

ИЗВЕШТАЈ О ОЦЕНИ ПОДОБНОСТИ ТЕМЕ, КАНДИДАТА И МЕНТОРА ЗА  
ИЗРАДУ ДОКТОРСКЕ ДИСЕРТАЦИЈЕ

**I ПОДАЦИ О КОМИСИЈИ**

Орган који је именовано комисију: Декан Факултета техничких наука, Универзитет у Новом Саду на основу одлуке Наставно-научног већа Факултета техничких наука, Универзитет у Новом Саду од 012-40/3621-2026

Датум именовања комисије: 28.05.2026.

Састав комисије именоване у складу са *Правилима докторских студија Универзитета у Новом Саду*:

1	Стефановић др Мирослав	доцент	информационо-комуникациони системи
	презиме и име	звање	ужа научна област
	Факултет техничких наука, Универзитет у Новом Саду	председник	
	установа у којој је запослен-а	функција у комисији	
2	Видаковић др Милан	редовни професор	примењене рачунарске науке и информатика
	презиме и име	звање	ужа научна област
	Факултет техничких наука, Универзитет у Новом Саду	члан	
	установа у којој је запослен-а	функција у комисији	
3	Дакић др Душанка	доцент	информационо-комуникациони системи
	презиме и име	звање	ужа научна област
	Факултет техничких наука, Универзитет у Новом Саду	члан	
	установа у којој је запослен-а	функција у комисији	
4	Николић др Данило	доцент	инжењерство информационих система
	презиме и име	звање	ужа научна област
	Факултет техничких наука, Универзитет у Новом Саду	члан	
	установа у којој је запослен-а	функција у комисији	
5	Савић др Душан	ванредни професор	софтверско инжењерство
	презиме и име	звање	ужа научна област
	Факултет организационих наука, Универзитет у Београду	члан	
	установа у којој је запослен-а	функција у комисији	

## II ПОДАЦИ О КАНДИДАТУ

1. Име, име једног родитеља, презиме: Алекса, Зоран, Комосар
2. Датум рођења: 06.10.1999. Место и држава рођења: Приједор, Босна и Херцеговина

### II.1 Основне или интегрисане студије

Година уписа:  Година завршетка:  Просечна оцена током студија:

Универзитет: Универзитет у Новом Саду

Факултет: Факултет техничких наука, Универзитет у Новом Саду

Студијски програм: Инжењерство информационих система

Стечено звање: дипломирани инжењер информационих технологија

### II.2 Мастер или магистарске студије

Година уписа:  Година завршетка:  Просечна оцена током студија:

Универзитет: Универзитет у Новом Саду

Факултет: Факултет техничких наука, Универзитет у Новом Саду

Студијски програм: Инжењерство информационих система

Стечено звање: мастер инжењер информационих технологија

Научна област: ИМТ студије – Информационе технологије

Наслов завршног рада: Истраживање *data literacy* концепта – мерење, развој, иницијативе и примери употребе

### II.3 Докторске студије

Година уписа:

Универзитет: Универзитет у Новом Саду

Факултет: Факултет техничких наука, Универзитет у Новом Саду

Студијски програм: Инжењерство информационих система

Број ЕСПБ до сада остварених:  Просечна оцена током студија:

#### **II.4 Приказ научних и стручних радова кандидата**

Р. бр.	аутори, наслов рада, <i>часопис</i> , <b>волумен</b> (година) странице од-до, DOI или ISBN/ISSN	категирија
1.	<b>A. Komosar</b> , M. Gnjatovic, D. Stefanovic, N. Macek, D. Savic, and T. Vuckovic, 'An Overview of Convolutional Neural Network-Based Static Malware Analysis Techniques', <i>Tehnicki vjesnik - Technical Gazette</i> , <b>Vol. 33/No. 4</b> , 2026, In Press, DOI: 10.17559/TV-20251009003047, (Engineering, Multidisciplinary (90/179); IF 2024 = 1.4)	M22

*Кратак опис садржине:*

Овај рад пружа преглед техника статичке анализе злонамерних софтвера заснованих на конволутивним неуронским мрежама. Разматрају се три истраживачка питања: Које архитектуре засноване на конволутивним неуронским мрежама или повезане са њима се користе у статичкој анализи злонамерних софтвера. Који корпуси се користе као подршка истраживањима у овој области и који су повезани изазови. У којој мери се добијени модели евалуирају. Претражене су три научне базе података - *Scopus*, *Web of Science*, *MDPI*, а ПРИЗМА оквир је коришћен за спровођење и транспарентно представљање 70 радова одабраних према наменским критеријумима укључивања и искључивања. Преглед указује на новији тренд концептуализације злонамерних софтвера као секвенцијалне структуре са локалним и далекододетним зависностима, потребу за преиспитивањем појма уравнотежености корпуса, као и потребу за доследном и транспарентном применом Ф1-мере.

*Рад припада проблематици докторске дисертације:*     ДА            НЕ            ДЕЛИМИЧНО

Р. бр.	аутори, наслов рада, <i>часопис</i> , <b>волумен</b> (година) странице од-до, DOI или ISBN/ISSN	категирија
2.	<b>A. Komosar</b> , S. Kijanovic, V. Mandic, D. Nikolic, and T. Vuckovic, 'ON THE APPLICATION OF STATIC CODE ANALYSIS TOOLS IN THE SERBIAN IT INDUSTRY: AN EMPIRICAL STUDY', in <i>Proceedings of the 17th IADIS International Conference Information Systems 2024</i> , IADIS Press, Aug. 2024. DOI: 10.33965/IS2024_202401L007.	M33

*Кратак опис садржине:*

Брз развој информационих технологија и пораст захтева клијената у области развоја софтверских производа стварају мотивацију за развој и унапређење алата за статичку анализу кода. Циљ овог рада је да испита утицај нивоа сениоритета на мишљење о алатима за статичку анализу кода, као и утицај ових алата на *deployment pipeline*. У раду је представљено емпиријско истраживање засновано на анкети, при чему су питања подељена у три целине које се односе на демографске податке, алате за статичку анализу кода и евалуацију алата. Циљна група били су технички стручњаци запослени у ИТ индустрији у Новом Саду и Београду. Обрада података извршена је коришћењем алата ЈАСП, а за добијање резултата примењени су Пеарсонови тестови. Уочено је да виши ниво сениоритета условљава нижу оцену алата. Поред тога, сви испитаници којима је статичка анализа кода обавезан део *deployment pipeline*-а чешће користе ове алате. На основу тога може се закључити да алати за статичку анализу кода представљају моћно средство које олакшава рад у ИТ индустрији, али да постоји велики број аспеката погодних за унапређење. Комплетна анкета доступна је на захтев.

*Рад припада проблематици докторске дисертације:*     ДА            НЕ            ДЕЛИМИЧНО

Р. бр.	аутори, наслов рада, <i>часопис</i> , <b>волумен</b> (година) странице од-до, DOI или ISBN/ISSN	категирија
3.	<b>A. Komosar</b> , D. Slavic, S. Rakić, and D. Stefanović, 'MAPPING THE INTERSECTION OF CYBERSECURITY AND INDUSTRY 5.0: A BIBLIOMETRIC ANALYSIS', in <i>Proceedings of the INTERNATIONAL Conference on Business, Management, and Economics Engineering Future-BME, 2025</i> , pp. 691–698. DOI: 10.24867/FUTURE-BME-2024-078.	M33

*Кратак опис садржине:*

Индустрија 5.0 представља стратегију усмерену на човека која наглашава сарадњу између људи и напредних технологија. Са друге стране, сајбер безбедност је у основи усмерена на заштиту људи и

<p>њихових интеракција са тим технологијама, посебно у оквиру концепта Индустије 5.0. Све већа дигитализација и ослањање на технологију огледају се у развоју и примени концепата, мера и имплементација сајбер безбедности. Овај рад обухвата пресек Индустије 5.0 и сајбер безбедности, са фокусом на њихову интеграцију и истраживања која из тога проистичу. Рад идентификује најутицајније ауторе и кључне истраживачке области, истиче најважније кључне појмове и анализира земље које остварују највећу продуктивност у области сајбер безбедности у оквиру Индустије 5.0.</p>		
<p><i>Рад припада проблематици докторске дисертације:</i>     <u>ДА</u>     НЕ     ДЕЛИМИЧНО</p>		

Р. бр.	аутори, наслов рада, часопис, волумен (година) странице од-до, DOI или ISBN/ISSN	категирија
4.	D. Slavic, <b>A. Komosar</b> , D. Stefanović, and S. Rakić, 'CYBERSECURITY IN INDUSTRIAL INTERNET OF THINGS AND COLLABORATIVE ROBOTS: INDUSTRY 5.0 PERSPECTIVE', in <i>Proceedings of the INTERNATIONAL Conference on Business, Management, and Economics Engineering Future-BME, 2025</i> , pp. 672–680. DOI: 10.24867/FUTURE-BME-2024-076.	M33
<p><i>Кратак опис садржине:</i>          Индустија 5.0 покреће значајне трансформативне промене у савременом свету. Кроз праксе усмерене на човека, одрживост и отпорност, ове промене одговарају на изазове препознате на глобалном нивоу. У производном сектору долази до преласка са технолошки оријентисане производње на производњу усмерену ка људима. Индустија 5.0 додатно наглашава значај људи, њихову улогу у Индустијском интернету ствари и рад у симбиози са колаборативним роботима. Овакве праксе захтевају прикупљање осетљивих података, због чега јачање и одржавање мера сајбер безбедности у компанијама постаје неопходно. Како би приказали на који начин сајбер безбедност прожима Индустијски интернет ствари и колаборативне роботе, аутори овог рада применили су ПРИСМА оквир. Главни налази рада показују како се сајбер безбедност користи у Индустијском интернету ствари и колаборативним роботима из перспективе Индустије 5.0.</p>		
<p><i>Рад припада проблематици докторске дисертације:</i>     <u>ДА</u>     НЕ     ДЕЛИМИЧНО</p>		

Р. бр.	аутори, наслов рада, часопис, волумен (година) странице од-до, DOI или ISBN/ISSN	категирија
5.	<b>A. Komosar</b> and S. Kijanovic, 'Research on the Application of Open Data in the Public Finance Sector', in <i>Proceedings of the 2023 22nd International Symposium INFOTEH-JAHORINA (INFOTEH)</i> , East Sarajevo, Bosnia and Herzegovina: IEEE, Mar. 2023, pp. 1–6. DOI: 10.1109/INFOTEH57020.2023.10094103.	M33
<p><i>Кратак опис садржине:</i>          Отворени подаци представљају снажан ресурс за развој сектора јавних финансија, стварајући отворено, транспарентно и демократско друштво. Иновацијама у техничкој области уз помоћ отворених података ствара се додатна вредност услуга и производа, не само у јавном већ и у приватном сектору. Фокус рада је на јавном сектору финансија, где се уз помоћ отворених података постиже висок степен транспарентности, који се остварује кроз примере њихове примене. Рад пружа преглед добрих пракси на државном нивоу у Естонији, Ирској, Словенији и Србији, уз коментаре о постигнутим резултатима на основу извештаја светских портала и организација које се баве развојем иницијатива отворених података у сектору јавних финансија.</p>		
<p><i>Рад припада проблематици докторске дисертације:</i>     ДА     <u>НЕ</u>     ДЕЛИМИЧНО</p>		

Р. бр.	аутори, наслов рада, часопис, волумен (година) странице од-до, DOI или ISBN/ISSN	категирија
6.	<b>A. Komosar</b> , S. Koprivica, D. Taibi, A. Ivic, D. Stefanovic, and S. Kijanovic, 'DATA LITERACY MEASUREMENTS: A SYSTEMATIC LITERATURE REVIEW', in <i>Proceedings of the 17th IADIS International Conference Information Systems 2024</i> , IADIS Press, Aug. 2024. DOI: 10.33965/IS2024_202401C008.	M33

<i>Кратак опис садржине:</i>			
<p><i>Data literacy</i> представља сложен концепт који обухвата вештине неопходне за успех појединца у дигиталном добу. Мерењем нивоа <i>data literacy</i> остварују се унапређења концепта и већи степен успешности. Циљ овог истраживања јесте да сагледа трендове у мерењу <i>data literacy</i>-ја у односу на методе, популацију и земље у којима су истраживања спроведена. Примена критеријума укључивања и искључивања довела је до анализе 22 рада. Резултати показују да су анкете најчешћи алат за мерење у области образовања, међу студентима и наставницима. Када је реч о државама, Кина и Индонезија имају највећи број спроведених истраживања.</p>			
<i>Рад припада проблематици докторске дисертације:</i>			
	ДА	<b>НЕ</b>	ДЕЛИМИЧНО

Р. бр.	аутори, наслов рада, часопис, <b>волумен</b> (година) странице од-до, DOI или ISBN/ISSN	категорија
7.	S. Kijanovic, S. Koprivica, D. Taibi, A. Ivic, D. Stefanovic, and <b>A. Komosar</b> , 'OVERVIEW OF USAGE OF OPEN GOVERNMENT DATA IN BUILDING MACHINE LEARNING AND AI SOLUTIONS: A SYSTEMATIC LITERATURE REVIEW', in <i>Proceedings of the 17th IADIS International Conference Information Systems 2024</i> , IADIS Press, Aug. <b>2024</b> . DOI: 10.33965/IS2024_202401C010.	M33

<i>Кратак опис садржине:</i>			
<p>Овај рад пружа систематски преглед литературе о интеграцији отворених државних података (ОГД) са решењима заснованим на машинском учењу и вештачкој интелигенцији. ОГД се односи на јавно доступне податке које производе или прикупљају државни органи, чиме се подстичу транспарентност и учешће грађана. Рад истражује примену отворених државних података у различитим областима друштвеног развоја, истичући њихов потенцијални утицај. Такође указује на потешкоће и изазове са којима се истраживачи суочавају. Налази сугеришу да коришћење отворених државних података у машинском учењу и вештачкој интелигенцији има потенцијал да подстакне иновације, унапреди доношење одлука и допринесе инклузивном развоју у различитим секторима. Преглед литературе наглашава значај одговорне примене отворених државних података у сврхе машинског учења и вештачке интелигенције.</p>			
<i>Рад припада проблематици докторске дисертације:</i>			
	ДА	<b>НЕ</b>	ДЕЛИМИЧНО

Р. бр.	аутори, наслов рада, часопис, <b>волумен</b> (година) странице од-до, DOI или ISBN/ISSN	категорија
8.	S. Kijanovic, <b>A. Komosar</b> , S. Koprivica, A. Milicevic, D. Dakic, 'Pregled upotrebe tehnologija u nastavnom procesu', XXX Skup Trendovi razvoja 2024 – Nastavnici i saradnici kao centar promena u visokom obrazovanju - TREND <b>2024</b> , Vrnjačka Banja.	M63

<i>Кратак опис садржине:</i>			
<p>У данашњем динамичном друштву, брза еволуција технологије поставља изазове пред образовне институције да се континуирано прилагођавају потребама тржишта рада. Факултети и предмети, као кључни чиниоци образовног система, не само да треба да прате технолошке иновације већ и да проактивно реагују на захтеве савременог тржишта. Сходно томе, Факултет техничких наука, Универзитет у Новом Саду као један од кључних фактора у контексту образовних институција у синергији са привредом, тежи да наставни процес унапређује и да студенти уче о актуелним технологијама. Овај рад истражује тренутну употребу технологија у наставном процесу на основу истраживања спроведеног међу студентима. Циљ истраживања је добијање увида у то који су програмски језици и технологије заступљени и колико су студенти задовољни стеченим знањем, као и компетенције студената да се одређене технологије раде више у контексту извођења наставе, а све са циљем да могу да прате актуелности у привреди. На основу добијених резултата, закључује се да студенти на Факултету техничких наука, Универзитет у Новом Саду раде широк спектар програмских језика и технологија, где су задовољни стеченим знањем, а такође дају сугестију да се у настави више изучавају актуелне технологије попут вештачке интелигенције.</p>			
<i>Рад припада проблематици докторске дисертације:</i>			
	ДА	<b>НЕ</b>	ДЕЛИМИЧНО



Сходно томе, јавља се потреба за унапређењем постојећих модела заснованих на машинском учењу у домену статичке анализе злонамерних софтвера, како би се унаредило њихово класификовање. Предложено истраживање ће бити усмерено на питања издвајања обележја злонамерних софтвера прикладних за његову статичку анализу и развој хибридног модела машинског учења који ће омогућити ефективније класификовање различитих породица, укључујући нове и претходно непознате варијанте.

*Комисија констатује да је предмет истраживања подобан, јер је истраживачка тема класификовања злонамерних софтвера засновано на визуелизацији и статичкој анализи машинског кода актуелна и значајна. Како је ова област релативно нова, омогућава и постизање значајних научних резултата и отвара даље правце истраживања у предметној ужој научној области.*

**Предмет истраживања је подобан?                    ДА                    НЕ                    ДЕЛИМИЧНО**

### III.3 познавања проблематике на основу изабране литературе са списком литературе

Систематски преглед литературе, урађен у сврху израде предложене докторске дисертације, односи се на период од 2019. до 2023. године и спроведен је коришћењем оквира ПРИЗМА [1]. Главни закључци овог прегледа односе се на употребу модела заснованих на различитим архитектурама, корпусима софтвера и начину валидирања предложених модела за класификовање злонамерног софтвера.

Увођење конволутивних неуронских мрежа у статичку анализу злонамерног софтвера резултовало је побољшаним перформансама у поређењу са традиционалним приступима. Примена конволутивних неуронских мрежа представља искорак ка концептуализацији злонамерног софтвера као структуре са локалним зависностима. На основу прегледа литературе уочено је да се злонамерни софтвер сматра секвенцијалном структуром са локалним и далекодометним зависностима, што се осликава на интеграцију са другим архитектурама неуронских мрежа. У овом контексту, далекодометне зависности се односе на зависности које превазилазе локалне, тј., на зависности између значајно удаљених статичких обележја софтвера, чиме се постиже моделовање шире структуре софтвера. Поред тога, још увек не постоји генерализовани концептуални модел који би омогућио потпуније разумевање предности и недостатака употребе машинског учења за класификовање злонамерног софтвера, јер добијена таксономија не пружа увид у узрочно-последичне везе [1].

Са друге стране, када је реч о доступним софтверским корпусима, уочавају се изазови небалансираних корпуса и недостатка инстанци појединих породица злонамерних софтвера у корпусима. У великом броју истраживања примењује се прекомерно узорковање (енгл. *oversampling*), које није увек методолошки оправдано [1].

Поред тога, коришћене мере квалитета за евалуацију модела често варирају. Уочава се непостојање консензуса у вези са израчунавањем вредности Ф1-мере, посебно у случајевима примене унакрсног валидирања. Ф1-мера представља једну од најиндикативнијих мера квалитета модела, која се заснива на мерама прецизности и одзива, при чему се у истраживачкој пракси примењује више начина за њено израчунавање. Сходно томе, евалуација модела није конзистентно вршена на транспарентни начин [1].

#### Литература

У пријави теме кандидат, за тражених 25 библиографских јединица, наводи:

- [1] Komosar, A., Gnjatovic, M., Stefanovic, D., Macek, N., Savic, D., & Vuckovic, T. (In Press, 2026). An overview of convolutional neural network-based static malware analysis techniques. *Tehnicki vjesnik – Technical Gazette*, 33(4). <https://doi.org/10.17559/TV-20251009003047>
- [2] Komosar, A., Stefanović, D., & Sladojević, S. (2024). An overview of image processing in biomedicine using U-Net convolutional neural network architecture. *Journal of Computational Forensic Sciences*, 3(1), 5–20. <https://doi.org/10.5937/jcfs3-48848>
- [3] Komosar, A., Kijanovic, S., Mandic, V., Nikolic, D., & Vuckovic, T. (2024). On the application of static code analysis tools in the Serbian IT industry: An empirical study. In *Proceedings of the 17th IADIS*

- International Conference Information Systems 2024.* IADIS Press.  
[https://doi.org/10.33965/IS2024\\_202401L007](https://doi.org/10.33965/IS2024_202401L007)
- [4] Slavic, D., Komosar, A., Stefanović, D., & Rakić, S. (2025). Cybersecurity in Industrial Internet of Things and collaborative robots: Industry 5.0 perspective. In *Proceedings of the International Conference on Business, Management, and Economics Engineering Future-BME* (pp. 672–680). <https://doi.org/10.24867/FUTURE-BME-2024-076>
- [5] Pan, Y., Ge, X., Fang, C., & Fan, Y. (2020). A Systematic Literature Review of Android Malware Detection Using Static Analysis. *IEEE Access*, 8, 116363–116379 <https://doi.org/10.1109/ACCESS.2020.3002842>
- [6] Alqahtani, A., Azzony, S., Alsharafi, L., & Alaseri, M. (2023). Web-Based Malware Detection System Using Convolutional Neural Network. *Digital*, 3(3), 273–285 <https://doi.org/10.3390/digital3030017>
- [7] Perić, D., Maček, N., & Bogdanoski, M. (2022). Application of convolutional neural networks to spoken words evaluation based on lip movements without accompanying sound signal. *Journal of Computer and Forensic Sciences*, 1(1), 7–16 <https://doi.org/10.5937/1-42696>
- [8] Alzubaidi, L., Zhang, J., Humaidi, A. J., Al-Dujaili, A., Duan, Y., Al-Shamma, O., Santamaría, J., Fadhel, M. A., Al-Amidie, M., & Farhan, L. (2021). Review of deep learning: Concepts, CNN architectures, challenges, applications, future directions. *Journal of Big Data*, 8(1), 53 <https://doi.org/10.1186/s40537-021-00444-8>
- [9] Nataraj, L., Karthikeyan, S., Jacob, G., & Manjunath, B. S. (2011). Malware images: Visualization and automatic classification. *Proceedings of the 8th International Symposium on Visualization for Cyber Security*, 1–7 <https://doi.org/10.1145/2016904.2016908>
- [10] Almomani, I., Alkhayer, A., & El-Shafai, W. (2023). E2E-RDS: Efficient End-to-End Ransomware Detection System Based on Static-Based ML and Vision-Based DL Approaches. *Sensors*, 23(9), 4467 <https://doi.org/10.3390/s23094467>
- [11] Maniriho, P., Mahmood, A. N., & Chowdhury, M. J. M. (2024). A systematic literature review on Windows malware detection: Techniques, research issues, and future directions. *Journal of Systems and Software*, 209, 111921 <https://doi.org/10.1016/j.jss.2023.111921>
- [12] Senanayake, J., Kalutarage, H., & Al-Kadri, M. O. (2021). Android Mobile Malware Detection Using Machine Learning: A Systematic Review. *Electronics*, 10(13), 1606 <https://doi.org/10.3390/electronics10131606>
- [13] Ehsan, A., Catal, C., & Mishra, A. (2022). Detecting Malware by Analyzing App Permissions on Android Platform: A Systematic Literature Review. *Sensors*, 22(20), 7928 <https://doi.org/10.3390/s22207928>
- [14] Gaber, M. G., Ahmed, M., & Janicke, H. (2024). Malware Detection with Artificial Intelligence: A Systematic Literature Review. *ACM Computing Surveys*, 56(6), 1–33 <https://doi.org/10.1145/3638552>
- [15] Ketebu, K. E., Onwodi, G. O., Ukhurebor, K. E., Eneche, B. M., & Yaah-Nyakkko, N. K. (2024). A recent survey of image-based malware classification using convolution neural network. *Journal of Autonomous Intelligence*, 7(5), 1287 <https://doi.org/10.32629/jai.v7i5.1287>
- [16] Ali, R., Ali, A., Iqbal, F., Hussain, M., & Ullah, F. (2022). Deep Learning Methods for Malware and Intrusion Detection: A Systematic Literature Review. *Security and Communication Networks*, 2022, 1–31 <https://doi.org/10.1155/2022/2959222>
- [17] Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. *Electronics*, 11(2), 198 <https://doi.org/10.3390/electronics11020198>
- [18] Jaisinghani, K., & Singh, S. (n.d.). Recent Advances in Image based Malware Classification through the Lens of Deep Learning—A Systematic Literature Review. *International Journal of Intelligent Systems and Applications in Engineering*
- [19] Ding, Y., Hu, J., Xu, W., & Zhang, X. (2019). A Deep Feature Fusion Method for Android Malware Detection. *2019 International Conference on Machine Learning and Cybernetics (ICMLC)*, 1–6 <https://doi.org/10.1109/ICMLC48188.2019.8949298>
- [20] Yakura, H., Shinozaki, S., Nishimura, R., Oyama, Y., & Sakuma, J. (2019). Neural malware analysis with attention mechanism. *Computers & Security*, 87, 101592 <https://doi.org/10.1016/j.cose.2019.101592>
- [21] Xue, D., Li, J., Lv, T., Wu, W., & Wang, J. (2019). Malware Classification Using Probability Scoring and Machine Learning. *IEEE Access*, 7, 91641–91656 <https://doi.org/10.1109/ACCESS.2019.2927552>

- [22] Singh, A., Handa, A., Kumar, N., & Shukla, S. K. (2019). Malware Classification Using Image Representation. In S. Dolev, D. Hendler, S. Lodha, & M. Yung (Eds.), *Cyber Security Cryptography and Machine Learning* (Vol. 11527, pp. 75–92). Springer International Publishing [https://doi.org/10.1007/978-3-030-20951-3\\_6](https://doi.org/10.1007/978-3-030-20951-3_6)
- [23] Lim, Kim, Kim, Hong, & Han. (2019). Payload-Based Traffic Classification Using Multi-Layer LSTM in Software Defined Networks. *Applied Sciences*, 9(12), 2550 <https://doi.org/10.3390/app9122550>
- [24] Song, Y., & Wang, J. (2019). Efficient Shellcode Detection Based on Convolutional Neural Network. 2019 International Conference on Communications, Information System and Computer Engineering (CISCE), 309–313 <https://doi.org/10.1109/CISCE.2019.00076>
- [25] Yen, Y.-S., & Sun, H.-M. (2019). An Android mutation malware detection based on deep learning using visualization of importance from codes. *Microelectronics Reliability*, 93, 109–114 <https://doi.org/10.1016/j.microrel.2019.01.007>

*У пријави теме за израду докторске дисертације, кандидат је изнео попис литературе коју ће користити у истраживању, а у складу са ограничењем од 10 до 25 библиографских јединица. Наведена литература релевантна је за област истраживања, а библиографске јединице јасно указују на актуелност истраживања у области, као и на већи број других повезаних библиографских јединица које су релевантне за област истраживања и које кандидат у свом даљем истраживању треба да проучи. Кандидат је показао да је истражио релевантну литературу из области класификовања злонамерних софтвера.*

**Избор литературе је одговарајући?      ДА      НЕ      ДЕЛИМИЧНО**

#### III.4 циљева истраживања

Истраживање се може дефинисати кроз следећа истраживачка питања (ИП):

- ИП 1. Који су основни изазови у класификовању злонамерних софтвера заснованих на визуелизацији и статичкој анализи машинског кода?
- ИП 2. На који начин се визуелизација машинског кода може искористити за издвајање репрезентативних обележја погодних за класификовање злонамерних софтвера?
- ИП 3. Који модел машинског учења показује најбоље перформансе при класификовању злонамерних софтвера на основу предложених обележја?

Циљеви предложеног истраживања јесу следећи:

1. Развој хибридног модела машинског учења за класификовање злонамерних софтвера заснованог на визуелизацији и статичкој анализи машинског кода
2. Предлог приступа извођењу статичких обележја злонамерних софтвера заснованог на традиционалним векторима обележја за представљање дигиталних слика.
3. Експериментално валидирање предложених модела.

Постављена истраживачка питања проистичу из потребе за унапређењем метода статичке анализе злонамерних софтвера применом техника визуелизације машинског кода и модела машинског учења. Одговори на наведена питања омогућавају идентификовање кључних изазова у класификацији злонамерних софтвера, дефинисање адекватног приступа за издвајање репрезентативних обележја, као и избор и евалуацију одговарајућих модела машинског учења.

Очекује се да ће резултати истраживања допринети бољем разумевању могућности примене визуелизације машинског кода у области класификовања злонамерних софтвера, као и развоју прецизнијих и ефикаснијих модела за њихово аутоматско класификовање.

*Комисија констатује да је циљ подобан, релевантан и адекватно постављен, и да је предложено истраживање оправдано.*

**Циљеви истраживања су одговарајући?      ДА      НЕ      ДЕЛИМИЧНО**

#### III.5 очекиваних резултата (хипотезе)

На основу систематског прегледа литературе и постављених циљева издвајају се следеће хипотезе:  
 Х1: Хибридни модели машинског учења који комбинују основну архитектуру конволутивних неуронских мрежа с другим моделима машинског учења могу да постигну боље перформансе у контексту класификовања злонамерних софтвера заснованом на статичким обележјима у односу на моделе засноване искључиво на конволутивним неуронским мрежама.

Х2: Примена традиционалних вектора обележја за представљање дигиталних слика може да унапреди перформансе система за статичку анализу злонамерних софтвера заснованих на визуелизацији машинског кода.

Х3: Начин израчунавања Ф1-мере утиче на адекватност процене квалитета модела за статичку анализу злонамерних софтвера

Примена резултата предложене докторске дисертације може допринети унапређењу више области сајбер безбедности и заштите информационих система, укључујући:

1. Унапређење система за крајњу заштиту рачунарских система (енгл. *End-Point Protection*) кроз ефикасније препознавање и класификовање злонамерних софтвера на крајњим уређајима, чиме се омогућава бржа реакција на безбедносне претње и смањење ризика од компромитовања система.
2. Развој и унапређење других модела за класификовање злонамерног софтвера пружањем нових метода за издвајање и представљање обележја, као и кроз примену предложених решења у различитим приступима заснованим на машинском учењу и вештачкој интелигенцији.
3. Повећање нивоа заштите података и сервиса у окружењима рачунарства у облаку (енгл. *Cloud Security*), омогућавајући ефикаснију детекцију злонамерних активности и идентификацију злонамерних софтвера који могу угрозити интегритет, поверљивост и доступност података.
4. Унапређење механизма заштите мобилних апликација кроз примену развијених метода за анализу и класификацију потенцијално злонамерних апликација, чиме се доприноси безбеднијем коришћењу мобилних уређаја и платформи.
5. Подршку поступцима дигиталне форензике кроз обезбеђивање додатних алата и метода за идентификацију, класификовање и анализу злонамерних софтвера, што може допринети ефикаснијем прикупљању и тумачењу дигиталних доказа током безбедносних истрага.
6. Унапређење система за евалуирање модела вештачке интелигенције који се користе у оквиру сајбер безбедности производа (енгл. *Product Cybersecurity*), кроз развој методологија и показатеља који омогућавају објективнију процену перформанси, поузданости и отпорности модела на различите врсте сајбер претњи.

*Комисија сматра да су наведене хипотезе и очекивани резултати подобни, јер представљају важан истраживачки резултат и основу за реализацију даљих истраживања и примена у пракси.*

**Очекивани резултати представљају значајан научни допринос? ДА НЕ ДЕЛИМИЧНО**

III.6 плана рада (на основу фаза истраживања и оријентационог садржаја дисертације из Обрасца 1)

Истраживање у оквиру докторске дисертације обухвата следеће фазе:

Фаза 1: Дефинисање стања у области, тренутних изазова и проблема кроз систематске прегледе литературе. Преглед кључних чинилаца истраживања, позиционирање истраживања, постављање циљева и истраживачких питања. Извођење иницијалног истраживања и прикупљање података о кључним чионицима истраживања.

Фаза 2: Дефинисање истраживачких модела и хипотеза, као и метода прикупљања и обраде података.

Фаза 3: Креирање мерног инструмента и дефинисање протокола систематског прегледа литературе за прикупљање података.

Фаза 4: Реализација истраживања у одабраним окружењима – прикупљање података.

Фаза 5: Анализа и интерпретација добијених резултата, те извођење закључака. као и дефинисање правца даљих истраживања.

План рада се заснива на истраживањима и објављивању радова на међународним конференцијама и часописима је следећи:

2023. - истраживање на тему употребе неуронских мрежа у области компјутерске визије; објављивање рада на међународној конференцији

2023. - Емпиријско истраживање на тему статичке анализе кода; објављивање рада на међународној конференцији

2024. - Истраживања на тему развоја сајбер безбедности у индустријским системима; објављивање рада на међународној конференцији

2024. - Истраживање на тему детектовања и класификовања злонамерног софтвера применом машинског учења

2025. - Развој експерименталног модела и верификација резултата објављивањем рада на међународној конференцији

2026. - Објављивање рада у међународном часопису са SCI/SCIE листе

Оријентациони садржај докторске дисертације структурисан је на следећи начин:

1. Увод
2. Преглед постојећих истраживања, са освртом на њихове домете и ограничења
3. Предлог хибридног модела машинског учења за статичку анализу злонамерног софтвера
4. Експериментално валидирање предложеног модела
5. Дискусија
6. Закључак
7. Литература
8. Прилози

*Комисија констатује да је план рада подобан и адекватно постављен.*

**План рада је одговарајући?                    ДА                    НЕ                    ДЕЛИМИЧНО**

### III.7 метода и узорак истраживања

На прикладним корпусима који садрже инстанце злонамерних софтвера биће развијени и експериментално валидирани хибридни модели машинског учења за класификовање злонамерних софтвера заснован на визуелизацији и статичкој анализи машинског кода. Полазни модел биће заснован на архитектури конволутивне неуронске мреже, а потом ће се разматрати његова унапређења и хибридне варијанте изведене комбиновањем основног модела с другим техникама машинског и дубоког учења, у циљу ефективнијег моделовања локалних и далекокометних зависности између статичких обележја.

У контексту предложеног истраживања, основне независне променљиве:

- а) вектор обележја који преставља извршни фајл,
- б) архитектура модела (комбиновање архитектуре конволутивне неуронске мреже са рекурентним архитектурама, ансамблима модела итд.),
- в) скуп и вредности хиперпараметара (број конволутивних слојева, број неурона по слоју, избор активационе функције, димензије и број филтера итд.). Зависне променљиве укључују стандардне мере за процену квалитета модела (тачност, прецизност, одзив, F1-мера, итд.).

Скуп јавно доступних корпуса злонамерних софтвера из којег ће бити изабрани подскуп корпуса за обучавање и валидирање модела машинског учења размотрених у предложеном истраживању дат је у следећој табели:

Корпус	Број инстанци			
	Инстанце злонамерног софтвера	Безопасне инстанце	Укупан број инстанци	Опис
<i>Malimg</i>	9 339	<i>N/A</i>	9 339	25 класа, сиве слике
<i>Microsoft Malware Classification Challenge (BIG 2015)</i>	21 741	<i>N/A</i>	21 741	9 класа, сиве слике (за сваки узорак су обезбеђена оба фајла: <i>.byte</i> и <i>.asm</i> )
<i>AndroZoo</i>	<i>N/A</i>	<i>N/A</i>	Преко 15 милиона	7 класа
<i>Drebin</i>	5 560	<i>N/A</i>	5 560	179 класа
<i>CICMalDroid202</i>	<i>N/A</i>	<i>N/A</i>	Више од 17 341	Више класа
<i>CICAndMal2017 and follow-up dataset 2019</i>	<i>N/A</i>	<i>N/A</i>	Више од 10 854	4 класе
<i>CICMalMem2022</i>	29 298	29 298	58 596	15 класа
<i>AMD</i>	24 553	<i>N/A</i>	24 553	17 класа
<i>ClAMP</i>	2 722	2 488	5 210	1 класа злонамерних софтвера и 1 класа безопасних узорака
<i>Benign &amp; Malicious PE Files</i>	14 600	5 010	19 612	1 класа злонамерних софтвера и 1 класа безопасних узорака
<i>MalwareDataSet</i>	40 918	96 526	137 444	1 класа злонамерних софтвера и 1 класа безопасних узорака
<i>SEL</i>	500	9 500	10 000	1 класа злонамерних софтвера и 1 класа безопасних узорака
<i>EMBER 2018</i>	400 000	400 000	Преко 1 милион	1 класа злонамерних софтвера и 1 класа безопасних узорака
<i>Dumpware10</i>	3 686	608	4 294	10 класа злонамерних софтвера и 1 безопасна
<i>Android Botnet</i>	1 929	<i>N/A</i>	1 929	14 класа
<i>IoT-23</i>	<i>N/A</i>	<i>N/A</i>	<i>N/A</i>	20 узорака злонамерног софтвера и 3 узорака безопасних
<i>MaMaDroid</i>	35 500	8 500	44 000	<i>N/A</i>
<i>MalGenome</i>	1 200	<i>N/A</i>	1 200	Више класа

<i>Andro-Dumpsys</i>	906	<i>N/A</i>	906	13 класа злонамерних софтвера
<i>MaleVis</i>	<i>N/A</i>	<i>N/A</i>	Више од 14 000	25 класа злонамерних софтвера и 1 класа безопасних
<i>Praguard Dataset</i>	<i>N/A</i>	<i>N/A</i>	10 479	Андроид инстанце

*Комисија констатује да је предложени метод истраживања потпуно одговарајући и да обезбеђује одличну основу за остварење постављених циљева истраживања.*

**Метод и узорак су одговарајући? ДА НЕ ДЕЛИМИЧНО**

### III.8 места, лабораторије и опреме за истраживачки рад

Истраживање је спровођено у лабораторији за Инжењерство информационих система Факултета техничких наука, Универзитет у Новом Саду користећи лаптоп *HP EliteBook 8 G1i, 2000 Mhz, 12 Core(s), 14 Logical Processor(s), 32GB*

*Комисија констатује да су обезбеђени одговарајући ресурси за експерименталан рад и да је овај аспект пријаве подобан.*

**Услови за истраживачки рад су одговарајући? ДА НЕ ДЕЛИМИЧНО**

### III.9 методе статистичке обраде података и осталих релевантних података

Предложеним истраживањем није предвиђена примена статистичких метода обраде података. Експериментална провера резултата у предложеном истраживачком пројекту обухвата стандардне мере за процену квалитета модела (тачност, прецизност, одзив, Ф1-мера, итд.).

*Комисија сматра да је оваква одлука оправдана и оцењује овај аспект пријаве тезе као подобан.*

**Предложене методе су одговарајуће? ДА НЕ ДЕЛИМИЧНО**

## IV ОЦЕНА ПОДОБНОСТИ КАНДИДАТА

Услови дефинисани за кандидата студијским програмом:

На основу чланова 65 и 100 Закона о високом образовању ("Сл. гласник РС" бр. 88/2017, 73/2018, 27/2018 - др. закони, 67/2019, /2020 - др. закони, 11/2021 - аутентично тумачење и 67/2021 и 67/2021 – др. закони), чланова 63 и 151 до 158 Статута Факултета техничких наука, Универзитет у Новом Саду од 2.7.2018., 17.10.2018. и 28.12.2018. године (Пречишћен текст од 28.12.2018. године), као и „Правилника о упису, студирању на докторским академским студијама и стицању звања доктора наука, односно доктора уметности“ (Број 01-195/11-1 од 7.10.2021. године) Факултета техничких наука, Универзитет у Новом Саду право да пријави тему докторске дисертације стиче студент који је положио све испите одређене студијским програмом и који је одбранио Теоријске основе докторске дисертације.

### Образложење:

Алекса Комосар уписао је докторске академске студије на студијском програму Инжењерство информационих система 2023. године. Испунио је све наставне обавезе предвиђене планом и програмом и положио је предвиђене испите са просечном оценом 10,00 и тиме стекао 90 ЕСПБ. Након тога, реализовао је обавезу одбране Теоријских основа докторске дисертације и тиме стекао још 30 ЕСПБ. У оквиру досадашњег научно-истраживачког рада, кандидат је аутор (први аутор) једног рада категорије М22, шест радова категорије М33, и једног рада категорије М63.

*На основу наведеног Комисија констатује да кандидат Алекса Комосар испуњава формалне услове и поседује неопходну компетентност за израду предложене докторске дисертације.*

**Да ли кандидат испуњава дефинисане услове? ДА НЕ**

## V ОЦЕНА ПОДОБНОСТИ ПРЕДЛОЖЕНОГ МЕНТОРА

### V.1 Биографија ментора (до 500 речи):

**Др Дарко Стефановић** је редовни професор за ужу научну област информационо-комуникациони системи на Факултету техничких наука, Универзитет у Новом Саду. Проф. Стефановић има више од седамдесет објављених радова у међународним и домаћим часописима и на међународним и домаћим конференцијама. Има вишегодишње педагошко искуство и ради као наставник на више предмета из области Инжењерства информационих система и Индустијског инжењерства и инжењерског менаџмента. У фокусу његовог истраживачког рада су е-управа, пословни информациони системи, статичка анализа кода и учење на даљину.

**Др Милан Ђатовић** је редовни професор на Криминалистичко-полицијском универзитету у Београду за ужу научну област рачунарство, и гостујући професор на СРХ Високој школи у Хајделбергу, Наиф арапском универзитету за сигурносне науке у Ријад и Факултету техничких наука, Универзитет у Новом Саду. Радио је и као професор на Факултету техничких наука, Универзитет у Новом Саду, Факултету за компјутерске науке у Београду и Високој школи електротехнике и рачунарства струковних студија у Београду, а као истраживач-сарадник на Факултету за информатику Универзитета Ото фон Герике у Магдебургу. Звање доктора наука у области рачунарских наука стекао је 2009. на Универзитету Ото фон Герике у Магдебургу. Његова научна интересовања обухватају област вештачке интелигенције, с посебним фокусом на интеракцији између човека и машине. Објавио је више од сто публикација у научним часописима, монографијама и зборницима, укључујући и седам књига.

### V.2 Референце ментора из научне области којој припада тема докторске дисертације:

Р. бр.	аутори, наслов, <i>часопис</i> , <b>волумен</b> (година) број страница од-до, DOI или ISBN/ISSN	категорија
1.	Dakić D., <b>Stefanović D.</b> , Vučković T., Žizakov M., Stevanov B.: Event Log Data Quality Issues and Solutions, <i>Mathematics</i> 2023, <b>Vol. 11</b> , pp. 1-39, ISSN 0378-7206, DOI: <a href="https://doi.org/10.3390/math11132858">https://doi.org/10.3390/math11132858</a> ( <i>Mathematics</i> 25/334, IF 2023=2.3)	M21a
2.	Vrhovac V., Dakić D., Milisavljević S., Čelić Đ. <b>Stefanović D.</b> , Žizakov M.: The Factors Influencing User Satisfaction in Last-Mile Delivery: The Structural Equation Modeling Approach, <i>Mathematics</i> , ISSN: 2227-7390, 2024, DOI: <a href="https://doi.org/10.3390/math12121857">10.3390/math12121857</a> ( <i>Mathematics</i> 25/334, IF 2023=2.3)	M21a
3.	Nikolić D., <b>Stefanović D.</b> , Nikolić M., Dakić D., Stefanović M., Havzi S.: Uncovering Determinants of Code Quality In Education Via Static Code Analysis, <i>IEEE Access</i> , 2024, ISSN 2169-3536 ( <i>Computer Science, Information Systems</i> : 79/163; IF 2023 = 3.4)	M22
4.	Sladojević S., Arsenović M., Nikolić D., Andraš A., <b>Stefanović D.</b> : Advancements in Mobile-Based Air Pollution Detection: From Literature Review to Practical Implementation, <i>Sensors</i> , 2024, ISSN: 1424-8220, DOI: <a href="https://doi.org/10.1155/2024/4895068">10.1155/2024/4895068</a> ( <i>Engineering, Electrical &amp; Electronic</i> : 103/271; IF 2023 = 3.4)	M22
5.	Anderla A., Sladojević S., Delso G., Čulibrk D., Mirković M., <b>Stefanović D.</b> : Suppression of metal artefacts in CT using virtual sinograms and corresponding MR images, <i>Current Science</i> , 2017, Vol. 112, No 7, pp. 1505-1511, ISSN 0011-3891 ( <i>Multidisciplinary sciences</i> , 41/64 IF 2017=0.883)	M22
6.	A. Komosar, M. Gnjatovic, <b>D. Stefanović</b> , N. Macek, D. Savic, and T. Vuckovic, "An Overview of Convolutional Neural Network-Based Static Malware Analysis Techniques", <i>Tehnicki vjesnik - Technical Gazette</i> , Vol. 33/No. 4, 2026, In Press, doi: <a href="https://doi.org/10.17559/TV-20251009003047">10.17559/TV-20251009003047</a> ( <i>Engineering, Multidisciplinary</i> 90/179, IF 2024 = 1.4)	M22

Р. бр.	аутори, наслов, часопис, волумен (година) број страница од-до, DOI или ISBN/ISSN	категорија
1.	S. Ilić, <b>M. Gnjatović</b> , I. Tot, B. Jovanović, N. Maček, and M. Gavrilović Božović, 'Going beyond API Calls in Dynamic Malware Analysis: A Novel Dataset', <i>Electronics</i> , vol. 13, no. 17, p. 3553, Sep. 2024, doi: 10.3390/electronics13173553 (Computer Science, Information Systems 136/258, IF 2024 = 2.6)	M22
2.	I. Košanin, <b>M. Gnjatović</b> , N. Maček, and D. Joksimović, 'A Clustering-Based Approach to Detecting Critical Traffic Road Segments in Urban Areas', <i>Axioms</i> , vol. 12, no. 6, p. 509, May 2023, doi: 10.3390/axioms12060509 (Mathematics, Applied 98/344, IF 2023 = 1.9)	M21
3.	<b>M. Gnjatović</b> , N. Maček, M. Saračević, S. Adamović, D. Joksimović, and D. Karabašević, 'Cognitively Economical Heuristic for Multiple Sequence Alignment under Uncertainties', <i>Axioms</i> , vol. 12, no. 1, p. 3, Dec. 2022, doi: 10.3390/axioms12010003 (Mathematics, Applied 98/344, IF 2022 = 2.0)	M21
4.	<b>M. Gnjatović</b> , I. Košanin, N. Maček, and D. Joksimović, 'Clustering of Road Traffic Accidents as a Gestalt Problem', <i>Applied Sciences</i> , vol. 12, no. 9, p. 4543, Apr. 2022, doi: 10.3390/app12094543 (Engineering, Multidisciplinary 50/179, IF 2023=2.7)	M21
5.	S. Barzut, M. Milosavljević, S. Adamović, M. Saračević, N. Maček, and <b>M. Gnjatović</b> , 'A Novel Fingerprint Biometric Cryptosystem Based on Convolutional Neural Networks', <i>Mathematics</i> , vol. 9, no. 7, p. 730, Mar. 2021, doi: 10.3390/math9070730 (Mathematics 25/334, IF 2023=2.59)	M21a
6.	A. Komosar, <b>M. Gnjatovic</b> , D. Stefanovic, N. Macek, D. Savic, and T. Vuckovic, "An Overview of Convolutional Neural Network-Based Static Malware Analysis Techniques", <i>Tehnicki vjesnik - Technical Gazette</i> , Vol. 33/No. 4, 2026, In Press, doi: 10.17559/TV-20251009003047 (Engineering, Multidisciplinary (90/179); IF 2024 = 1.4)	M22

### V.3 Услови дефинисани за ментора у складу са *Правилима докторских студија Универзитета у Новом Саду* за област којој припада докторска дисертација:

На основу чланова 65 Закона о високом образовању ("Сл. гласник РС" бр. 88/2017, 73/2018, 27/2018 - др. закони, 67/2019, /2020 - др. закони, 11/2021 - аутентично тумачење и 67/2021 и 67/2021 – др. Закони), као и према члану 7 став 1 и члану 8 став 5 „Правила докторских студија Универзитета у Новом Саду“, који је усвојен на седници Сената Универзитета у Новом Саду одржаној 25.2.2021, и који је ступио на снагу 5.3.2021., а примењује се од 1.4.2021. године и према члану 5 став 3 „Правилника о упису, студирању на докторским академским студијама и стицању звања доктора наука, односно, доктора уметности“ Факултета техничких наука, Универзитет у Новом Саду (број 01-195/11-1) од 7.10.2021. године, ментор је по правилу наставник датог студијског програма, који поред услова, који су дефинисани стандардима за акредитацију има најмање пет радова који су публиковани у часописима са импакт фактором са *SCI* листе, односно *SCIE* листе у претходних 10 година.

#### Образложење:

**Проф. др Дарко Стефановић**, редовни професор са Факултета техничких наука, Универзитет у Новом Саду се предлаже као ментор за вођење истраживања у оквиру предложене докторске дисертације. У области Информационо-комуникационих система бави се активно истраживањем из области квалитета кода и статичке анализе кода, а из које се пријављује докторска дисертација. Проф. Стефановић има преко 20 објављених радова у часописима на *SCIE* листи са импакт фактором у области из које се пријављује дисертација. На основу свих научних и стручних резултата, као и резултата у наставном процесу, комисија констатује да проф. др Дарко Стефановић испуњава све формалне, стручне и педагошке услове неопходне за ментора ове докторске дисертације. Комисија

констатује да је др Дарко Стефановић подобан за ментора предложене докторске дисертације, у предложеној ужој научној области.

**Проф. др Милан Гњатовић**, редовни професор са Криминалистичко-полицијског универзитета у Београду се предлаже као ментор за вођење истраживања у оквиру предложене докторске дисертације. У области Рачунарства бави се активно истраживањем из области статичке анализе злонамерних програма, а из које се пријављује докторска дисертација. Проф. Гњатовић има преко 15 објављених радова у часописима на *SCIE* листи са импакт фактором у области из које се пријављује дисертација. На основу свих научних и стручних резултата, као и резултата у наставном процесу, комисија констатује да проф. др Милан Гњатовић испуњава све формалне, стручне и педагошке услове неопходне за ментора ове докторске дисертације. Комисија констатује да је др Милан Гњатовић подобан за ментора предложене докторске дисертације, у предложеној ужој научној области.

**Да ли ментор испуњава услове?**

**ДА**

**НЕ**

## VI ЗАКЉУЧАК

Тема је подобра	<u>ДА</u>	НЕ	ДЕЛИМИЧНО
Кандидат је подобра	<u>ДА</u>	НЕ	
Ментор је подобра	<u>ДА</u>	НЕ	

*Образложење о подобрности теме, кандидата и ментора (до 500 речи):*

Комисија је детаљно проучила достављену пријаву кандидата, извршила анализу постављеног проблема, утврђеног циља истраживања, очекиваних резултата, усвојене методологије и предложене структуре истраживања, проценила значај референци везаних за тему истраживања, референци кандидата и предложеног ментора, као и досадашњи ангажман и резултате кандидата и предложеног ментора, у наведеној области истраживања. На основу свих изнетих чињеница у овом Извештају, Комисија закључује следеће:

- Да су предложено истраживање, истраживачка питања, циљеви, методологија и очекивани резултати истраживања добро осмишљени и да је предложена тема подобра за израду докторске дисертације.
- Да је кандидат **Алекса Комосар**, мастер инжењер информанионих технологија, подобра за израду предложене докторске дисертације.
- Да су др **Дарко Стефановић**, редовни професор Факултета техничких наука, Универзитет у Новом Саду, и др **Милан Гњатовић**, редовни професор Криминалистичко-полицијског универзитета у Београду, подобрни за менторе предложене докторске дисертације.

Имајући у виду дате закључке, Комисија предлаже Наставно-научном већу Факултета техничких наука, Универзитета у Новом Саду и органима Универзитета у Новом Саду да прихвате тему за израду докторске дисертације под насловом:

**„Хибридни модел машинског учења за класификовање злонамерних софтвера заснован на визуелизацији и статичкој анализи машинског кода”**

кандидата **Алексе Комосара** и да се као ментори именују др **Дарко Стефановић**, редовни професор Факултета техничких наука, Универзитет у Новом Саду и др **Милан Гњатовић**, редовни професор Криминалистичко-полицијског универзитета у Београду.

Нови Сад, **10.06.2026.**

1. др Мирослав Стефановић, доцент  
\_\_\_\_\_, председник

2. др Милан Видаковић, редовни професор  
\_\_\_\_\_, члан

3. др Душанка Дакић, доцент  
\_\_\_\_\_, члан

4. др Данило Николић, доцент  
\_\_\_\_\_, члан

5. др Душан Савић, ванредни професор  
\_\_\_\_\_, члан

**НАПОМЕНА:** Члан комисије који не жели да потпише извештај јер се не слаже са мишљењем већине чланова комисије, дужан је да унесе у извештај образложење односно разлоге због којих не жели да потпише извештај и да исти потпише.