РЕЦЕНЗИЯ
на дисертационен труд

за придобиване на образователната и научна степен „Доктор“ в област на висше образование 4. Природни науки, математика и информатика

професионално направление 4.6. Информатика и компютърни науки

докторска програма: „Информационни системи и технологии, информатика и компютърни науки“

Автор: магистър Али Сабра

Тема: Deep Learning Approach for Modeling DDoS Attacks in Cybersecurity

Моделиране на DDOS атака чрез Deep Learning

Рецензент: проф. д-р инж. Теодора Иванова Бакърджиева,
Варненски свободен университет „Черноризец Храбър“
катедра „Компютърни науки“

Рецензията е изготвена на основание на решение на Ректора на Варненския свободен университет „Черноризец Храбър“ със заповед №892/28.11.2025 г.

1. Общи сведения за процедурата и представените материали

Али Сабра е зачислен за докторант на самостоятелна подготовка към катедра „Компютърни науки“ със заповед на Ректора на ВСУ „Ч. Храбър” №15/18.01.2021 г. За научен ръководител е определен проф. д-р Златогор Минчев.

Докторантът е положил успешно изпитите по специалността, предвидени в индивидуалния учебен план, както и изпит по английски език. Той е отчислен с право на защита със заповед на Ректора на на ВСУ „Ч. Храбър” №100/21.02.2024 г.

2. Обща характеристика и актуалност на дисертационния труд

Дисертационният труд на Ali Sabra е с общ обем 118 страници**,** Състои се от въведение, изложение в четири глави, заключение, списък с използвани съкращения, 23 фигури, 6 таблици. Използваната библиография включва 77 литературни източника. Трудът е професионално структуриран, с ясна логика, последователност и академичен стил на изложение. Изследването е посветено на разработването на интелигентен модел за откриване на DDoS атаки**,** базиран на машинно и дълбоко обучение, чрез анализ на реални логове от уеб сървъри. Темата е изключително актуална**,** тъй като DDoS атаките на приложно ниво са сред най-честите и трудни за откриване заплахи в

съвременната мрежова сигурност, а прилагането на дълбоко обучение за тяхното моделиране и детекция е едно от най-иновативните направления в областта.

Във Въведението се обосновава актуалността на темата, формулирани са целта, задачите, хипотезите и изследователските въпроси. Авторът подчертава съществуващите проблеми в откриването на DDoS атаки на приложно ниво и очертава научната новост на своя подход, базиран на методи от дълбокото обучение. Авторът ясно дефинира проблема – недостатъчната ефективност на съществуващите системи за откриване на DDoS атаки, които използват синтетични или остарели набори от данни. В началото на разработката е направен литературен обзор на съществуващите подходи за откриване на DDoS атаки и приложението на алгоритми за машинно и дълбоко обучение в киберсигурността. Разгледани са различни типове атаки (Volumetric, Protocol, Application-level), архитектури на IDS/IPS системи, както и предимствата и ограниченията на класическите ML модели спрямо дълбоките невронни мрежи. Авторът ясно формулира научния проблем**,** който остава нерешен — липсата на реалистични данни и ефективни DL модели за приложно ниво. Главата представя задълбочен преглед на съвременните подходи за защита от DDoS атаки, класификации, методи за машинно и дълбоко обучение, използвани в киберсигурността.

В изследователската част е представено изграждането на нов набор от данни от реални логове на Apache уеб сървър, генерирани чрез осем различни DDoS инструмента. Извършени са анализи на характеристиките на трафика, предобработка, обучение и тестване на модели – Random Forest, k-NN, SVM, ANN и LSTM. Резултатите показват, че LSTM моделът достига точност 99%, което превъзхожда другите модели. Включен е и анализ чрез SHAP за интерпретация на влиянието на отделните признаци, което е важен принос към прозрачността и обяснимостта на AI системите.
Главата завършва с дискусия за потенциалната адаптация на архитектурата към други типове атаки и възможности за реално внедряване. Заключението съдържа изводите от изследването, оценка на хипотезите и предложения за бъдещо развитие, включително тестване в реални среди, разширяване на набора от данни и интеграция в облачни решения за сигурност.

3. Научни приноси

Съгласна съм по същество с предложените приноси на дисертационния труд и ги определям като научно-приложни и приложни.

Те могат да бъдат отнесени към *Формулиране и обосноваване на нова хипотеза (концепция); Създаване на нови методи*; *Доказване с нови средства на съществени нови страни на вече съществуващи научни области и проблеми; Получаване на потвърдителни факти*.

Научно-приложни приноси:

- Разработен е **нов методологичен подход** за откриване на DDoS атаки, базиран на дълбоко обучение върху реални уеб сървърни логове.
- Проведен е **сравнителен анализ на ML и DL модели** с ясно количествено оценяване на ефективността им.
- Въведен е **интерпретируем модел чрез SHAP анализ**, който обяснява влиянието на отделните признаци върху решенията на модела.
- Предложен е **универсален експериментален протокол**, който може да се използва при обучение и тестване на други типове атаки (SQL Injection, XSS и др.).

Приложни приноси:

- Създаден е **реалистичен набор от данни** за DDoS атаки, базиран на български сървърна инфраструктура, който може да се използва за обучение на киберспециалисти.
- Разработеният модел може да бъде **интегриран в системи за мониторинг и откриване на инциденти** в публични и частни организации.
- Методологията може да се **приложи при обучение на студенти по киберсигурност** за демонстрация на AI базирани механизми за защита.
- **Доказана генерализираща способност** на системата и потенциал за прилагане при други видове кибератаки

4. Публикации по дисертационния труд

1. A. Sabra, N. Rmeiti, and M. Atieh, “Using Machine Learning Techniques to Detect Cyberattacks in Smart Homes: A Survey,” in 2023 International Scientific Conference on Computer Science (COMSCI), IEEE, Sep. 2023, pp. 1–6. doi: 10.1109/COMSCI59259.2023.10315831.

2. M. ATIEH, O. MOHAMMAD, A. SABRA, and N. RMAYTI, “IdO, apprentissage profond et cybersécurité dans la maison connectée : une étude,” in Cybersécurité des maisons intelligentes, ISTE Group, 2024, pp. 215–256. doi: 10.51926/ISTE.9086.ch6.

3. M. Atieh, O. Mohammad, A. Sabra, and N. Rmayti, “IOT, Deep Learning and Cybersecurity in Smart Homes: A Survey,” in Cybersecurity in Smart Homes, Wiley, 2022, pp. 203–244. doi: 10.1002/9781119987451.ch6.

4. G. Momcheva, A. Sabra, and N. Rmeiti, MACHINE LEARNING in CYBERSECURITY. Varna Free University “Chernorizetz Hrabar” University Publishing House, 2022.

5. A. Sabra, N. Rmeiti, and Z. Minchev, “Machine Learning Approaches to Detect Application Layer DDoS Attacks”, Applications of Mathematics in Engineering and Economics (AMEE’24); AIP Publishing (accepted) .

6. Rmeiti, N., Sabra, A., Shibbi, A., & Marinova, R. (2025). Detecting Human Emotions Using Machine Learning Techniques: A Comprehensive Approach. 2025 International Conference on Computer Systems and Technologies (CompSysTech), 01–09. https://doi.org/10.1109/CompSysTech65493.2025.11137007

Съгласно Правила и процедури за приемане и обучение на докторанти и придобиване на ОНС „Доктор” във ВСУ „Ч. Храбър”, за присъждане на ОНС „доктор“ е необходимо (освен представяне на дисертационен труд – Показател А - 50 т.) покриване на изисквания за Публикационна дейност минимум 30 т. Публикациите отразяват основни резултати от изследванията в дисертацията и може да се счита, че е постигната необходимата публичност пред научната общност. От представените научни публикации се вижда, че точките надминават Минималните национални изисквания от 30 точки. Докторантът не е представил данни за цитирания на публикациите. Приложена е справка за плагиатство с добър процент.

5. Автореферат

Авторефератът е структуриран в общ обем от 38 стр. Изложението представлява голяма по обем извадка от дисертационния труд. Отразена е основната част от изследванията, както и постигнатите резултати, включени са приносите и публикациите, свързани с дисертацията. Считам, че Авторефератът удовлетворява изискванията и е с оптимален обем.

6. Мнения, препоръки и забележки по дисертационния труд

Нямам критични забележки, но в бъдеще добре би било да се направи по-задълбочен анализ на рисковете от реално внедряване в производствени среди и да се направят тестове в реална или симулирана корпоративна инфраструктура. Може да се добави сравнение с платформи като Snort, Suricata, Cloudflare ML, за по-пълна оценка на предимствата.

Препоръчително е да се опишат конкретни технически изискавания за интеграция на модела, като се уточнят минимални хардуерни/софтуерни параметри за внедряване. При по-нататъшни изследвания може да се изследва икономическата ефективност, да се оценят разходите и да се направи анализ на потенциалните икономии от внедряването на интелигентна защита.

7. Заключение

Отправените препоръки и забележки не омаловажават стойността на разработката. Те могат да бъдат взети предвид при следващи разработки, свързани с разгръщане на дисертационния труд.

Докторантът притежава задълбочени теоретични знания по тематиката, както и способности за провеждане на самостоятелни научни изследвания и практическо внедряване на постигнатите резултати.

Считам, че дисертацията е актуална, предложените методики могат да намерят широко приложение в различни сфери. Представеният дисертационен труд като значимост на изследванията представлява една задълбочена и завършена разработка, съдържа достатъчно научноприложни и приложни приноси. Удовлетворени са изискванията на *Закона за развитие на академичния състав в Република България* и на *Правилника* за неговото прилагане, както и на *Правила и процедури за приемане и обучение на докторанти и придобиване на ОНС „Доктор“* във ВСУ „Черноризец Храбър”.

Постигнатите резултати ми дават достатъчно основание да дам положителна оценка на представената дисертация и да предложа на уважаемото Научно жури да присъди на **Али Сабра** образователната и научна степен „доктор“ в докторската програма „Информационни системи и технологии, информатика и компютърни науки“, професионално направление 4.6. „Информатика и компютърни науки“.

16.01.2026 г. Рецензент: 

/ проф. д-р инж. Теодора Бакърджиева/