СТАНОВИЩЕ

от проф. Даниела Иванова Борисова – Институт по Информационни и комуникационни технологии при БАН
член на Научното жури, назначена от Ректора на Варненския свободен университет „Черноризец Храбър“ със заповед № 892 от 28 ноември 2025 г.

относно дисертация на ALI MOHAMAD SABRA
на тема “Deep Learning Approach for Modeling DDoS Attacks in Cybersecurity”
представена за придобивана на образователна и научна степен „Доктор“
по докторска програма “Информационни системи и технологии, компютърни науки и компютърни науки”, професионално направление 4.6. “Информатика и компютърни науки”

На първото заседание на научното жури, проведено на 5 декември 2025 г., бях избрана да изготвя становище по процедурата, за което получих всички необходими документи.

АКТУАЛНОСТ

Моделирането на DDoS атаки е критична практика в киберсигурността, защото позволява на организациите да разбират, предвиждат и защитават срещу една от най-разрушителните и скъпи форми на кибератаки. DDoS моделирането помага на екипите по сигурността да анализират вектори на атака (обемни, протоколни, на ниво приложение), модели на трафик и аномалии, координация на нападателите и поведение на ботнет мрежите. Чрез моделиране на тези характеристики, защитниците получават представа за това как атаките се развиват и разпространяват. Традиционните методи за откриване често разчитат на прагове или статични правила, докато моделирането позволява откриване въз основа на поведение, идентифициране на аномалии с помощта на статистически и ML модели и

системи за ранно предупреждение, преди да възникнат пълномащабни атаки. Моделирането подкрепя проактивна, а не реактивна защита. DDoS моделите също така помагат за оценка на максималното натоварване на трафика, точките на изчерпване на ресурсите и праговете на влошаване на услугите. Това позволява по-добро мащабиране на инфраструктурата, планиране на резервирането и гаранции за наличност на услугите. Съвременните DDoS атаки се адаптират динамично. Моделирането предоставя етикетирани набори от данни за обучение на ML модели, реалистични модели на трафик за тестване и враждебни сценарии за AI срещу AI защитни системи. Без моделиране, интелигентните защитни системи не могат да бъдат обучени надеждно. Не на последно място, много разпоредби и стандарти изискват оценка на риска, планиране на реагиране при инциденти и стрес тестове на критични услуги. DDoS моделирането помага за демонстриране на киберустойчивост и съответствие с регулаторните изисквания. Всичко това определя актуалността на дисертационното изследване.

ПОЗНАВАНЕ НА ИЗСЛЕДОВАТЕЛСКИЯ ПРОБЛЕМ

От направения обзор, както и от публикуваните резултати от дисертацията, може да се установи, че докторантът е добре запознат с естеството на изследваните проблеми. Като допълнително доказателство за това могат да се използват представените приложения, документиращи подробности за имплементацията на LSTM-базиран модел с Conv1D, нормализиране на партиди, планиране на скоростта на обучение и ранно спиране, използвани за откриване на DDoS атаки на приложно ниво от лог файлове за достъп до уеб сървър.

АНАЛИТИЧНИ ХАРАКТЕРИСТИКА

Дисертацията на Ali Mohamad Sabra е с общ обем от 118 страници, включително 23 фигури, 5 таблици и 77 цитирани източника. Тя е структурирана по следния начин: благодарности, резюме, 3 глави, заключение – обобщение на резултатите и бъдещи насоки на изследване,

списък с публикации, библиография и 4 приложения. На страница 13 основната цел на дисертационното изследване е дефинирана като „Да се разработи и оцени интелигентна система за откриване на DDoS атаки на приложно ниво, използвайки модели за машинно обучение и дълбоко обучение, обучени върху реални файлове с логове за достъп до уеб сървъри”.

АВТОРЕФЕРАТ И АВТОРСКА СПРАВКА

Представеният автореферат отразява съдържанието на дисертационния труд, с изключение на библиографията, и е съобразен с изискванията на Закона за развитие на академичния състав в Република България (ЗРАСРБ) и Правилника за неговото прилагане. От представената декларация за оригиналност, както и от публикациите по темата на дисертацията, може да се определи, че описаните резултати са лично дело на автора. Освен това, следва да се отбележи, че докладът от проверката в платформата Strikeplagiarism.com показа, че коефициентът на сходство 1 е 2,02%, а коефициентът на сходство 2 е 0,00%, което потвърждава оригиналността на резултатите от проведеното изследване.

ОЦЕНКА НА СЪОТВЕТСТВИЕТО С МИНИМАЛНИТЕ НАЦИОНАЛНИ ИЗИСКВАНИЯ И С ДОПЪЛНИТЕЛНИТЕ ИЗИСКВАНИЯ НА ПРАВИЛНИКА ЗА ПРИЛАГАНЕ НА ЗРАСРБ

Представени са общо 6 публикации, 5 от които са публикувани, а една е приета за публикуване. Три от публикациите са индексирани в Световната база данни за научна информация Scopus. Докторантът е първи автор на 2 от тези публикации. Всички публикации са колективни. Следователно, съгласно Правилника за прилагане на LDASPB, публикуваните публикации имат еквивалент от 54 точки, което надвишава минималните национални изисквания и специфичните изисквания на Варненския свободен университет „Черноризец Храбър“ от 30 точки за образователната и научна степен „Доктор“.

ПРИНОСИ

Предлага се емпиричен методологичен подход, който комбинира усъвършенствани техники за машинно обучение (ML) и дълбоко обучение (DL) за откриване на DDoS атаки на приложното ниво, пригоден за уеб трафик. Методологията е базирана на рамката „Междуиндустриален стандартен процес за извличане на данни“, която включва разбиране на бизнеса, последвано от разбиране на данните, подготовка на данните, моделиране, оценка и накрая внедряване.

Приемам приносите, формулирани от докторанта, и ги оценявам като научно-приложни, обогатяващи съществуващите знания.

КРИТИЧНИ КОМЕНТАРИ И ПРЕПОРЪКИ

Нямам критични забележки, но е интересно да се тества как предложената методология ще се представи върху реален набор от данни за IoT трафик, вместо върху симулирани DDoS атаки в лабораторна мрежа. Добро впечатление прави използването на обясним изкуствен интелект чрез SHAP-базирана интерпретируемост, което позволява подобряване на разграничаването между доброкачествен и злонамерен трафик на приложения, като по този начин се увеличава прозрачността и доверието.

ЗАКЛЮЧИТЕЛНА КОМПЛЕКСНА ОЦЕНКА

Получените резултати по темата на дисертационното изследване показват, че ALI MOHAMAD SABRA притежава необходимите теоретични знания и практически умения в областта на информатиката и компютърните науки, както и способности за самостоятелна научна изследователска работа. Представената дисертационна работа отговаря на изискванията на Закона за развитие на академичния състав в Република България, Правилника за неговото прилагане, както и на Правилника за специфичните условия за придобиване на научни степени и за заемане на академични длъжности във Варненския свободен университет „Черноризец Храбър“. Получените

резултати по темата на дисертационното изследване ми дават достатъчно основание да дам положителна оценка на представената дисертация и предлагам на уважаемото Научно жури да присъди на ALI MOHAMAD SABRA образователната и научна степен „доктор“ в докторската програма „Информационни системи и технологии, компютърни науки и компютърни науки“, професионално направление 4.6. „Информатика и компютърни науки“.

12.01.2025 Член на научното жури:

/проф. д.н. Даниела Борисова/