ФОНД НАУЧНИ ИЗСЛЕДВАНИЯ
Министерство на образованието и науката

Информация за финансиран на проект

Наименование на конкурса:
Конкурс за финансиране на фундаментални научни изследвания – 2021 г.
Основна научна област:
Технически науки
№ на договор:
КП-06-Н57/4
Начална дата на проекта и срок на договора:
16 Ноември 2021 36 месеца
Заглавие на проекта:
Изследване и приложение на алгоритми за машинно обучение при анализ и разработка на високо сигурен софтуер
Базова организация:
Технически Университет - София
Партньорски организации:
Софийски университет „Св. Климент Охридски“
Ръководител на научния колектив (академична длъжност, научна степен, име):
доц. д-р инж. Аделина Пламенова Алексиева-Петрова
Общ размер на договореното финансиране:
170 000 лева

Резюме на проекта (до 1 стр. в рамките на полето по-долу):

Откриването на уязвимост на софтуера изисква критично внимание по време на фазата на разработване, за да го направи сигурно и по-малко уязвимо. Уязвимият софтуер винаги е предпоставка за извършване на злонамерени дейности и до нарушават работата на софтуера, което води до милионни финансови загуби за компаниите. За да се намалят загубите, има много надеждни и ефективни системи, целящи да открият уязвимостите на софтуера още във фазите на разработка или тестване. Повечето от тях използват предимно традиционни техники за откриване на уязвимости. Липсват обаче дискусии относно ново-популярните подходи за ***машинно обучение***, като и техники за дълбоко обучение. Анализът на изследванията в областта показва, че има значителен интерес към адресирането на методи и проблеми с откриването на уязвимости, докато само малцина се интересуват от ***проблеми с кода и набора от данни***.

Сигурността като част от процеса на разработка на софтуер е непрекъснат процес, включващ хора и практики, осигуряващ поверителност на приложенията, целостта и наличността им. Сигурният софтуер е резултат от процесите на разработка на софтуер, съобразени със сигурността. Сигурността е най-ефективна, ако е планирана и управлявана на всеки етап от жизнения цикъл на разработка на софтуер, особено в критични приложения или такива, които обработват чувствителна информация.

Откриването на аномалии и атаки на приложно ниво трябва да се извършват именно на това ниво и да се позволи тяхното вграждане при непрекъсната интеграция и доставка. Познанията за изкуствения интелект, особено техниките за машинно обучение, могат да се използват за справяне с тези проблеми.

Описаните по-горе предизвикателства на **приложно ниво** (софтуер) в областта на **сигурността** дефинира *двете основни цели* на този проект. ***Първата цел*** е да се изследват и анализират ***различни подходи и алгоритми от машинно обучение за откриване, анализиране и предотвратяване на зловредните атаки към софтуерните продукти***.

Втората цел на проекта е да се изследват и предложат ***процеси на автоматизация при проектиране, реализиране и внедряване на софтуер с оглед сигурност на системата***. Особено внимание да се обърне на проблема на писането и гарантирането на сигурен код, който е свързан с първопричината за слабостите в софтуерните системи и технологии. Тя се корени в недостатъчно устойчивия и издържан откъм сигурност процес по писане на код.

Очакваните резултати от изпълнението на проекта са:

- подобряване на квалификацията на учените чрез съвместни изследвания и разработване за постигането на целите на проекта;
- публикуване на резултатите от изследванията в рецензирани и индексирани международни научни издания с импакт фактор IF (Web of Science) и SJR (SCOPUS);
- участие на млади учени, докторанти и пост-докторанти.

Членове на научния колектив

Организации/участници[1]	***Бележка***[2]
Базова организация:	
Техническият университет – София	
Ръководител на научния колектив	
доц. д-р инж. Аделина Пламенова Алексиева-Петрова	
Участници:	
проф. д-р Милена Кирилова Лазарова- Мицева доц. д-р инж. Антония Тодорова Ташева доц. д-р Веска Стефанова Ганчева Венета Калинова Йосифова Добрин Александър Иванов	 млад учен, докторант докторант
Партньорска организация:	
Софийски университет „Св. Климент Охридски“	
Участници:	
доц. д-р инж. Милен Йорданов Петров ас. Явор Иванов Данков Георги Калинов Йосифов Петър Пашинов Събев	 млад учен млад учен, докторант млад учен, докторант

[1] Отбележете академичната длъжност, научната степен, име и фамилия на всеки участник като включите и участниците, които са работили по проекта не през целия период за изпълнение на проекта

[2] Отбележете дали участникът в колектива е млад учен (МУ), постдокторант (ПД), докторанти (ДО) или студенти (СТ), или учен от чужбина (УЧ).