

КОМИСИЈИ ЗА СТУДИЈЕ II СТЕПЕНА ЕЛЕКТРОТЕХНИЧКОГ ФАКУЛТЕТА У БЕОГРАДУ

Комисија за студије II степена, Електротехничког факултета у Београду, на својој седници одржаној 25.09.2025 године именовала нас је у Комисију за преглед и оцену мастер рада дипл. инж. Никола Јовановић под насловом „Сигурносни изазови великих језичких модела: Интерактивна апликација за демонстрацију напада и заштите“. Након прегледа материјала Комисија подноси следећи

ИЗВЕШТАЈ

1. Биографски подаци кандидата

Никола Јовановић је рођен 29.10.1999. године у Београду. Завршио је основну школу „Ћирило и Методије“ у Београду. Уписао је Шесту београдску гимназију у Београду, коју је завршио са одличним успехом. Електротехнички факултет Универзитета у Београду уписао је 2018. године. Дипломирао је 2023. године на Одсеку за рачунарску технику и информатику, а дипломски рад одбранио је у јулу 2023. године, са оценом 10, на тему „Реализација апликације за мерење квалитета ваздуха“. Мастер академске студије на Електротехничком факултету у Београду, на Модулу за софтверско инжењерство уписао је у октобру 2023. године.

2. Извештај о студијском истраживачком раду

Кандидат Никола Јовановић спровео је истраживачки рад у области примене великих језичких модела у сајбер безбедности. Истраживање је обухватило анализу постојећих приступа у откривању напада и неауторизованих активности на мрежи, преглед релевантних модела и њихових перформанси на скуповима података који садрже реалне податке. Урађена је и упоредна анализа постојећег решења LLM Security Labs Playground и решења које је урађено у оквиру овог мастер рада.

3. Опис мастер рада

Мастер рад припада области вештачке интелигенције и информационих технологија. Примарни циљ овог рада је дизајнирање и имплементација интерактивне веб апликације која демонстрира кључне безбедносне ризике великих језичких модела и практичне технике одбране, омогућавајући систематско извођење, посматрање и евалуацију напада и заштиту у контролисаном окружењу.

Рад има 55 страна, укључује 39 слика, три табеле и 22 референци. Подељен је у шест поглавља. Уводно поглавље описује мотиве израде и истраживања, примарни циљ рада, као и структуру самог рада. У другом поглављу представљен је преглед области и теоријски оквир како би читалац имао основу за разумевање резултата рада и имплементације. Треће поглавље описује коришћене алате и описана функционална спецификација. У четвртном поглављу описана је архитектура и структура апликације израђене у овом раду. У петом поглављу је представљен резултат, односно опис апликације кроз примере и слике. У последњем шестом поглављу представљен је закључак рада и смернице за надоградњу.

4. Анализа са кључним резултатима

Рад је систематски обрадио безбедност великих језичких модела од теоријских основа до практичне примене. Полазећи од објашњења како велики језички модели уче и закључују из контекста, теоријски оквир послужио је као полазна тачка за пројектовање и изградњу интерактивне апликације која уједињује демонстрације напада, мерење успешности и преглед препоручених одбрамбених механизма. Посебна пажња посвећена је избору алата и архитектуре комуникације, са јасним раздвајањем системских инструкција од корисничких података и контролом приступа реалним моделима, чиме је обезбеђена поновљивост експеримената и транспарентност тока података.

Коначни производ је едукативна платформа која претвара апстрактне појмове безбедности у конкретно искуство. Свака страница напада води корисника кроз дефиницију проблема, типичне примере упита, интерактивно тестирање на различитим моделима и закључивање на основу статистике. Демонстрације обухватају репрезентативне векторе ризика - занемаривање контекста, цурење упита, усвајање штетних персона, префикс инјекције и реконструкцију података, тако да корисник може одмах да уочи обрасце који

доводе до погрешних или опасних одговора. Секције са проценом ризика и стратегијама одбране премोшћују јаз између теорије и праксе. Из експерименталних резултата изводе се јасне смернице попут санитизације улаза, очувања контекста, робусних системских правила, детекције образаца и ограничавања учесталости упита.

5. Закључак и предлог

Кандидат Никола Јовановић је у истраживању које је пратило овај мастер рад успео да покаже значај примене великих језичких модела у сајбер безбедности. При реализацији истраживања, колега Јовановић је показао значајан степен самосталности у раду, иновативности, и одговорио је на све захтеве који су му били постављени.

На основу свега изложеног, Комисија за преглед и оцену мастер рада предлаже Комисији за студије другог степена Електротехничког факултета у Београду да рад под називом „Сигурносни изазови великих језичких модела: Интерактивна апликација за демонстрацију напада и заштите“ дипл. инжењера ел. и рач. Николе Јовановића, прихвати као мастер рад и кандидату одобри јавну усмену одбрану.

Београд, 19.10.2025. године

Чланови комисије:

др Дражен Драшковић Ванредни професор
сагласан, 19.10.2025.

Јелица Цинцовић Асистент
сагласан, 19.10.2025.