Тел: (018) 500-201, 500-203
Факс: (018) 4523-747

Трг краља Александра 11 18000 Ниш
п. фах 122

Универзитет у Нишу
ПРАВНИ ФАКУЛТЕТ
Бр. 01-2121/1
29/06/2026. године

На основу члана 36. Правилника о мастер академским студијама права Служба за наставу и студентска питања даје следеће

О Б А В Е Ш Т Е Њ Е

1. Обавештава се јавност да су завршни мастер рад и Извештај Комисије за оцену и одбрану мастер рада под називом „Сајбер простор као ново криминогено окружење: теоријске основе и практични изазови", кандидата Александров Дарка, број досјеа М007/23-УП ,студента мастер академских студија права на Правном факултету у Нишу, примљени дана 29/06/2026. године и да се налазе у Библиотеци и на сајту Факултета.

2. Извештај и мастер рад доступни су, у року од 5 (пет) дана од дана истицања овог обавештења на огласну таблу Факултета, заинтересованим лицима у времену од 08,00 до 15,00 сати сваког радног дана.

3. Извештај Комисије за оцену и одбрану мастер рада су саставни део овог обавештеања.

4. Ово обавештење истаћи на сајт и доставити Библиотеци.

СЛУЖБА ЗА НАСТАВУ И
СТУДЕНТСКА ПИТАЊА

E-mail: pravni@prafak.ni.ac.rs
E-mail: pravni@prafak.ni.ac.rs

Катедри за кривичноправне науке
Правног факултета Универзитета у Нишу

На седници Катедре за кривичноправне науке која је одржана 24.06.2026. године на основу члана 34. Правилника о мастер студијама Правног факултета у Нишу формирана је Комисија за оцену и јавну одбрану мастер рада под називом: „Сајбер простор као ново кримоногено окружење: теоријске основе и практични изазови“, кандидата Александров (Владо) Дарка М007/23-УП, Комисија, после детаљног прегледа мастер рада подноси следећи

И З В Е Ш Т А Ј

Мастер рад под називом Сајбер простор као ново кримоногено окружење: теоријске основе и практични изазови“, кандидата Александров (Владо) Дарка је написан на 61 страницу компјутерски обрађеног текста, са проредом 1.5 . Кандидат је цитирање вршио у фуснотама (укупно 94). Литерарну подлогу рада чини 15 домаћих извора књига, монографија, библиографских јединица (уџбеника, приручника, закона, научних чланака и статистичких података) уз друге бројне научне и стручне радове објављене у часописима и електронске изворе.

Структурално је рад подељен у 8 дела: 1) Сајбер простор-појам и дефиниција, 2) Криминал у сајбер простору – сајбер криминал 3) Сајбер претње и 4) Заштита у сајбер простору 5) Правни и институционални оквир борбе против сајбер криминала 6) Дигитална форензика, 7) Практични изазови борбе против сајбер криминалитета – студије случаја и 8) Унапређење система борбе против сајбер криминала.

У уводу (стр. 1-3) кандидат излаже предмет свог рада указујући на чињеницу да савремени човек живи у дигиталном свету у коме сајбер простор, због својих специфичности попут анонимности и техничких рањивости, постаје идеално окружење за деловање појединаца и група са противправним циљевима. Значај обрађивања ове теме кандидат објашњава кроз брзи технолошки развој сајбер криминалитета који превазилази традиционалне облике криминала, те истиче да сајбер напади имају глобални карактер, не познају географске границе и захтевају глобални одговор. Разлоге за избор теме кандидат проналази и у личним мотивима и потреби да се дубље

разуме функционисање овог окружења „иза екрана“, будући да се већина грађана ослања на технологију без истинског разумевања ризика. Након тога, кандидат даје кратак приказ већих целина рада кроз његову структуру која обухвата појам сајбер простора, облике криминала против државе и приватног сектора, класификацију претњи, мере заштите ИКТ система, правни оквир на међународном и националном нивоу, као и анализу студија случаја попут глобалног напада „WannaCry“ и Dark Web операције „Silk Road“. На крају је изложен јасан циљ мастер рада, који се огледа у пружању свеобухватног увида у природу сајбер криминалитета, указивању на слабости система и предлагању препорука за унапређење сајбер безбедности.

У првом поглављу (4-8 стр.) кандидат се бави појмовним одређењем и еволуцијом сајбер простора као новог криминогеног амбијента, истичући да брзи развој информационо-комуникационих технологија и интернета доноси револуционарне бенефите, али и масовне злоупотребе кроз лакше, брже и анонимније извршење кривичних дела у односу на класичан криминал. Кандидат детаљно анализира настанак самог термина који је од научнофантастичног концепта Вилијама Гибсона из 1984. године еволуирао у дефиниције релевантних међународних организација (ITU, ISO) и Министарства одбране САД, при чему се сајбер простор одређује као сложено, нематеријално, децентрализовано и транснационално виртуелно окружење које превазилази контролу националних држава. Поред техничке и инфраструктурне хетерогености, у раду се осветљавају и социолошки аспекти сајбер простора као модерног пандана античком форуму у коме се трансформишу друштвени односи и стварају специфичне дигиталне заједнице засноване на заједничким интересима, али и ризици од отуђења и културолошког глобалистичког утицаја. Као неопходан одговор на ове негативне феномене и ради заштите дигиталне имовине, кандидат уводи појам сајбер безбедности коју дефинише кроз тријаду организационих, техничких и оперативних мера, закључујући да управо глобална и отворена природа овог паралелног универзума неминовно отвара врата за појаву и развој сајбер криминалитета.

У другом поглављу (9-23 стр.) кандидат се детаљно бави феноменологијом и класификацијом сајбер криминалитета, наглашавајући да дигитална сфера делује као нови простор извршења у коме интернет није примарни узрок, већ ефикасно средство које модификује и олакшава традиционалне облике криминала због глобалног

карактера и високе анонимности. Након прецизног разграничења компјутерског криминала (где је рачунар мета или средство) од ширег појма сајбер криминала (који обухвата целокупан дигитални простор), кандидат усваја класификацију Радомира Антовића и анализира три кључна безбедносна сегмента. Први сегмент обухвата сајбер криминал против државе, где се кроз теоријску призму и примере (попут напада у Нагорно-Карабаху и Украјини) обрађују сајбер тероризам, разорни напади на критичну инфраструктуру, сајбер шпијунажа великих сила, хактивизам, као и хибридно ратовање путем дезинформација и координисаног деловања „ботова" на друштвеним мрежама. Други сегмент је усмерен на приватни сектор, при чему кандидат кроз студије случаја масовног цурења података (Yahoo) и компромитовања трансакција (British Airways) указује на економску шпијунажу, преваре и широко распрострањену дигиталну пиратерију. Као посебно значајну целина, кандидат додаје и трећи сегмент – сајбер криминал против грађана, где детаљно расветљава дигитално насиље (cyberbullying), повреду приватности на интернет порталима (пример PleaseRobMe), родно засновано онлајн узнемиравање, „порнографију из освете", као и алармантне облике сексуалне експлоатације и злостављања деце на интернету кроз дечју порнографију и груминг (grooming). Пратећи развој овог феномена у историјском контексту – од првих усамљених компанијских „инсајдера" из шездесетих година, преко романтизованих „хакера старе школе" из осамдесетих (Митник, Полсен) и деструктивних црва попут Морисовог, па све до савремених паметних телефона и уређаја који су масовно проширили простор напада после пандемије COVID-19 – кандидат закључује да је сајбер криминал еволуирао у моћну, високопрофитабилну и транснационалну делатност организованих криминалних група која захтева радикално унапређење безбедносних механизама.

У трећем поглављу (24-32 стр.) кандидат се бави безбедносном димензијом дигиталног простора, анализирајући сајбер претње које угрожавају интегритет, поверљивост и доступност података. Ослањајући се на класификацију Ненада Путника, кандидат материју дели на сајбер нападе и злоупотребу сајбер простора као средства масовне комуникације. У оквиру напада техничког типа, кандидат разликује ненамерне софтверске пропусте од намерно креираног малициозног софтвера (малвера). Унутар ове категорије прецизно дефинише вирусе (кроз механизам саморепликације и активације), црве (који се аутономно шире и загушују мрежу), споредна врата и тројанске коње, уз занимљив осврт на њихову легалну примену у полицијским

истрагама САД и Аустралије. Такође, јасно разграничава функције adware-a, spyware-a и спама, док DoS и DDoS нападе исправно позиционира као атаке усмерене искључиво на нарушавање доступности ИКТ ресурса. Када је реч о нападима уз коришћење обмане, кандидат детаљно елаборира фишинг (илегално прикупљање података лажним представљањем) и социјални инжењеринг, који, према Дејану Тепавцу, кроз манипулацију, лажно представљање и искоришћавање људске емпатије циља људски фактор као најслабију карику безбедности. У сегменту злоупотребе сајбер простора, информационо ратовање дефинише се као стратешко слабљење противника контролом информација и пропагандом, што се примењује и у корпоративном сектору ради економске шпијунаже. Повезујући ово са сајбер тероризмом и психолошким ратом, кандидат се позива на Вајмана и указује на то да терористичке организације користе вишејезичне сајтове како би ширили панику и дезоријентисале три кључне групе: подржаваоце, међународно мњење и противничку јавност. На крају, кандидат се посвећује профилисању починилаца, наглашавајући специфичност њихове просторне удаљености од места злочина. Позивајући се на Мају Вукман, кандидат демистификује појам хакера и класификује субјекте према мотивима на крекере (вођене материјалном користи или извитопереним идеологијама), хактивисте (политички активизам) и инсајдере (интерне претње вођене новцем или осветом). Ова структура је додатно проширена традиционалном поделом на „беле капе" (етички хакери који легално унапређују заштиту), „црне капе" (малициозни хакери који врше крађу и деструкцију) и „сиве капе" (који делују у међупростору). Поглавље се заокружује закључком да је разумевање и профилисање сложене мотивације починилаца — од забаве и личне користи до политичких и психијатријских мотива — кључно како за криминалистичко оперативни рад, тако и за процесуално доказивање кривице пред надлежним органима.

У четвртом поглављу (33-35 стр.) кандидат анализира одбрамбену архитектуру сајбер простора кроз препознавање системских рањивости и систематизацију мера заштите ИКТ система. Кандидат дефинише контролу ризика кроз разграничење претњи и слабих тачака, те мапира интерне и екстерне тачке упада у мрежну инфраструктуру. Наглашавајући да је управо човек најслабија карика безбедносног ланца, као кључну превентивну меру истиче континуирану едукацију кадрова. У централном делу поглавља кандидат елаборира шест фундаменталних безбедносних сервиса (аутентификација, тајност, непорицање, интегритет, контрола приступа и расположивост), а потом анализира техничке алате за њихову реализацију. Посебан

значај придаје криптографској енкрипцији података и улози заштитних зидова (firewall) као баријера против неовлашћеног приступа из спољне мреже. Поглавље се заокружује прецизном таксономијом антималвер система, при чему кандидат јасно разграничава функције континуиране антивирусне заштите, антиспајвер алата који се покрећу на захтев, антитројан програма и личних заштитних зидова, закључујући да се ефикасна сајбер одбрана постиже искључиво интеграцијом техничких софтвера и људског фактора.

У петом делу рада (36-43 стр.) кандидат врши свеобухватну анализу правног и институционалног оквира борбе против сајбер криминала на међународном, европском и националном нивоу, уз упоредни приказ глобалних безбедносних стратегија.

На међународном плану, кандидат мапира кључна тела Уједињених нација (WSIS, UN GGE, UN Expert Group, ITU и UN ICT TF), истичући њихову улогу у стандардизацији и признавању међународног права у дигиталној сфери. У оквиру европских стандарда, детаљно анализира Будимпештанску конвенцију (2001) као темељни и обавезујући документ који кодификује четири категорије сајбер деликата. Еволуцију европске регулативе кандидат прати кроз прелазак са NIS на строжу NIS2 директиву (2022), eIDAS регулативу, те кроз институционално деловање тела ENISA, CIWIN и CERT-EU.

У контексту Републике Србије, фокус је на 27. глави Кривичног законика, која санкционише осам кривичних дела против безбедности рачунарских података. На институционалном пољу, кандидат прецизно дефинише спрегу између Одељења за високотехнолошки криминал МУП-а и Посебног тужилаштва за високотехнолошки криминал као носилаца оперативне борбе против дигиталних претњи.

Поглавље се заокружује упоредном анализом стратегија САД, Велике Британије и Немачке. Кандидат закључује да, упркос формалним разликама, све водеће силе деле јединствен, мултидимензионални приступ заснован на јавно-приватном партнерству, заштити критичне инфраструктуре, детекцији инцидената и континуираној едукацији, што представља и јасан путоказ за даљи развој домаћег безбедносног система.

У шестом поглављу (44-48 стр.) кандидат анализира дигиталну форензику као научну дисциплину, насталу 1999. године, која обезбеђује методе за откривање рачунарских злоупотреба, прикупљање доказа и њихово процесуално представљање пред судом.

Према предмету истраживања, кандидат ову област дели на четири потдисциплине: форензику рачунарских система, мобилних уређаја, база података и рачунарских мрежа. Саму истражну праксу кандидат разграничава на званичне истраге (које воде државни органи уз судски налог ради кривичног гоњења) и корпоративне истраге (које решавају интерне инциденте унутар компанија), наглашавајући да обе почивају на истим форензичким принципима.

У централном делу поглавља кандидат прави јасну дистинкцију између физичких и дигиталних компоненти, делећи их на:

- Физичке доказе (хардвер попут рачунара и телефона) и дигиталне доказе (подаци, лог фајлови, садржај RAM-а);
- Физичко место (материјално окружење) и дигитално место кривичног дела (виртуелни простор апликација и система), уз разликовање примарних и секундарних локација.

Кандидат успешно пореди класичну криминалистику и Локардов закон размене материје са дигиталним траговима активности у систему. Поглавље се заокружује прегледом фаза форензичког поступка — од утврђивања инцидента и прикупљања података, до строго контролисаног транспорта (уз употребу антистатичке и антирадијационе заштите за SSD дискове), чиме се гарантује интегритет доказа и законитост целог процеса.

У седмом полгављу (49-52 стр.) кандидат кроз три карактеристичне студије случаја успешно контекстуализује теоријске поставке из претходних делова рада, демонстрирајући деструктивни потенцијал, оперативне механизме и друштвене последице савременог сајбер криминалитета.

У оквиру прве студије случаја, кандидат анализира глобални ransomware напад „WannaCry" (2017), који је погодио преко 150 земаља и инфицирао више од 300.000 рачунара. Кандидат најпре дефинише рансомвер као уцењивачки малвер који шифрује податке и блокира системе, тражећи откуп у биткоинима ради очувања анонимности нападача. Посебно је осветљен оперативни аспект ширења вируса кроз Windows рањивост *EternalBlue*, као и његово специфично заустављање преко „килсвич" (killswitch) механизма — регистрацијом случајног домена од стране безбедносних истраживача. Извлачећи паралелу са традиционалним тероризмом због напада на критичну цивилну (здравствену) инфраструктуру, кандидат правилно диференцира мотиве, наглашавајући да је код рансомвера примарни циљ материјална корист, а не политичка идеологија.

Друга студија случаја посвећена је Dark Web операцији „Silk Road". кандидат демистификује даркнет као неиндексирани део сајбер простора коме се приступа преко анонимизационог система *Tor*. На примеру платформе „Silk Road", коју је 2011. основао Рос Улбрих (*Dread Pirate Roberts*), кандидат приказује како су криптовалуте и софтверска прикривеност омогућили развој глобалног дигиталног подземља за трговину дрогом, оружјем и фалсификованим документима. Студија успешно експлицира истражне капацитете безбедносних органа, описујући како је ФБИ (FBI)

кроз анализу Тор саобраћаја, праћење биткоин трансакција и лоцирање техничких пропуста успео да заплени сервере и процесуира организатора.

Трећи сегмент обрађује малвер „Blackshades" и његову повезаност са дигиталним сексуалним насиљем. Кандидат овај софтвер дефинише као деструктивни тројанац за даљинско управљање рачунарима (RAT) који је инфицирао преко пола милиона система. Кроз високопрофилисани случај напада на Кесиди Вулф од стране Цереда Абрахамса, кандидат детаљно описује механизам сајбер изнуде и уцене (секс торзије). Студија показује како нападачи даљинским активирањем веб-камера и прикупљањем компромитујућег материјала врше психолошку манипулацију и секундарну виктимизацију жртава, чиме је кандидат јасно указао на дубоку социолошку и криминалистичку димензију злоупотребе ИКТ-а у сврху нарушавања личне безбедности и приватности.

У деветом поглављу (53-54) кандидат се фокусира на стратешке правце и оперативне мере за унапређење система борбе против сајбер криминала, наглашавајући да ефикасна заштита захтева синергију финансијских улагања, стручног кадра, јавно-приватног партнерства и савремених технолошких решења. Кандидат као примарни стуб развоја безбедносне архитектуре издваја едукацију и управљање људским ресурсима. Указујући на потребу за системским школовањем и задржавањем ИКТ стручњака, кандидат наводи компаративни пример из Сенегала и оснивање Националне школе за сајбер безбедност (2018), што је позитивно утицало на јачање одбрамбених капацитета региона Западне Африке. Паралелно са институционалним образовањем, наглашава се важност подизања опште друштвене свести о дигиталним ризицима, као и државног субвенционисања научних института који прате муњевиту еволуцију малвера. Ослањајући се на теоријске поставке Дејана Вулетића, кандидат апострофира важност прецизног пописа националних ресурса и формирања специјализованих тимова за одговор на инциденте (CERT/CSIRT) који имају кључну координациону улогу у моменту напада.

Посебну пажњу у поглављу кандидат посвећује односу државних и недржавних актера. Кандидат истиче да је сарадња између јавног сектора и приватних корпорација од пресудног значаја за очување сајбер безбедности, али истовремено нуди критички осврт на комплексност овог партнерства кроз ретроспективу афере Едварда Сноудена. На овом примеру кандидат илуструје како су обавештајне службе САД и Велике Британије, уз техничку подршку приватних технолошких гиганата (попут компанија Google и Yahoo), спроводиле масовни дигитални надзор, што је након обелодањивања узроковало озбиљан пад међународног угледа ових држава.

На крају, у домену технолошких императива, кандидат систематизује концепт вишеслојне заштите система. Овај модел обухвата истовремену примену заштитних зидова, комплексне аутентификације, енкрипције података, као и редовног креирања резервних копија (*backup*) ради брзог опоравка система у случају компромитовања. Поглавље се заокружује прегледом глобалних платформи за мониторинг претњи у реалном времену, где се истичу организације попут *Internet Storm Center*, *CAIDA*, као и

пројекти Европске уније (нпр. *Lobster*), уз закључак да експанзија сајбер простора диктира непрекидну и динамичну борбу за очување безбедности ИКТ система.

У „Закључку“ (96-97 стр.) У Закључку свог рада кандидат на систематичан начин сумира резултате спроведеног истраживања, потврђујући полазну тезу да је сајбер простор постао кључан, али истовремено и најризичнији амбијент савременог друштва, у коме традиционални механизми контроле губе на ефикасности. Кандидат наглашава да сајбер претње попут малвера, фишинга, рансомвера и DDoS напада показују изузетан степен техничке софистицираности и прилагодљивости. Своје тврдње кандидат снажно утемељује на претходно анализираним студијама случаја, где су инфекција WannaCry и црно тржиште Silk Road апострофирани као еклатантни примери деструктивне моћи дигиталног криминала који је у стању да парализе здравствене системе, угрози стабилност јавних институција и омогући несметано деловање организованих криминалних мрежа на Дарквебу. Кључни допринос закључних разматрања огледа се у идентификацији неколико критичних фактора за изградњу одрживог система заштите. Првенствено, кандидат уочава трајни дискорак између брзине технолошких промена и рестриктивне природе законодавства, истичући да прекогранични карактер сајбер деликата захтева континуирано унапређење међународно-правне коопције, зачете још Будимпештанском конвенцијом 2001. године. Поред правне регулативе, Кандидат инсистира на модернизацији дигиталне форензике, материјално-техничком опремању оперативног апарата и континуираном улагању у специјализоване кадрове који једини могу парирати нападачима у сајбер простору. Посебан фокус у раду стављен је на безбедносну културу самих корисника ИКТ-а, при чему се човек препознаје као најслабија карика у систему безбедности. Кандидат аргументује да су лоше лозинке, компромитовање личних података и неопрезно поступање у онлајн окружењу најчешћи покретачи великих безбедносних криза, због чега се едукација позиционира као примарни превентивни штит. Рад се заокружује јасном научно-стручном поруком да је борба против сајбер криминалитета перманентан, асиметричан процес који никада неће бити окончан. С обзиром на то да се дигитални екосистем непрекидно шири, кандидат закључује да одбрамбени систем не сме деловати механички, већ проактивно, непрестано креирајући нове и ефикасне одговоре на инхерентне ризике виртуелног простора.

Закључак и предлог

После детаљног разматрања мастер рада: „Сајбер простор као ново криминогено окружење: теоријске основе и практични изазови“, можемо да закључимо да пред кандидатом није био једноставан задатак. Требало је, наиме, проучити и анализирати обимну домаћу и иностранu правнотеоријску литературу.

Сајбер криминалитет као безбедносни изазов модерног доба је посебно опасан друштвени проблем који погађа сва друштва. Кандидат је при писању овог рада кроз свеобухватну студију законске регулативе, институционалних оквира, дигиталне форензике и безбедносних стратегија дао јасан и целовит преглед сузбијања дигиталних претњи, како кроз анализу кривичних дела везаних за безбедност рачунарских података у Републици Србији, тако и кроз упоредну анализу глобалних безбедносних стратегија САД, Велике Британије и Немачке.

Значај овог рада се огледа у обједињеној анализи како међународних и европских стандарда у борби против сајбер криминала, почевши од Будимпештанске конвенције па до савремене NIS2 директиве, тако и у детаљном теоријском и практичном утемељењу дигиталне форензике. Нарочито је важно напоменути да рад обрађује тему криминалитета у виртуелном простору кроз специфичну дистинкцију физичких и дигиталних доказа, примењујући класичне криминалистичке принципе, попут Локардовог закона размене материје, на савремене токове информационих технологија.

Међу посебним квалитетима по којима се издваја овај мастер рад је свеобухватно теоријско и практично посматрање сајбер криминалитета, у примени не само области домаће и иностране теорије кривичног права, већ и илустровање теоријских решења кроз анализу глобалних студија случаја, као што су рансомвер напад WannaCry, Дарк веб операција Silk Road и злоупотреба малвера Blackshades у сврху сексуалног насиља. При обради постављене теме, кандидат се није задржао само на пуком интерпретирању законске и техничке литературе, већ је аргументовано изнео кључне правце унапређења система кроз едукацију кадрова, јавно-приватно партнерство и вишеслојну технолошку заштиту, износећи и бранећи своја оригинална гледишта.

Стога, Комисија закључује да мастер рад кандидата под називом „Сајбер простор као ново криминогено окружење: теоријске основе и практични изазови“ представља резултат самосталног и оригиналног научног рада из области кривичног права и безбедносних наука. Кандидат је у раду систематизовао и анализирао постојећу правнотеоријску, прикупио практичну, техничку и законску литературу и својим радом дао одређени допринос науци кривичног права.

Пошто су испуњени услови предвиђени у члану 36. Правилника о мастер студијама Правног факултета у Нишу, Комисија сматра да је мастер рад „Сајбер простор као ново криминогено окружење: теоријске основе и практични изазови“ кандидата подобан за јавну одбрану, па предлаже Комисији за докторске и мастер студије Правног факултета у Нишу да усвоји Извештај о оцени мастер рада и његовој подобности за јавну одбрану.

У Нишу, 26.06.2026. год.

ЧЛАНОВИ КОМИСИЈЕ

проф. др Миомира Костић
редовни професор Правног факултета у Нишу

проф. др Дарко Димовски
редовни професор Правног факултета у Нишу

проф. др Душица Миладиновић-Стефановић
редовни професор Правног факултета у Нишу