конволуционе неуронске мреже (енгл. *Convolutional Neural*

Networks - CNN) и анализа главних компоненти (енгл. *Principal Component Analysis* - PCA) [15], комбинација CNN и рекурентних неуронских мрежа (енгл. *Recurrent Neural Networks* - RNN) [16], логичка анализа података [17], аутоенкодери, дубоке неуронске мреже и стабла одлучивања [18]. Иако надгледани приступи неретко дају добре резултате над скуповима за тестирање, велики недостатак њихове примене представља изузетно мала способност генерализације развијених класификатора на процесе и сценарије напада који нису коришћени током обучавања. Сличне карактеристике имају и системи добијени техникама ненадгледаног учења.

Како је у оквиру ICS-а по правилу могуће генерисати довољну количину података у нормалном раду, механизми за детекцију напада базирани на полу-надгледаном учењу привукли су највише пажње. У бројним истраживачким радовима разматране су различите архитектуре дубоког учења: RNN [19, 20], CNN [20, 21], аутоенкодери [22], вишеслојни перцептрон [23]. Поред дубоког учења, развијени су и други алгоритми за детекцију напада засновани на графичком приступу који комбинује Бајесове мреже и временске аутомате (енгл. *time automata*) [24] и приступу који користи анализу сингуларног спектра [25].

Иако су кроз наведене истраживачке радове остварени одређени резултати, у њима се може идентификовати низ недостатака који су изузетно значајни са аспекта практичне имплементације на реалним системима и у реалном времену [14, 26, 27]. По правилу, у анализираним литературним изворима предлаже се један, ручно изабран, модел са одређеном архитектуром који је креиран за разматрани систем и чија је имплементација у другим системима упитна. Поред параметара модела, у оквиру постојећих метода ручно се одређују и остали параметри попут прагова за детекцију напада и то на основу сигнала са нападима што поставља питање способности генерализације метода на сценарије напада који нису разматрани, слично као у случају метода заснованих на надгледаном и ненадгледаном учењу. Још један недостатак досадашњих приступа је што они не узимају у обзир архитектуру система управљања и за велики број система не постоји уређај у оквиру система управљања на коме се он може применити. Овде је потребно нагласити да су по правилу методе реализоване коришћењем јавно расположивих скупова података и да за њих није извршена експериментална верификација.

3. ОСНОВНЕ ХИПОТЕЗЕ

На основу знања и вештина акумулираних досадашњим истраживањима и детаљне анализе релевантних литературних извора у области детекције кибернетских напада на индустријске системе управљања с једне и у областима обраде сигнала и машинског учења с друге стране, а узимајући у обзир архитектуру управљачких система и тренутне потребе индустрије за системима за детекцију кибернетских напада, дефинишу се следеће полазне хипотезе у оквиру ове дисертације:

Хипотеза 1:
Ауто-регресиони модели података чија се комуникација врши између елемената система управљања дистрибуираних на паметне уређаје, а који су креирани коришћењем техника машинског и дубоког учења, могу представљати основу за креирање система за детекцију напада на комуникационе везе у оквиру система управљања производним ресурсима.

Хипотеза 2:
Из фамилије ауто-регресионих модела података чија се комуникација врши између елемената система управљања могуће је аутоматски одабрати модел као и све остале параметре алгоритма за детекцију напада заснованог на том моделу који ће се ефикасно користити у процесу детекције напада у реалном систему узимајући у обзир архитектуру система управљања.

Хипотеза 3:

Применом алгоритма за детекцију напада заснованих на машинском и дубоком учењу могуће је у реалном времену у оквиру прорачунски и енергетски ограничених кибернетско-физичких система постићи висок ниво детекције напада не изазивајући притом кашњења које ће угрозити функционалност система.

4. НАУЧНЕ МЕТОДЕ ИСТРАЖИВАЊА

Имајући у виду свеобухватност, комплексност и мултидисциплинарни карактер тематске области, у овој докторској дисертацији планира се коришћење следећих метода:

1. Методе машинског учења засноване на статистичкој теорији учења (пре свега машине са носећим векторима) – користиће се за креирање модела података у току рада система у условима без напада;
2. Методе дубоког машинског учења (пре свега CNN и RNN) – користиће се за креирање модела података у току рада система у условима без напада;
3. Генеративне супарничке мреже (енгл. *Generative Adversarial Networks* - GAN) – користиће се за проширивање скупа података за системе из којих је количина података која се може прикупити ограничена;
4. Методе за обраду сигнала у реалном времену – користиће се за претпроцесирање сигнала прикупљених са комуникационих веза у оквиру система управљања;
5. Методе статистичке анализе података – користиће се за анализу експерименталних резултата;
6. Методе за софтверску и хардверску имплементацију алгоритама – користиће се приликом експерименталне верификације.

5. ОЧЕКИВАНИ НАУЧНИ ДОПРИНОС

Научни допринос дисертације припада домену сајбер безбедности у оквиру индустријских система управљања у аутоматизацији производње. На основу полазних хипотеза и уз примену наведених метода, очекивани научни резулати истраживања у оквиру ове дисертације подразумевају:

- Израду нове методологије за креирање алгоритама за детекцију кибернетских напада заснованих на предикцији сигнала добијених из система применом техника машинског и дубоког учења која:
  - Креира алгоритме са релативно малим бројем параметара модела који омогућују ефикасну детекцију напада у реалном времену и на енергетски и прорачунски ограниченим ресурсима,
  - Врши аутоматски избор одговарајућег алгоритма за детекцију кибернетских напада и свих његових параметара што омогућује брзо креирање и имплементацију IDS приликом реконфигурисања производних ресурса и креирања нових ICS,
  - Има могућност примене у централизованим и дистрибуираним ICS узимајућу у обзир њихову архитектуру.

Очекује се да се применом развијене методе за детекцију кибернетских напада оствари висок ниво детекције напада како на сигналима добијеним из јавно доступних скупова података, тако и у случају примене алгоритама на експерименталној инсталацији где се процес одвија у реалном времену. Поред тога, изабрани алгоритми подразумевају релативно ниску прорачунску комплексност, чиме ће се испунити циљ очувања потпуне функционалности ICS приликом њихове примене у реалном времену и на ограниченим ресурсима што отвара нове могућности за заштиту од кибернетских напада у аутоматизацији производње.

6. ПЛАН ИСТРАЖИВАЊА И СТРУКТУРА РАДА

План истраживања, у оквиру предметне докторске дисертације, реализује се кроз следеће фазе:

1. Анализа стања у области сајбер безбедности индустријских система управљања. Анализа постојећих врста кибернетских напада и њихов утицај на ICS;
2. Преглед и критичка анализа литературних извора и претходних истраживања релевантних за различите приступе за детекцију кибернетских напада у ICS са централизованом и дистрибуираном архитектуром, базираних на дизајну система управљања и на подацима;
3. Анализа техника машинског и дубоког машинског учења са аспекта могућности њихове примене у моделирању понашања система у нормалним условима рада (без напада);
4. Развој метода за креирање модела на основу података прикупљених са комуникационих линија између CPS у условима без напада;
5. Развој метода заснованих на принципу полу-надгледаног учења за креирање IDS за нападе на комуникационе везе између CPS;
6. Развој методе за аутоматски избор алгоритма, као и свих његових параметара који ће се користити за детекцију кибернетских напада;
7. Верификација новоразвијених алгоритама за детекцију кибернетских напада на сигналима из јавно доступних скупова података, укључујући и скупове података који су прикупљени са експерименталне инсталације;
8. Тестирање и практична експериментална верификација новоразвијених алгоритама за детекцију кибернетских напада на креираној експерименталној инталацији;
9. Анализа остварених експерименталних резултата и дискусија о будућим правцима развоја.

Оквирна структура предложене докторске дисертације обухвата следеће целине:

1. Увод
    a) ICS – дистрибуирана и централизована архитектура
    b) CPS и њихова улога у ICS
    c) Сајбер безбедност у оквиру ICS
2. Анализа и класификација постојећих врста кибернетских напада
3. Преглед и анализа постојећих метода за детекцију кибернетских напада
    a) Методе засноване на дизајну система управљања
    b) Методе засноване на подацима
4. Развој методологије за креирање алгоритама за детекцију кибернетских напада
    a) Развој методе за генерисање модела заснованог на подацима
    b) Развој методе за креирање IDS
    c) Развој методе за аутоматски избор алгоритма
5. Детекција кибернетских напада у ICS
    a) Верификација развијеног IDS на јавно доступним скуповима података и скуповима података добијених са експерименталне инсталације
    b) Имплементација и експериментална верификација развијеног IDS на креираној лабораторијској инсталацији
6. Закључци
7. Литература
8. Прилози

7. ЗАКЉУЧАК И ПРЕДЛОГ

На основу Одлуке Наставно-научног већа број 663/3 од 02.06.2022. године, за **ментора** кандидата Душана Недељковића, маст.инж.маш. током рада на предметној докторској дисертацији именована је **др Живана Јаковљевић**, редовни професор Универзитета у Београду – Машинског факултета са чиме је Комисија у потпуности сагласна.

На основу анализе пријаве теме докторске дисертације кандидата Душана Недељковића, маст.инж.маш. архиниране под евиденционим бројем 663/1 од 27.04.2022. године, а сходно сагласности Колегијума наставника Катедре за производно машинство број 663/2 од 11.05.2022. године, као и Одлуци Наставно-научног већа број 663/3 од 02.06.2022. године, Комисија за подношење реферата о теми докторске дисертације закључује да је предложена тема научно утемељена и адекватна за израду докторске дисертације високог ранга, као и да кандидат испуњава све законске и суштинске услове који га квалификују за рад на предметној докторској дисертацији. Имајући у виду наведено, Комисија предлаже Већу докторских студија Машинског факултета Универзитета у Београду да се

Душану Недељковићу, маст. инж. маш.

одобри израда докторске дисертације са темом

Детекција кибернетских напада на системе за управљање производним ресурсима

научна област: **машинско инжењерство** (**производно машинство**).

Београд, 10.06.2022. год.

ЧЛАНОВИ КОМИСИЈЕ:

_____

др Бојан Бабић, редовни професор
Универзитет у Београду, Машински факултет

_____

др Зоран Миљковић, редовни професор
Универзитет у Београду, Машински факултет

_____

др Никола Славковић, ванредни професор
Универзитет у Београду, Машински факултет

_____

др Милица Петровић, ванредни професор
Универзитет у Београду, Машински факултет

_____

др Младен Николић, ванредни професор
Универзитет у Београду, Математички факултет

УНИВЕРЗИТЕТ У БЕОГРАДУ
- МАШИНСКИ ФАКУЛТЕТ –
Број: 663/4
Датум: 02.06.2022. године
Београд, Краљице Марије бр.16

На основу члана 64. Статута Машинског факултета Универзитета у Београду – пречишћен текст, арх. бр. 1136/4 од 28.06.2021. године и члана 20. а сагласно члану 29. Правилника о докторским студијама на Универзитету у Београду од 24.05.2016.г., Наставно-научно веће Машинског факултета на седници одржаној дана 02.06.2022. године, донело је следећу

О Д Л У К У

Именује се **др Живана Јаковљевић, ред. проф.** за ментора докторске дисертације **„Детекција кибернетских напада на системе за управљање производним ресурсима“** кандидата **Душана Недељковића, маст. инж. маш.**, студента докторских студија.

Одлуку доставити: ментору, докторанту и архиви.

ДЕКАН
МАШИНСКОГ ФАКУЛТЕТА

проф. др Владимир Поповић