

UNIVERSITET SINGIDUNUM
4-170/125
09-12-2025

УНИВЕРЗИТЕТ СИНГИДУМУ

Департаман за последипломске студије

Данијелова 32, Београд

ВЕЋУ ДЕПАРТМАНА ЗА ПОСЛЕДИПЛОМСКЕ СТУДИЈЕ

Одлуком Већа Департамана за последипломске студије број 4 – 151/2020. од 18.09.2020. године, одређени смо за чланове Комисије за оцену и одбрану докторске дисертације кандидата Радуновић Владимира, под називом „*The Impact of Good Practices on the Security of Digital Products and the Limitation of Offensive Cyber Operations*“ (срб. „Утицај добрих пракси на безбедност дигиталних производа и ограничавање офанзивних сајбер-операција“) и на основу тога подносимо следећи о чему подносимо следећи

ИЗВЕШТАЈ

1. Основни подаци о кандидату и докторској дисертацији

Владимир Радуновић рођен је 8.6.1978. године у Београду, где је завршио основну школу и Математичку гимназију. Након завршетка средње школе уписује Електротехнички факултет у Београду (1997.). У току студија био је активан у домаћим и међународним студентским организацијама. На Електротехничком факултету 2006. године стиче звање Дипломираног инжењера електротехнике, програм физичке електронике, са дисертацијом "Системи за дигиталну обраду слике: примена Кохоненове неуралне мреже у сегментацији слике". Потом уписује програму савремене дипломатије при Факултету уметности Универзитета на Малти, који завршава 2010. године стицањем звања "Master of Arts (MA) in Contemporary Diplomacy", са дисертацијом "The Role of Information and Communication Technologies in Diplomacy and

Diplomatic Service". Докторске студије на Факултету за информатику и рачунарство Универзитета Сингидунум, смер Напредни системи заштите, уписује школске 2012. године.

Од 2005. године запослен је са пуним радним временом у међународној образовној невладиној организацији DiploFoundation, један период и при канцеларији ове организације у Београду – Удружењу грађана ДиплоЦентар. У склопу DiploFoundation прво води образовне и истраживачке програме на тему управљања Интернетом, да би од 2015. године преузео позицију Директора програма сајбер-безбедности и е-дипломатије, на послу координације међународних образовних и истраживачких програма из области сајбер-безбедности и е-дипломатије (истраживања, конференције, обуке, курсеви и едукације), и као предавач предавач на онлајн академским и професионалним курсевима при DiploFoundation и Универзитета на Малти на теме е-дипломатије, управљања Интернетом, и сајбер-безбедности. У склопу тог ангажмана, био је предавач на међународним обукама у сарадњи са Уједињеним Нацијама (UN), Међународном телекомуникационом унијом (ITU), Саветом Европе, Организацијом за европску безбедност и сарадњу (ОЕБС), Европском унијом, RIPE и ICANN, гостујући предавач на Дипломатској академији Министарства спољних послова Републике Србије, као и стручњак при "*Geneva Internet Platform*", међународној платформи за информисање и едукацију на тему дигиталних политика, са седиштем у Женеви. Од 2018. године покреће и води међународни пројекат "*Geneva Dialogue on Responsible Behaviour in Cyberspace*" у сарадњи са Владом Швајцарске, и учешћем многобројних међународних партнера из пословног, техничког, академског и невладиног сектора. Од 2016. до 2020. био је Члан Саветодавног одбора "*Global Forum on Cyber Expertise*" (GFCE), а од 2012. до 2014. служио као Члан Мултиактерске саветодавне групе Генералног секретара Уједињених нација при Форуму за управљање Интернетом (IGF).

Оснивач је "AVACom Ing" из Београда, компаније за управљање и развој ИКТ система, чији је директор био од 2006. до 2013. године, када је продата. Пре тога био је сарадник-стажиста у консултантској кући "evolaris" из Граца, Аустрија (2005.), запослен на телевизији Б92 у Београду, у одељењу B92.Net, на функцији ИТ администрације и подршке (2003.-2005.), те запослен у Алтернативној академској образовној мрежи (ААОМ), у Београду, у компјутерском центру на пословима ИТ администрације и подршке (2000.-2003.).

Владимир Радуновић је ожењен, и отац двоје деце. Живи и ради у Словенији.

Области научно-истраживачког рада и интересовања Владимира Радуновића су: сигурност кроз дизајн (security-by-design) и безбедност дигиталних производа и сервиса, употреба сајбер-

простора у геополитичким односима, сајбер-ратовање и међународни преговори за одговорно коришћење сајбер-простора у контексту међународне безбедности, као и дигиталне политике и глобално управљање Интернетом.

Кандидат има следеће објављене радове:

1. Radunović V, Veinović M, Jevremović A (2025) "The Efficiency of ICT Suppliers' Product Security Incident Response Teams in Reducing the Risk of Exploitation of Vulnerabilities in the Wild". Computers & Security Vol. 152, February. Print ISSN: 0167-4048, Online ISSN: 1872-6208; IF 2025: 5.4 (M21). DOI:10.1016/j.cose.2025.104388

2. Radunovic V, Veinovic M (2020) "Malware Command and Control Over Social Media: Towards the Server-less Infrastructure", Serbian Journal of Electrical Engineering. Print ISSN: 1451-4869, Online ISSN: 2217-7183 (M52). DOI:10.2298/SJEE2003357R

3. Radunovic V (2013) "DDoS - Available Weapon of Mass Disruption", Zbornik radova međunarodne konferencije 21. Telekomunikacioni forum (TELFOR), str.5-9, novembar 2013. Print ISBN: 978-1-4799-1419-7, Online ISBN: 978-1-4799-1420-3. DOI:10.1109/TELFOR.2013.6716157

чиме је испуњен предуслов за одбрану докторске дисертације.

Остали објављени радови:

Часописи и конференције:

1. Radunović V, Grätz-Hoffmann J, Maciel M (2021) "Impact of Good Corporate Practices for Security of Digital Products on Global Cyber Stability," 2021 13th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 2021, pp. 25-42. DOI:10.23919/CyCon51939.2021.9467805

2. Radunovic V (2016) "Internet Governance, Security, Privacy and the Ethical Dimension of ICTs in 2030 [Leading Edge]," in IEEE Technology and Society Magazine, vol. 35, no. 3, pp. 12-14, Sept. DOI:10.1109/MTS.2016.2592779

3. Radunovic V, Barjaktarovic M (2014) "Primena i bezbednosni rizici Cloud rešenja u eZdravlju", Proceedings of the SINTEZA conference "Impact of Internet on Business activities in Serbia and Worldwide", pp.661-667, May 2014. DOI:10.15308/sinteza-2014-661-667

4. Dickinson S, Dutton W H, Maciel M, Miloshevic D, Radunovic V (2014) "Enhanced Cooperation in Governance", Oxford Internet Institute Forum Discussion Paper, University of Oxford, January 2014. SSRN: <http://dx.doi.org/10.2139/ssrn.2376807>

5. Radunovic V (2013), "Pacifizam u kiber-prostoru: Zašto je za kiber-bezbednost važnija saradnja medju sektorima i akterima nego njegova militarizacija", 2103 Informaciona bezbednost, Beograd, Srbija, jun 2013.

Други радови и публикације:

1. Gavrilović A, Grottola S, Ittelson P, Kazakova A, Petit Siemens S, Radunović V, Roellinger JL, Stadnik I (2025) OEWG and Cybersecurity Negotiations at the United Nations: Issues, Dynamics, and Divides. DiploFoundation, 2025. <https://www.diplomacy.edu/resource/oewg-and-cybersecurity-negotiations-at-the-united-nations-issues-dynamics-and-divides/>

2. Mladenovic D, Radunovic V (2018) "Defining Offensive Cyber Capabilities", GCSC Issue Brief 2: Briefing and Memos from the Research Advisory Group, The Hague Centre for Strategic Studies, pp.91-134, June 2018. <https://hcss.nl/wp-content/uploads/2022/06/GCSC-Research-Advisory-Group-Issue-Brief-2-Bratislava.pdf>

3. Radunovic V (2017) "Towards a secure cyberspace via regional cooperation." DiploFoundation. <https://www.diplomacy.edu/resource/towards-a-secure-cyberspace-via-regional-co-operation/>

4. Radunovic V and Rüfenacht D (2016) "Cybersecurity Competence Building Trends". DiploFoundation. <https://www.diplomacy.edu/resource/cybersecurity-competence-building-trends/>

5. Rizmal I, Radunovic V, Krivokapic Dj (2016) "Vodič kroz informacionu bezbednost u Republici Srbiji". Centar za evroatlantske studije – CEAS i Misija OEBS-a u Srbiji. <http://www.osce.org/serbia/272171>

6. Abusara A, Radunovic V et al (2016) "Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities". DiploFoundation. <https://www.diplomacy.edu/resource/cybersecurity-in-the-western-balkans-policy-gaps-and-cooperation-opportunities/>

7. Radunovic V (2015) "Ka nacionalnom okviru za sajber-bezbednost". DiploFoundation i OEBS Misija u Srbiji. https://issuu.com/diplo/docs/ka_nacionalnom_okviru_za_sajber-bez

Докторска дисертација кандидата Владимира Радуновића је урађена на укупно 118 страна, од чега 20 страна чине прилог и списак литературе. Списак литературе обухвата 237 референци

које чине научни радови, књиге, зборници радова, законски прописи, корпоративна истраживања, као и електронски извори. Уз основни текст дисертација садржи и 11 слика и 8 табела.

Докторска дисертација кандидата Владимира Радуновића је била подвргнута провери софтвером за установљавање преклапања/плагијаризма (*iThenticate Plagiarism Detection Software*). Укупан процентуални износ запажених преклапања износи 23% дисертације, од чега 17% са сопственим радом у међународном часопису, на коме је дисертација заснована.

2. Предмет и циљ истраживања

Присутност рањивости у дигиталним производима и сервисима једна је од основа за извођење офанзивних сајбер-операција (енг. *offensive cyber operations, OCO*) од стране држава, а сајбер-наоружавање, уз изградњу офанзивних сајбер-способности (енг. *offensive cyber capabilities, OCC*), са собом често носи и тражење – па и куповину – а потом и складиштење ретких и непознатих рањивости ради злоупотребе. Овиме се наноси несагледива економска штета, угрожава међународни мир и безбедност, и урушава поверење у дигиталну трансформацију друштва.

Како би се подигли трошкови извођења офанзивних сајбер-операција, и тиме демотивисало наоружавање, неопходно је умањити доступност и могућност злоупотребе рањивости у системима. Индустрија, као и академска заједница, развили су неколике оквире, моделе и методе за безбедни развојни циклус (енг. *Secure Development Lifecycle, SDL*) софтвера, хардвера и сервиса, како би лакше реаговали на обзнањивање рањивости и нудили закрпе, али и превентивно реаговали ка отклањању рањивости кроз безбедност кроз дизајн (енг. *security-by-design*) и архитектуру својих производа. Једна од добрих пракси је и успостављање тимова за одговор на безбедносне инциденте производа (енг. *Product Security Incident Response Team, PSIRT*) као специјализованих јединица за управљање рањивостима.

Иако се праксе као што су PSIRT-ови препознају као добра пракса у појачању безбедности производа, њихова ефикасност у реалним условима остаје недовољно испитана. Студије случаја и искуства из праксе указују на то да оне унапређују координацију, убрзавају санацију и побољшавају комуникацију са спољним актерима. Међутим, постоји ограничен број емпиријских доказа који показују да ли такве праксе систематски смањују вероватноћу да ће

рањивости бити злоупотребљене у стварном окружењу, ван контролисаних или лабораторијских услова, и да ли оне заиста ограничавају извођење ОСО.

Штавише, иако модели зрелости играју улогу у примени корпоративних пракси, релативно мали број студија испитује узрочну везу између ових пракси и уочених исхода злоупотреба рањивости. То указује на потребу за аналитичким методама које су у стању да повежу организационе праксе са мерљивим безбедносним ефектима. Постоји посебна потреба за методологијама које могу да процене да ли праксе безбедности кроз дизајн повећавају сложеност, трошкове или неизвесност са којима се суочавају актери који настоје да злоупотребе преостале рањивости, поготово кроз ОСО.

Предмет овог истраживања обухвата идентификацију, класификацију и анализу постојећих добрих пракси за безбедан развој дигиталних производа, као и процену њихове ефикасности у управљању рањивостима. Дисертација је посебно усмерена на праксе чији је циљ управљање рањивостима и смањење ризика повезаних са њиховом злоупотребом током читавог животног циклуса производа.

Централно место у анализи заузима PSIRT тим као организациона пракса за координацију откривања рањивости, њихове процене, обелодањивања и отклањања. Истраживање предлаже и примењује методолошки модел за верификацију ефикасности PSIRT-а у смањењу вероватноће реалне злоупотребе рањивости.

На крају, дисертација разматра шира дејства оваквих пракси на изводљивост офанзивних сајбер-операција, развој и употребу сајбер-капацитета, као и последице по међународну безбедност и геополитичку стабилност.

Циљ истраживања је да се, прикупљањем и класификацијом пракси за подизање безбедности дигиталних производа водећих глобалних компанија – пре свега PSIRT-а, те предлагањем и симулирањем модела за верификацију њихове ефикасности, испита сврсисходност тих пракси на смањење рањивости дигиталних производа и услуга, и подизање трошкова извођења офанзивних сајбер-операција.

3. Хипотетички оквир истраживања

Општа хипотеза:

Гео-политички тренд сајбер-наоружавања и извођења политички мотивисаних софистицираних офанзивних сајбер-операција може се ограничити кроз систематску примену пракси за безбедност кроз дизајн и управљање рањивостима од стране произвођача дигиталних производа.

Посебна хипотеза:

Могућност извођења офанзивних сајбер-операција може се умањити кроз смањивање смањују вероватноће да ће рањивости бити злоупотребљене, и то кроз примену PSIRT-а као добре праксе.

Појединачне хипотезе:

1. Водећи произвођачи дигиталних производа развили су, и примењују, препознате добре праксе за безбедност кроз дизајн и управљање рањивостима, кроз цео животни циклус производа.

2. Међу овим праксама, успостављање и вођење PSIRT-а доприноси мерљивом умањењу вероватноће да ће откривене рањивости бити злоупотребљене у стварним околностима, као део софистицираних офанзивних сајбер-операција.

4. Методологија истраживања

У току научног и истраживачког рада употребљене су различите методе како би били задовољени основни методолошки захтеви (објективност, поузданост, општост и систематичност) и норме научне мисли (објективност, логичност, систематичност, проверљивост, мерљивост, прецизност, и складност).

Од основних метода, превасходно су употребљене анализа (рашчлањивање), синтеза (повезивање), апстракција (уочавање суштине), конкретизација, генерализација (уопштавање), дедукција, и компарација. Ове основне методе су примењене првенствено у обради секундарних извора (научно-теоријских сазнања других аутора, релевантне литературе и савремене пословне праксе, као и међународних стандарда, регулаторних аката и међународних договора), али и при обради примарних података истраживања. Од посебних метода је искоришћен структурализам,

ради проучавања односа међусобно зависних и повезаних сложених гео-политичких, економских и технолошких појава.

За прикупљање података су коришћене методе анализе садржаја, испитивања и посматрања секундарних извора података (прикупљање добрих пракси, и метода верификације ефикасности добрих пракси), те метода студије случаја за разумевање карактеристика рањивости злоупотребљених за извођење софистицираних сајбер-напада.

Од општенаучних метода су примењене метода моделовања за формулисање модела верификације ефикасности добрих пракси, статистичка метода за емпиријску проверу валидности предложене методе, те аналитичко-дедуктивна за обраду добијених података.

Као посебна метода за предложену нову методологију процене ефикасности добрих пракси коришћена је рандомизована студија истраживања парова (енг. randomised matched case-control design). За имплементацију предложене методологије примењена је техника узорковања, спаривања и поновног узимања узорака на насумичној бази (eng. bootstrapping) над подацима, уз контролу спољашњих утицаја кроз ко-вариабле. За примену методологије у сврху добијања резултата коришћен је програмски језик Python.

5. Кратак приказ садржаја докторске дисертације

Поглавље 1 уводи тему истраживања и поставља његов шири контекст. Даје преглед позадине проблема безбедности дигиталних производа и њихове улоге у савременим друштвеним, економским и безбедносним процесима, дефинише предмет и циљеве истраживања, формулише општу и специфичне хипотезе, истраживачка питања и научни допринос рада, те на крају приказује структуру дисертације и логику њеног развоја.

У Поглављу 2, постављају се интердисциплинарни теоријски и контекстуални темељи истраживања кроз преглед литературе о сајбер-наоружавању, офанзивним сајбер-операцијама и злоупотреби рањивости у дигиталним производима. Такође се разматрају технолошки, економски, регулаторни и политички приступи којима државе и други актери настоје да повећају трошкове офанзивних сајбер-способности и ограниче њихову употребу.

Поглавље 3 анализира и класификује постојеће праксе за унапређење безбедности дигиталних производа и смањење рањивости. Обухваћени су академски модели, међународни стандарди,

регулаторни оквири и индустријске SDL праксе, са посебним фокусом на управљање рањивостима и механизме координације, попут PSIRT-a.

У Поглављу 4 разматрају се постојеће индустријске и академске методологије за процену ефикасности пракси безбедности кроз дизајн и управљања рањивостима. Поглавље идентификује њихова ограничења у сагледавању ризика од реалних злоупотреба, те формулише кључне техничке, организационе и контекстуалне параметре релевантне за процену утицаја ових пракси на офанзивне сајбер-операцијаме.

Поглавље 5 уводи нову методологију за процену ефикасности добрих пракси у смањењу злоупотреба рањивости у реалном окружењу. У њему је представљен методолошки дизајн заснован на рандомизованој студији истраживања парова, као и избор варијабли, скупова података и аналитичких техника.

У Поглављу 6 предложена методологија се примењује кроз технику узорковања, спаривања и поновног узимања узорака над подацима о рањивостима из праксе, уз контролу спољашњих утицаја. Поглавље уводи изабране метрике смањења ризика и статистичке тестове за процену робусности резултата и улоге кључних спољашњих фактора од утицаја.

Поглавље 7 представља и анализира резултате симулације, процењујући њихову статистичку поузданост и практични значај. Посебно се разматра утицај постојања PSIRT-a на вероватноћу злоупотребе рањивости, као и утицај других фактора попут доступности кода за тест злоупотребе (eng. proof-of-concept) и типа индустрије.

У Поглављу 8 се налази детаљна дискусија налаза у ширем техничком, организационом и геополитичком контексту. Поглавље критички сагледава улогу индустријских пракси у ограничавању офанзивних сајбер-операција и сајбер-наоружавања, идентификује структурна ограничења и разматра импликације за политике, регулативу и међународну безбедност.

На крају, Поглавље 9 сумира проблем истраживања, предложени модел и кључне налазе, те јасно издваја научне доприносе рада. Такође се дају практичне препоруке за индустрију и доносиоце одлука, као и правци за будућа академска истраживања.

6. Постигнути резултати и научни допринос докторске дисертације

Примарни научни допринос ове дисертације огледа се у формулисању и емпиријском тестирању новог методолошког модела за процену ефикасности корпоративних пракси безбедности кроз дизајн и управљања рањивостима у смањењу вероватноће злоупотребе рањивости у пракси. Модел представља аналитички оквир који се може примењивати више пута и на различите праксе, а бити од користи и за теоријске моделе и политике усмерене на унапређење безбедности дигиталних производа. Модел такође даје концептуални допринос идентификовањем оних параметара који се могу посматрати и аналитички су релевантни за процену безбедносних исхода, чиме се отварају нови правци за методолошко унапређење.

Кључни емпиријски допринос представља примена предложеног модела на једну значајну индустријску праксу – PSIRT – уз коришћење јавно доступних скупова података о објављеним и активно злоупотребљеним рањивостима. Ова анализа, заснована на симулацији, показује да је постојање PSIRT-а у компанији, произвођачу дигиталног производа, у корелацији са статистички значајним смањењем вероватноће злоупотребе рањивости у пракси. Поред потврде ефикасности PSIRT-а, студија успоставља поновљив приступ тестирању других безбедносних пракси кроз прилагођавање скупова података, параметара или спољних фактора.

У циљу развоја и валидације модела, дисертација додатно доприноси систематичним прикупљањем, класификацијом и анализом пракси за унапређење безбедности које примењују водеће глобалне технолошке компаније, као и академских и индустријских методологија за процену њихове ефикасности. Рад мапира глобалну дистрибуцију PSIRT-а по индустријама, регионима и величинама компанија и идентификује кључне организационе, економске и регулаторне изазове повезане са њиховим успостављањем и континуираним функционисањем. Ово емпиријско мапирање омогућава упоредну анализу најбољих пракси по више димензија.

Додатно, дисертација унапређује методолошко размишљање кроз критичку анализу параметара повезаних са рањивостима, релевантних за ризик од злоупотребе, као што су нивои критичности откривене рањивости, брзина реакције, доступност кода за злоупотребу, и спољни фактори. Ова анализа представља основу за будућа истраживања која могу узети у разматрање различите параметаре, или даље унапређивати истраживање постојећих, потенцијално доводећи до модела прилагођених различитим типовима пракси или окружењима.

Повезујући емпиријске налазе предложеног модела са ширим расправама о сајбер-наоружавању и офанзивним сајбер-операцијама, дисертација даје интердисциплинарни допринос који повезује

техничку праксу у области сајбер-безбедности са студијама међународне безбедности. Рад показује како унапређења безбедности дигиталних производа могу повећати трошкове, сложеност и неизвесност извођења политички мотивисаних офанзивних сајбер-операција, чиме – иако посредно – доприносе стратешкој стабилности у сајбер-простору. У практичном смислу, модел нуди креаторима политика, регулаторима и лидерима у индустрији алат, заснован на чињеницама, за процену, подстицање и приоритизацију пракси безбедности кроз дизајн, путем регулаторних и тржишних механизма.

На крају, дисертација доприноси теоријском развоју повезивањем технолошких, организационих, политичких и економских аспеката сајбер-безбедности. Она повезује корпоративно доношење одлука и инжењерске праксе са безбедносним политикама и праксама на нивоу држава, показујући како организационе праксе на микро-нивоу имати последице по сајбер-конфликте и међународне односе. Оваквим приступом подстиче се даље интердисциплинарно истраживање на пољу рачунарских наука, студија безбедности, и политичких наука.

7. Мишљење и предлог Комисије о докторској дисертацији

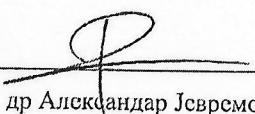
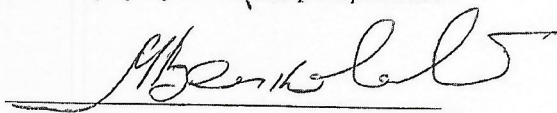
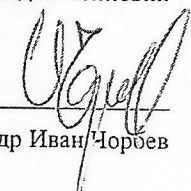
На основу свега изложеног Комисија је мишљења да докторска дисертација кандидата Владимира Радуновића по својој теми, приступу, структури и садржају рада, квалитету и начину излагања, методологији истраживања, начину коришћења литературе, релевантности и квалитету спроведеног истраживања и донетим закључцима задовољава критеријуме захтеване за докторску дисертацију, те се може прихватити као подобна за јавну одбрану.

Сагледавајући укупну оцену докторске дисертације кандидата Владимира Радуновића под називом „*The Impact of Good Practices on the Security of Digital Products and the Limitation of Offensive Cyber Operations*“ (срб. „Утицај добрих пракси на безбедност дигиталних производа и ограничавање офанзивних сајбер-операција“) предлажемо Већу департмана за последипломске студије и Сенату Универзитета Сингидунум да прихвати напред наведену докторску дисертацију и одобри њену јавну одбрану.

Потврђујемо својим потписом, под пуном професионалном одговорношћу, да су подаци у Извештају веродостојни и у потпуности тачни, укључујући тачну категоризацију

научноистраживачких резултата кандидата, а све у складу са Правилницима и актима
Универзитета.

У Београду, 8.12.2025. године


Проф. др Александар Јевремовић
Проф. др Младен Веиновић
Проф. др Иван Чорбев