Република Србија

КРИМИНАЛИСТИЧКО-ПОЛИЦИЈСКИ УНИВЕРЗИТЕТ

Број: 43/2-7

Датум: 23.10.2026. год

ВЕЋУ ДЕПАРТМАНА ИНФОРМАТИКЕ И РАЧУНАРСТВА
КРИМИНАЛИСТИЧКО-ПОЛИЦИЈСКОГ УНИВЕРЗИТЕТА У БЕОГРАДУ

Предмет: Извештај о урађеној докторској дисертацији кандидата Драгана М. Јевтића

Поштовани чланови Већа Департмана информатике и рачунарства,

Одлуком Већа научних области природно-математичких и техничко-технолошких студија Криминалистичко-полицијског универзитета број 16 бр. 83/3-4-2026 од 18.09.2026. године образована је Комисија за оцену урађене докторске дисертације кандидата Драгана М. Јевтића под насловом **„Оптимизација firewall система у процесу детектовања DDoS напада на рачунарске мреже применом вишеструке анализе алгоритмима машинског учења“**. После прегледа достављене дисертације и пратеће документације, Комисија подноси следећи

ИЗВЕШТАЈ

1. УВОД

1.1 Хронологија одобравања и израде дисертације

Кандидат Драган М. Јевтић уписао је докторске академске студије информатике у октобру 2022. године на Криминалистичко-полицијском универзитету, под бројем индекса 2R1/0001/22. Тема докторске дисертације односи се на оптимизацију firewall система ради поузданог и правовременог детектовања DDoS напада применом алгоритама машинског учења.

Након испуњења обавеза предвиђених студијским програмом, кандидат је поднео пријаву теме докторске дисертације број 43/2 од 20.02.2026. године, под називом „Оптимизација firewall система у процесу детектовања DDoS напада на рачунарске мреже применом вишеструке анализе алгоритмима машинског учења“, у научној области Рачунарске науке и ужој научној области Рачунарство.

Надлежно веће одобрило је тему и именовало проф. др Петра Чисара, редовног професора Криминалистичко-полицијског универзитета у Београду, за ментора одлуком број 14 бр. 81/4-3-2026 од 09.04.2026. године.

Кандидат је завршену докторску дисертацију поднео на оцену надлежном Већу департмана дана 03.09.2026. године, уз документацију прописану Правилником о докторским студијама. Ментор је дао писану сагласност број 43/2-4 од 03.09.2026. године, којом је констатовао да је дисертација подобна за оцену.

У складу са Правилником о докторским студијама извршена је провера оригиналности достављене докторске дисертације, а подаци о извештају о оригиналности и позитивном мишљењу ментора уносе се према службеној евиденцији Универзитета.

На предлог руководиоца Департмана информатике и рачунарства, надлежно веће је одлуком број 43/2-6 од 11.09.2026. године образовало Комисију за оцену докторске дисертације у саставу:

- др Милан Гњатовић, редовни професор Криминалистичко-полицијског универзитета у Београду, председник,
- др Кристијан Кук, редовни професор Криминалистичко-полицијског универзитета у Београду, члан,
- др Далибор Добриловић, редовни професор Техничког факултета „Михајло Пупин“ у Зрењанину, Универзитета у Новом Саду, члан.

1.2 Научна област дисертације

Докторска дисертација припада образовно-научном пољу природно-математичких наука, научној области рачунарске науке и ужој научној области Рачунарство. Предмет истраживања обухвата информациону безбедност, анализу мрежног саобраћаја, системе за детектовање упада и примену алгоритама машинског учења у процесу препознавања и заустављања DDoS напада. Комисија констатује да је тема дисертације у области за коју је Криминалистичко-полицијски универзитет матичан.

Истраживање повезује теоријске основе машинског учења са експериментом у реалном мрежном окружењу. Посебно је размотрена могућност да резултати класификовања лог-записа подрже правовремену измену заштитне политике на firewall уређају. Такав приступ предмет сврстава у савремена истраживања на пресеку рачунарских мрежа, сајбер-безбедности и анализе података.

Ментор проф. др Петар Чисар је наставник Департмана информатике и рачунарства Криминалистичко-полицијског универзитета, изабран у ужој научној области Рачунарство. Задовољава све услове за ментора и налази се на листи ментора Департмана информатике и рачунарства Криминалистичко-полицијског универзитета.

1.3 Биографски подаци о кандидату

Драган Јевтић је рођен 03.08.1975. године у Београду.

После завршене Средње електротехничке школе „Никола Тесла“ у Београду, 1994. године уписао је Вишу ПТТ школу у Београду, смер Телекомуникације. У јуну 1998. године стекао је звање инжењера електротехнике.

У октобру 2001. године уписао је Технички факултет у Чачку Универзитета у Крагујевцу, смер Рачунарске науке. Основне студије завршио је у јулу 2005. године и стекао звање дипломираног инжењера електротехнике.

Почиње да ради у Инфраструктури железница Србије, у Сектору за ИТ, на месту администратора рачунарских мрежа. Године 2017. стекао је услов да врши дужност Руководилаца пројекта рачунарских мрежа са задацима да надгледа рад рачунарске мреже, система за контролу упада у мрежу као и виртуелну структуру сервера.

У октобру 2022. године уписао је докторске академске студије на Криминалистичко-полицијском универзитету, студијски програм Информатика.

2. ОПИС ДИСЕРТАЦИЈЕ

2.1 Садржај и структура дисертације

Докторска дисертација „Оптимизација firewall система у процесу детектовања DDoS напада на рачунарске мреже применом вишеструке анализе алгоритмима машинског учења“ у достављеној електронској верзији има 168 страна формата А4. Садржи 77 нумерисаних слика, 43 нумерисане табеле и 120 библиографских јединица. Поред насловних страна на српском и енглеском језику, захвалнице, сажетака и кључних речи на оба језика, рад садржи садржај, спискове слика, табела и скраћеница, 10 основних поглавља, списак литературе, стручну биографију кандидата и прописане изјаве.

Основни текст дисертације организован је у следећа поглавља:

1. Увод и проблем истраживања
2. Предмет и циљ научног истраживања
3. Преглед релевантних истраживања
4. Основе вештачке интелигенције
5. Мрежни напади
6. Принципи детекције упада у рачунарске мреже
7. Приказ модела коришћене рачунарске мреже за анализу саобраћаја
8. Приказ напада и одбране
9. Анализа скупа података и резултата истраживања
10. Закључак

Структура рада прати ток од дефинисања истраживачког проблема и прегледа релевантних сазнања, преко теоријских основа и описа експерименталног окружења, до приказа резултата, провере хипотеза и критичког разматрања ограничења.

2.2 Кратак приказ појединачних поглавља

Наслов докторске дисертације јасно одређује тематику и садржај истраживања.

У првом поглављу образложен је проблем поузданог и правовременог детектовања DDoS напада. Указано је на ограничења класичних механизама заснованих на статичким правилима, као и на последице лажно позитивних и лажно негативних резултата. Истраживачки проблем је постављен у контексту примене машинског учења над обележјима стварног мрежног саобраћаја.

У другом поглављу дефинисани су предмет, циљ и хипотезе истраживања. Општа хипотеза односи се на могућност идентификовања образаца малициозног саобраћаја анализом података са мрежних уређаја и IDS система. Посебна хипотеза односи се на могућност класификовања нормалног и малициозног саобраћаја на основу ограниченог скупа обележја лог-записа. Описан је и вишефазни процес који обухвата обучавање, тестирање и валидацију модела, примену заштитне политике и проверу ефеката њене примене.

Треће поглавље доноси обиман преглед домаћих и страних истраживања у области детектовања DDoS напада, анализе firewall и IDS логова, избора обележја и примене класичних модела, ансамбла модела и дубоких модела машинског учења. У прегледу литературе издвојени су фактори који ограничавају непосредно поређење резултата различитих радова: структура скупа података, неуниформна расподела класа, начин предобраде података, избор обележја, поступак валидације и тип напада. На основу тога образложен је истраживачки простор за упоредну анализу више алгоритама над истоветно припремљеним лог-записима у три експерименталне фазе.

Четврто поглавље приказује развој вештачке интелигенције, основе машинског учења и моделе релевантне за истраживање. Обрађени су линеарна и логистичка регресија, класификатор K најближих суседа, наивни бајесовски класификатор, стабло одлучивања, метода потпорних вектора и неуронске мреже. Поред начина рада, размотрени су услови под којима се поједини модели могу применити у безбедносном класификовању.

Пето поглавље систематизује типове мрежних напада, са посебним осврtом на DoS и DDoS нападе. Описани су начини злоупотребе рачунарских и мрежних ресурса, улога ботнет-инфраструктуре и механизам координисаног генерисања саобраћаја према циљном систему. Тиме је обезбеђена теоријска основа за разумевање сценарија који је касније реализован у експерименталном делу.

Шесто поглавље разматра принципе детектовања упада у рачунарске мреже. Приказани су приступи засновани на потписима и аномалијама, основне компоненте IDS система, начини прикупљања података и улога лог-записа у препознавању одступања од нормалног мрежног саобраћаја. Посебна пажња посвећена је повезивању резултата детектовања напада са механизмима заштите.

Седмо поглавље описује модел рачунарске мреже коришћен за анализу саобраћаја. Приказани су архитектура тестног окружења, конфигурациони, серверски и клијентски кодови, софтвер за генерисање напада, Check Point 6400 firewall уређај и систем за детектовање упада. Опис омогућава да се разумеју извори података и редослед корака у експерименту.

Осмо поглавље приказује напад и примену одбрамбене мере у три периода: пре напада, за време DDoS напада и после примене заштитне политике. NetBot окружењем генерисан је

тестни саобраћај, а логови са firewall и IDS компоненти коришћени су за даљу анализу. Приказани су ток напада, уочене промене мрежног саобраћаја и поступак блокирања саобраћаја који је означен као малициозан.

Девето поглавље представља централни експериментални део дисертације. Анализирано је приближно 64.200 инстанци логова, са почетним скупом од једанаест одабраних обележја. Подаци су обрађени у програму Orange применом следећих модела: Neural Network, Random Forest, Naive Bayes, Decision Tree, KNN и SVM. Резултати у сва три периода упоређени су применом стандардних мера квалитета: AUC, F1-мера, прецизност и одзив. Додатно су анализирана изабрана обележја и понашање сваког модела у тренуцима прелазака из нормалног стања у напад, и преласка из стања напада у стање одбране.

У десетом поглављу сумирани су резултати и формулисан је модел вишеструке провере. Општа хипотеза и посебна хипотеза потврђене су у контексту контролисаног експеримента. Наведени су ограничења истраживања и могући смерови даљег рада.

Литература обухвата 120 прегледно систематизованих библиографских навода.

3. ОЦЕНА ДИСЕРТАЦИЈЕ

3.1 Савременост и оригиналност

Предмет дисертације је актуелан због раста обима DDoS напада и њихове разноврсности, те потребе да се механизми детектовања напада повежу са брзом применом одбрамбених правила. Савремени информациони системи генеришу велики број лог-записа, при чему статичка правила не могу адекватно да моделују промене образаца напада. Примена скупа алгоритама машинског учења над истим подацима представља оправдан начин да се одлука не заснива на резултату само једног класификатора.

Оригиналност истраживања се огледа у организацији поступка вишеструке анализе образаца мрежног саобраћаја у три корака, при чему се у сваком кораку примењују два комплементарна алгоритма – алгоритма са највећом вредношћу посматране мере квалитета и алгоритма који најосетљивије реагује на промену стања. Решење је испитано над логовима прикупљеним у контролисаном, али реалистичном мрежном окружењу које генерише период нормалног рада, период напада и период после примене одбрамбене политике.

Посебна вредност приступа јесте повезивање анализе података са практичним током одбране: детектовано стање мрежног саобраћаја се користи као основа за промену firewall политике и накнадну проверу да ли је мрежа враћена у стање одбране. Добијене резултате, међутим, треба тумачити у контексту конкретног модела и експерименталног сценарија, а не као доказ универзалне предности изабраних алгоритама.

3.2 Осврт на коришћену литературу

Литература садржи 120 прегледно систематизованих библиографских навода који покривају основе вештачке интелигенције и машинског учења, моделе DDoS напада, IDS и firewall системе, технике избора карактеристика, поступке уравнотежавања података, дубоко и

ансамбл учење, као и објашњивост безбедносних модела. Литература је адекватно одабрана и одговара тематици ове дисертације.

3.3 Опис и адекватност примењених научних метода

Истраживање је реализовано применом метода за машинско учење, дубоко учење, статистичку анализу, извођење обележја, рачунарско моделовање, упоредну анализу, као и експерименталног метода. Све методе су адекватно примењене.

3.4 Применљивост остварених резултата

Предложени приступ оптимизацији firewall система рачунарски је имплементиран, а његова применљивост је практично демонстрирана у реалистичном окружењу. Модел има потенцијал за примену у класичним корпоративним мрежама, cloud и IoT окружењима, и софтверски дефинисаним мрежама.

3.5 Оцена достигнутих способности кандидата за самостални научни рад

Кандидат је у својој дисертацији идентификовао актуелан проблем из области информационе безбедности, спровео истраживање литературе из предметне области, извршио анализу постојећег стања истраживања и предложио приступ оптимизовању firewall система у процесу детектовања DDoS напада на рачунарске мреже. Демонстрирао је самосталност у истраживачком раду и способност критичког размишљања. Објављивањем резултата у научном часопису са импакт-фактором на СЦИ/СЦИе листи, кандидат је демонстрирао способност за представљање научних доприноса. Комисија је мишљења да је кандидат показао адекватан степен способности за самосталан научноистраживачки рад.

4. ОСТВАРЕНИ НАУЧНИ ДОПРИНОС

4.1 Приказ остварених научних доприноса

Научни доприноси дисертације могу се систематизовати на следећи начин:

- Развијен је модел вишеструке анализе за детектовање DDoS напада који повезује резултате скупа изабраних алгоритама машинског учења са поступком примене и провере firewall заштитне политике.
- Дефинисан је трокорачни поступак провере заснован на стандардним мерама квалитета модела машинског учења, у којем се комбинују алгоритам са највећом вредношћу дате мере квалитета и алгоритам са најизраженијом променом посматране мере.
- Генерисан је и анализиран скуп од приближно 64.200 инстанци firewall и IDS логова у три различита стања мреже, са издвојеним скупом од једанаест обележја релевантних за класификовање саобраћаја.
- Спроведено је упоредно вредновање шест алгоритама машинског учења над истоветно припремљеним подацима, с посебним освртом на комплементарне улоге ансамбла стабала одлучивања и неуралне мреже у посматраном сценарију.

- Експериментално је повезано детектовања напада са применом одбрамбене мере на активној мрежној опреми и накнадном провером стања, што доприноси процени оперативне применљивости резултата.
- Критички су утврђене границе добијених резултата и формулисани су могући смерови даљег развоја.

Наведени доприноси чине повезану целину. Њихова вредност није само у појединачним класификационим резултатима, већ у начину на који су прикупљање података, вишеалгоритамска провера, примена заштитне политике и провера ефекта одбране организовани у јединствен истраживачки ток.

4.2 Критичка анализа резултата истраживања

Резултати истраживања су систематично приказани по примењеним алгоритмима и за различите периодима снимања мрежног саобраћаја. Дато тумачење резултата методолошки је значајно, јер разликује два критеријума процене квалитета: квалитет класификовања у датом периоду заснован на стандарндим мерама квалитета, и осетљивост модела на промену саобраћаја. Анализа резултата посебно издваја комплементарне улоге ансамбла стабала одлучивања и неуралне мреже у посматраном сценарију. Ансамбл стабала одлучивања издвојен се по оствареним вредностима стандардних мера квалитета (AUC=0,979, P=R=F1=0,990), док је посматрана неуронска мрежа издвојена због осетљивости на промену саобраћаја, тј. могућности раног детектовања промене стања.

У раду је коректно наведено да су постављене хипотезе потврђене у контексту контролисаног експеримента. Практично су демонстрирани могућности детектовања и провере одбране у посматраном систему, односно да посматрани скуп обележја допушта ефикасно класификовање нормалног и малициозног саобраћаја.

Основна ограничења односе се на примену само једног мрежног окружења и само једног сценарија DDoS напада, одсуство независног производног теста и непостојање посебних мерења времена обраде и потрошње ресурса. Ова ограничења су јасно препозната и не умањују ваљаност резултата.

4.3 Верификација научног доприноса

Кандидат је први аутор на раду објављеном у међународном часопису категорије М23:

Jevtić, D., Čisar, P., Kuk, K., & Stojanović, V. (2025). Application of Machine Learning in the Optimisation of Firewall Parameters Based on Attack Detection. IPSI Transactions on Internet Research, 21(1), 86–100. https://doi.org/10.58245/ipsi.tir.2501.08

Овај рад припада научној области докторске дисертације и тематски одговара проблему и предмету научног истраживања дефинисаним у предлогу теме докторске дисертације.

5. ЗАКЉУЧАК И ПРЕДЛОГ

Комисија за оцену докторске дисертације „Оптимизација firewall система у процесу детектовања DDoS напада на рачунарске мреже применом вишеструке анализе алгоритмима машинског учења“ кандидата Драгана М. Јевтића сматра да је дисертација адекватно методолошки постављена, правилно спроведена, заснована на актуелним сазнањима, урађена у складу са образложењем наведеним у пријави теме и да садржи све елементе специфициране Правилником о докторским студијама Криминалистичко-полицијског универзитета у Београду.

На основу свега изложеног, имајући у виду научне резултате истраживања, практичну примену истраживања, методолошки оквир и научни и друштвени допринос, Комисија даје позитивну оцену предметне докторске дисертације и Већу департмана информатике и рачунарства Криминалистичко-полицијског универзитета у Београду

ПРЕДЛАЖЕ

да се докторска дисертација „Оптимизација firewall система у процесу детектовања DDoS напада на рачунарске мреже применом вишеструке анализе алгоритмима машинског учења“ кандидата Драгана М. Јевтића прихвати, изложи на увид јавности и упути на коначно усвајање Већу научних области природно-математичких и техничко-технолошких студија Криминалистичко-полицијског универзитета.

У Београду, _____

ЧЛАНОВИ КОМИСИЈЕ

др Милан Гњатовић, редовни професор Криминалистичко-полицијског универзитета у Београду, председник

_____

др Кристијан Кук, редовни професор Криминалистичко-полицијског универзитета у Београду, члан

_____

др Далибор Добриловић, редовни професор Техничког факултета „Михајло Пупин“ у Зрењанину, Универзитета у Новом Саду, члан

_____