„КОНКУРС ЗА ФИНАНСИРАНЕ НА ФУНДАМЕНТАЛНИ НАУЧНИ ИЗСЛЕДВАНИЯ – 2016 г.”

Анотация на проекта

Наименование на конкурса:
КОНКУРС ЗА ФИНАНСИРАНЕ НА ФУНДАМЕНТАЛНИ НАУЧНИ ИЗСЛЕДВАНИЯ – 2016 Г.
Основна научна област/тематично направление, в което проектът кандидатства:
ТЕХНИЧЕСКИ НАУКИ/ ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ ТЕХНОЛОГИИ
Допълнителни научни области/тематични направления при интердисциплинарни проекти:
/МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ, ИЗКУСТВЕН ИНТЕЛЕКТ
Заглавие на проекта:
ПОВИШАВАНЕ НИВОТО НА МРЕЖОВАТА И ИНФОРМАЦИОННА СИГУРНОСТ ЧРЕЗ ИЗПОЛЗВАНЕ НА ИНТЕЛИГЕНТНИ МЕТОДИ
Вид на планираните научни изследвания (фундаментални или приложни):
ФУНДАМЕНТАЛНИ
Базова организация:
ТЕХНИЧЕСКИ УНИВЕРСИТЕТ - СОФИЯ
Партньорски организации:
-
Ръководител на научния колектив (академична длъжност, научна степен, име):
Доц. д-р Румен Трифонов, ръководител на катедра „Информационни технологии в индустрията“, Факултет по Компютърни системи и управление

Ръководител на научния колектив:
(подпис)

/доц. д-р инж. Румен Трифонов/

Ръководител на базовата организация:
(подпис и печат)

/проф.д-р инж. Георги Михов/

Резюме на проекта:

В съвременното общество информационните и комуникационни технологии са пронкнали дълбоко и са се превърнали в основа на всички дейности в икономиката, администрацията, обществото и личния живот. Дигиталните инфраструктури се превръщат от поддържаща среда в основен и критичен фактор за управлението и нормалното функциониране на всички ресурси и системи с национално значение, на развитието на конкурентна и иновативна икономика, прозрачно управление и на модерно демократично гражданско общество. Същевременно, нарастващата и необратима дигитална зависимост на основните функции и дейности на обществото поражда нови значими рискове и заплахи.Поради това, постигането на достатъчно високо ниво на мрежовата и информационна сигурност е от изключителна важност за надеждното ефективно функциониране на тези дейности. Особено това се проявява в т.н. „критични инфраструктури“, осигуряващи жизнено важни функции на икономиката и обществото (енергетика, транспорт, банкови операции, здравеопазване, сигурност и отбрана и пр.).

От друга страна, паралелно с позитивните явления на информационното общество се появи и бурно се разпространи в световен мащаб и неговия негативен антипод – световната кибер-престъпност. Според болшинството анализатори, тя отбелязва вече пето поколение, характеризиращо се с автоматизация на разработването и разпространението на инструментите за атака, както и интеграция в рамките на няколко комплекта инструменти, които изпълняват различни функции. Една от особеностите на петото поколение са т.н. "Модерни настойчиви заплахи (APT - Advanced Persistent Threats)" - целенасочени атаки срещу конкретни организации от определени, добре координирани кибер-престъпници. В общността на експертите, APT най-често се отнася до сложни атаки, насочени към правителства и корпорации. APT често се използва от държавни органи или техни агенти, както и от терористични и сепаратистки политически групи.

Свързаността и зависимостта в кибер пространството позволява пробивът в сигурността или дефект на една комуникационна и информационна система от даден сектор да доведе до каскаден ефект и отказ в други, отново със сериозни възможни последици и вреда на жизненоважни услуги. Реакцията при такива инциденти налага координирани действия и превантивни мерки за минимизиране на възможностите за прерастване в кризи, както и за адекватни последващи действия, които да доведат до своевременното възстановяване на нормалното функциониране на системите.

В тези условия преобладаващото количество експерти се обединяват около тезата, че традиционните методи за защита са вече слабо продуктивни и е необходим качествен преход към нови инструменти за реализация на мрежовата и информационна сигурност.

Едно от посочваните с приоритет направления на този преход е широкото приложение на интелигентни методи за анализ на обменяната информация, на потоците в мрежите, на източниците на заплахи, както и планиране на ефективни мерки за въздействие, в т.ч. проактивни (т.е. атакуващи основните източници на заплаха, такива като управляващи центрове на „бот-нет“-и пр.).

Целта на проекта е да се систематизират, анализират и оценят различните видове приложения на „изкуствения интелект“ в компютърната сигурност. Да се изберат най-перспективните за националната практика методи. Да се изготвят препоръки за тяхното използване.

Необходимо е да се отбележи, че съгласно литературните източници приложенията на изкуствения интелект се употребяват в три основни действия, свързани с компютърната сигурност: откриване (detection); отстраняване на последствията (repair); отбрана (defense) – пасивна и активна.

В настоящия проект се предвижда да се обърне основно внимание на първото действие. Ще бъде направен опит за обосноваване и формулиране на елементи от новото понятие „Кибер-разузнаване“.

Предварителните анализи на методите на „изкуствения интелект“, използвани в системите за мрежова и информационна сигурност, показват, че повечето от тях притежават както достойнства, така и недостатъци. Една от основните цели на проектното предложение е, след като се проведе задълбочен анализ, съпроводен от експериментално изследване на най-перспективните методи, да се направи опит за подобряване на положителните страни и избягване на недостатъците – или чрез модифициране на избран метод, или за хибридизация на няколко избрани метода.

Членове на научния колектив

Организации/участници[1]	*Бележка*[2]	*Подпис*
Базова организация:		
Технически университет - София		
Ръководител на научния колектив		
доц. д-р инж. Румен Иванов Трифонов		
Участници:		
проф. д-р инж. Огнян Наков Наков		
проф. д-р инж. Даниела Асенова Гоцева		
проф. д-р инж. Милена Кирилова Лазарова-Мицева		
проф. д-р инж. Христо Ангелов Христов - пенсионер		
доц. д-р инж. Пламен Иванов Вачков - пенсионер		
доц. д-р инж. Славчо Алекснадров Манолов - пенсионер		
Доц. д-р инж. Радослав Даков Йошинов – Лаб. по телематика, БАН		
доц. д-р инж. Георги Илинчев Попов		
доц. д-р инж. Аделина Пламенова Алексиева-Петрова		
ас. инж. Галя Веселинова Павлова	ДО	
маг. инж. Георги Руменов Цочев	ДО	
инж. Момчил Мариянов Петров	СТ	

[1] Отбележете академичната длъжност и научната степен на всеки участник
[2] Отбележете дали участникът в колектива е млад учен (МУ), постдокторант (ПД), докторанти (ДО) или студенти (СТ), или учен от чужбина (УЧ)