РАБОТНА ПРОГРАМА

1.1. Описание на работна програма на проекта

Основните дейности по работата по проекта са разделени на работни пакети (РП). В рамките на изпълнението на целият проект се разграничават следните работни пакет:

РП1: Анализ за възможностите за ефективно приложение на методите на изкуствения интелект в кибер-сигурността на индустриалните системи

Този работен пакет е свързан с описаните по-горе подцели на проекта А и Б. Акцентира се върху спецификите на кибер-заплахите, насочени към т.н. кибер-физични системи, като по аналогия с информационните системи, където тази проблематика е по-добре проучена, ще се изследва приложението на военните методи, такива като „веригата на убийството“ и „кибер-разузнаването“, а също така такива категории, като: агенти на заплахата, вектор на заплахата. Всичко това е свързано с проблема на ефективния избор на най-подходящи методи на изкуствения интелект за специфичните цели на кибер-защитата на индустриалните системи.

От своя страна, анализът на съществуващите и използваните вече за целите на кибер-сигурността методи на изкуствения интелект ще се фокусира именно върху спецификата на индустриалните системи.

Дейност 1.1. Анализ на заплахите, насочени към индустриалните системи, в частност, към техните кибер-физични компоненти.

Дейност 1.2. Анализ на съществуващите и използваните вече за целите на кибер-сигурността методи на изкуствения интелект от гледна точка на използването им за кибер-защита на индустриалните системи. Разработка на критерии за избор.

Дейност 1.3. Подготовка на научни статии и участия в национални и международни научни конференции

РП2: Моделиране и експериментално изследване на „базов“ метод на изкуствен интелект

Вторият работен пакет е предназначен да реализира описаните по-горе под-цели В и Г. Преди всичко, на база на разработените в Работен пакет 1 критерии, ще се избере „базов“ метод, който ще се заложи в теоретичния модел на приложение, реализиращо кибер-защита на индустриална система.

По предварителни оценки, базирани от опита от експериментирането с информационни системи, вероятно за основа ще бъде взета мулти-агентна система от мобилни агенти.

Въз основа на модела ще се изгради експериментална постановка и ще се изследва поведението на приложението при симулирани кибер-атаки от различен характер. Ще се проведе анализ на ефективността на детектирането на заплахите и отразяването на съответните атаки.

Дейност 2.1. Теоретичен модел.

Дейност 2.2. Създаване на експериментална и изследователска постановка на теоретичния модел.

Дейност 2.3. Изследване на работата на експерименталния модел.

Дейност 2.4. Подготовка на научни статии и участия в национални и международни научни конференции

РП3: Разработване и изследване на модифициран метод за повишаване нивото на кибер-сигурността на индустриални системи

Третият работен пакет е свързан с разработване и изследване на модифициран метод за повишаване нивото на кибер-сигурността в съответствие с посочената по-горе под-цел Д. Въз основа на резултатите от изследванията на създадения теоретичен модел чрез методи и подходи спомагащи за решаване на проблемите в кибер-сигурността ще се разработи модифициран метод, съчетаващ силните страни и компенсиращ слабите страни на няколко метода на изкуствения интелект.

Дейност 3.1. Разработване на модифициран метод.

Дейност 3.2. Експериментално изследване на модифицирания метод.

Дейност 3.3. Подготовка на научни статии и участия в национални и международни научни конференции

РП4: Разпространение на резултатите

За разпространение на резултатите, екипът на проекта ще разработи специален план, включващ следните дейности:

Дейност 4.1. Създаване на интернет страница на проекта и представяне на проекта.

Дейност 4.2. Организиране на семинари с цел разпространяване на научните резултати от проекта.

Дейност 4.3. Публикуване на научни статии в научни издания, реферирани и индексирани в световни вторични литературни източници, и/или в издания с импакт фактор IF (Web of Science) и/или импакт ранг SJR (SCOPUS).

Дейност 4.4 Изготвяне на доклад за препоръчително използване на методи на изкуствения интелект за повишаване нивото на кибер-сигурността на индустриални системи.

Публикуваните, приетите или изпратените за печат научни статии в сборници или в списания с импакт фактор и/или импакт ранг ще предоставят полученото ново знание от фундаменталните научни изследвания по проекта на широката световна научна общност чрез достъп до реферирани и индексирани в световни вторични литературни източници издания с/без импакт фактор, IF (Web of Science) и/или импакт ранг SJR (SCOPUS), както и представянето на специално разработения в края на проекта доклад за препоръчително използване на методи на изкуствения интелект за повишаване нивото на кибер-сигурността на индустриални системи ще насочи учени и

заинтересовани експерти от бизнеса за възможността за потенциална бъдеща разработката на реални приложни системи от последно поколение с използване на интелигентни методи в кибер-сигурността на индустриалните системи.

1.2. График за изпълнение на проекта

График за изпълнението проекта

РП/месец	01-03	04-06	07-09	09-12	13-15	16-18	19-21	22-24	25-27	28-30	31-33	34-36
РП 1												
РП 2												
РП 3												
РП 4												