РЕЦЕНЗИЯ

от проф. д-р Васил Гуляшки

Институт по информационни и комуникационни технологии –БАН
за дисертационен труд за придобиване на образователната и научна степен **„доктор“** по професионално направление 4.6. „Информатика и компютърни науки“, Докторска програма „Информатика“

Относно: Дисертационен труд на **Илиян Магдаленов Барзев** на тема:

“ИЗСЛЕДВАНЕ И АНАЛИЗ НА ВЪЗМОЖНОСТИТЕ ЗА ОТКРИВАНЕ НА ЗЛОНАМЕРЕН СОФТУЕР ЧРЕЗ СРЕДСТВАТА НА МАШИННО ОБУЧЕНИЕ”

Със заповед № 27/30.01.2026 г. на директора на ИИКТ – чл.-кор. д.м.н. Светозар Маргенов - във връзка с процедурата за придобиване на образователната и научна степен „доктор“ по професионално направление 4.6 Информатика и компютърни науки, докторска програма „Информатика” от Илиян Магдаленов Барзев с дисертация на тема „Изследване и анализ на възможностите за откриване на злонамерен софтуер чрез средствата на машинното обучение“ съм включен в състава на Научното жури.
Като член на научното жури съм получил:

1. Дисертация за присъждане на образователна и научна степен „доктор“ на български език;
2. Автореферат на български език;
3. Автореферат на английски език;
4. Справка за изпълнение на минималните национални изисквания за придобиване на образователната и научна степен „доктор“;
5. Списък на публикациите по темата на дисертационния труд;
6. Копия на публикациите по дисертационния труд;
7. Декларация за оригиналност на получените резултати;
8. Доклад за сходство от системата StrikePlagiarizm.com.

При оценката на дисертационния труд, определящи са условията на Закона за развитие на академичния състав в Република България (ЗРАСРБ), ППЗРАСРБ (Постановление No. 26 от 13 февруари 2019 г.) и Правилника на ИИКТ - БАН за прилагане на Закона за развитието на академичния състав в Република България.

1. Съгласно чл. 27 (1) от ЗРАСРБ "дисертационният труд трябва да съдържа научни или научноприложни резултати, които представляват оригинален принос в науката. Дисертационният труд трябва да показва, че кандидатът притежава задълбочени теоретични знания по съответната специалност и способности за самостоятелни научни изследвания".
2. Според чл. 27 (2) от ЗРАСРБ дисертационният труд трябва да бъде представен във вид и обем, съответстващи на специфичните изисквания на първичното

звено. Дисертационният труд трябва да съдържа: заглавна страница; съдържание; увод; изложение; заключение – резюме на получените резултати с декларация за оригиналност; библиография.

Научен ръководител на дисертацията е проф. д.н. Даниела Борисова

Актуалност на темата

Откриването и анализът на зловреден софтуер е особено актуално в днешно време при наличието на войни, многобройни кибер-заплахи и хакерски атаки. защитата от зловреден софтуер е важна по няколко причини. Защитата срещу злонамерен софтуер е важна по няколко причини: 1) сигурност на данните (лични и финансови данни), загубата на която води до кражба на самоличност или финансови загуби. 2) Щети върху компютърните системи и информационните мрежи - заразяването с компютърни вируси води до загуба на информация и скъпи ремонти. 3) Влияние върху производителността – могат да възникнат сривове, нарушаващи нормалния ритъм на работа, което е свързано със загуби на време и ресурси. 4) Защитата на данните от страна на много организации се изисква по закон.

Считам, че полезността и актуалността на дисертационните изследвания е лесно видима и разбираема. Оценявам положително тематичната насоченост и актуалната проблематика на дисертационното изследване.

Степен на познаване състоянието на проблема и творческа интерпретация на литературния материал

Въз основа на първата обзорна глава оценявам положително степента на познаване на проблема за анализа и техниките за откриване и класификация на зловреден софтуер.

Съответствие на избраната методика на изследване с поставената цел и задачи на дисертационния труд

Избраната методика на изследване е логична и последователно изпълнявана. Тя включва:

- Анализ на научната литература – с цел класифициране на методите за откриване на зловреден софтуер с помощта на машинно обучение.
- Разработване на математически модели, чрез които да се направи избор на софтуер за подходяща виртуална машина за целите на откриването на зловреден софтуер.
- Разработване на подход за статичен анализ за откриване на зловреден софтуер с оптимизиране извличането на характеристики чрез комбиниране на различни алгоритми за машинно обучение.
- Разработване на рамка за статична класификация на зловреден софтуер, която използва оптимизация на функции и ансамблово обучение.
- Разработване на адаптивна рамка, съобразена с доверието, за класификация на зловреден софтуер с корекции за обратна връзка, която включва самоосъзнат класификатор на модели.

ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

Дисертационният труд е в обем от 143 страници с 20 таблици и 43 фигури, и се състои от увод, три глави, заключение и библиография от 155 източника. Съдържа списък на използваните съкращения.

Целта на дисертационния труд е да се изследват и анализират възможностите за откриване на злонамерен софтуер чрез средствата на машинно обучение, на база на които да се предложат подходящи хибридни модели, рамки и приложения за получаване на по-добри резултати при откриването на зловреден софтуер. За реализиране на тази цел са формулирани и изпълнени **следните задачи**:

1) да се направи анализ на различни алгоритми на машинното обучение относно тяхното представянето за целите на откриване на зловреден софтуер;

2) да се определи подходяща виртулна машина, която да се използва при провеждане на тестове за откриване и класификация на зловреден софтуер;

3) да се предложи подобрен подход за статичен анализ за откриване на зловреден софтуер чрез оптимизиране извличането на характеристики и комбинирайки различни алгоритми за машинно обучение;

4) да се предложи рамка за статична класификация на зловреден софтуер, използваща оптимизация на функции и ансамблово обучение;

5) да се предложи самоосъзната класификация на зловреден софтуер чрез рутиране на модели на базата на система за доверие за избора и обяснимост на характеристиките;

6) да се предложи адаптивна рамка, съобразена с доверието, за класификация на зловреден софтуер с корекции за обратна връзка.

Формулираните цел и задачи имат научен и научно-приложен потенциал за изследвания и приложение в областта на информационните процеси, информационните системи и технологии.

Кратка аналитична характеристика на материала, върху който се градят приносите на дисертационния труд

Дисертационният труд има вътрешна логика и съответства на изискванията за академична изследователска работа.

В първа глава е направен анализ на различни алгоритми на машинното обучение относно тяхното представянето за целите на откриване на зловреден софтуер. Представено е тестване на приложимостта на алгоритми за двоична класификация за откриване на зловреден софтуер, използвайки публичен набор от данни, заразен с 9 вида зловреден софтуер, чрез предложена методология..

Във втора глава са предложени два модела за избор на виртуална машина за целите на провеждането на експерименти за откриване на зловреден софтуер. Представен е подобрен подход на статичен анализ чрез оптимизиране извличането на характеристики, комбинирайки различни алгоритми за машинно обучение за откриване на зловреден софтуер. Представена е предложена рамка за статична класификация на зловреден софтуер, използваща оптимизация на функции и ансамблово обучение. За прецизиране на класификацията на зловредния софтуер е предложена адаптивна рамка, съобразена с доверието, позволяваща класификация на зловреден софтуер с възможност за корекции чрез обратна връзка.

В трета глава са представени резултатите от проведеното тестване на предложените модели за избор на софтуер за виртуална машина. Описани са резултати от тестуването на предложения подобрен подход на статичен анализ чрез оптимизиране извличането на характеристики, комбинирайки различни алгоритми за машинно обучение. Описани са числени експерименти, използвайки предложената рамка за статична класификация на

зловреден софтуер, в която е направено оптимизиране на функциите и е използвано ансамблово обучение.
В заключението е направено обобщение на получените резултати при проведените изследвания са посочени някои насоки за бъдещи изследвания.
Нямам критични забележки по дисертацията в методологично отношение.

Публикации
По дисертационния труд са представени **4 публикации,** които са в съавторство. Три от тях са в издания с импакт ранг (SJR) в квартил Q4 на Scopus. До момента има 8 забелязани цитирания на публикациите. Публикациите са показателни за личния принос на докторанта. С тях се покриват минималните национални изисквания за придобиване на образователната и научна степен „доктор“. Освен това е представен списък от три приети за публикуване статии. Представените публикации дават основание да се приеме, че изследването има необходимата публичност.

ПРИНОСИ

Получените **резултати** са систематизирани в следните **приноси**:

1) Предложени са два математически модела, чрез които може да се направи избор на софтуер за подходяща виртуална машина за целите на експерименталното тестване за откриване на зловреден софтуер.

2) Предложен е подобрен подход за статичен анализ за откриване на зловреден софтуер чрез оптимизиране извличането на характеристики чрез комбиниране на различни алгоритми за машинно обучение. Проведените тестове с предложените хибридни алгоритми показват по-добра производителност.

3) Предложена е рамка за статична класификация на зловреден софтуер, която използва оптимизация на функции и ансамблово обучение. Резултатите показват, че анализът на фалшиво положителните резултати за ансамбъла е значително по-нисък от този на отделните модели.

4) Предложена е самоосъзнатата класификация на зловреден софтуер чрез рутиране на модели на базата на система за доверие за избора и обяснимост на характеристиките. Логиката на рутиране увеличава мощността на ансамбъла с решения, базирани на доверие, и предоставя гъвкав механизъм, полезен както за минали, така и за съвременни характеристики на зловредния софтуер.

5) Предложена е адаптивна рамка, съобразена с доверието, за класификация на зловреден софтуер с корекции за обратна връзка. Тази рамка е едновременно адаптивна и устойчива, тъй като включва самоосъзнат класификатор на модели, който използва адаптивна логика за автоматичен избор между традиционни и съвременни слоеве на моделите чрез измерване на надеждността на прогнозирането. Интеграцията на обяснимостта допринася за доверието в решенията, което се е увеличило чрез повече информация за функциите от локална и глобална гледна точка.

Приемам формулираните приноси. Считам, че представените резултати покриват в достатъчна степен обхвата на поставените цели и задачи.

Авторефератът на български език е в обем 45 стр. и представя дисертационния труд.

Авторефератът на английски език е в обем 43 стр. и представя дисертационния труд.

КРИТИЧНИ БЕЛЕЖКИ

1) При въвеждането на метриките за оценка на работата на съответните алгоритми на стр. 24 в дисертацията би трябвало да представят и съответните формули за всяка метрика.

2) В т. 2.1.1. в дисертацията се изброяват три критерия за оценка при вземането на решение за избор на софтуер за виртуална машина за откриване на зловреден софтуер. След това обаче се говори за четири критерия (виж стр. 40).

3) В дисертацията са забелязани някои правописни грешки, които лесно могат да бъдат отстранени.

КОМЕНТАР

Получените резултати в дисертацията показват високата работоспособност на разработеното приложение „Shipka Guard“. Следва то да намери широка практическа реализация, например, в системи за киберсигурност в държавни и научни организации, в университетите, както и в предприятия в промишлеността. В тази връзка препоръчвам провеждане на рекламни демонстрации на работата на приложението и представянето му на технически изложби и панаири.

ЗАКЛЮЧИТЕЛНА КОМПЛЕКСНА ОЦЕНКА

Направените технически критични бележки не омаловажават приносите на дисертацията. Считам, че представеният дисертационен труд **отговаря** на изискванията на Закона за развитие на академичния състав в Република България. Постигнатите резултати ми дават основание убедено да предложа на уважаемото Научно жури да присъди на **Илиян Магдаленов Барзев** образователната и научна степен „Доктор” в професионално направление – 4.6 „Информатика и компютърни науки“, Докторска програма „Информатика“ за дисертацията на тема „Изследване и анализ на възможностите за откриване на злонамерен софтуер чрез средствата на машинното обучение“.

На основание
ЗЗЛД

06.03.2026 г.
гр. София