

RESEARCH PLAN AND TASKS

1.1. Description of the project's outline and work break down structure

The main activities of the project are divided into work packages (WP). Within the framework of the implementation of the entire project these work packages can be distinguished:

WP 1 Analysis of the Possibilities for the Effective Application of Artificial Intelligence Methods in the Cyber Security of Industrial Systems

This work package is related to the sub-objectives of Project A and B, described above. It focuses on the specifics of the cyber threats targeting the so-called cyber-physical systems, similar to information systems where this issue is better studied. The application of military methods such as the "kill chain" and "cyber intelligence" will be explored, as well as categories: threat agents, threat vector.

All this is connected with the problem of effectively selecting the most appropriate artificial intelligence methods for the specific purposes of cyber-protection of industrial systems.

For its part, the analysis of existing and already used for the purposes of cybersecurity artificial intelligence methods will focus precisely on the specifics of industrial systems.

Task 1.1 Analysis of threats targeting industrial systems, in particular their cyber-physical components

Task 1.2 Analysis of existing and already used for the purposes of cybersecurity artificial intelligence methods in terms of their use for cyber defence of industrial systems. Development of selection criteria

Task 1.3 Preparation of scientific articles and participation in national and international scientific conferences

WP 2: Modelling and experimental study of a "basic" artificial intelligence method

The second working package is intended to realize the sub-objectives C and D described above. First of all, based on the criteria developed in Working Package 1, a "basic" method will be chosen, which will be incorporated into the theoretical model of the application implementing the cyber protection of industrial system.

According to the preliminary estimates, based on the experience of experimenting with information systems, a multi-agent system of mobile agents is likely to be taken as the basis.

An experimental set-up will be built on the model and the application behavior of simulated cyber-attacks of different nature will be investigated. An analysis of the effectiveness of threat detection and the reflection of the respective attacks will be conducted.

- Task 2.1 Creating a theoretical model based on the chosen "base" method
- Task 2.2 Creation of experimental and research settings of the theoretical model
- Task 2.3 Investigation of the experimental model
- Task 2.4 Preparation of scientific articles and participation in national and international scientific conferences

WP 3: Development and testing of a modified method for increasing the level of the cyber security of industrial systems

The third working package is related to the development and research of a modified method for increasing the level of cybersecurity in accordance with the above sub-objective E. Based on the results of the research of the created theoretical model through methods and approaches that help to solve the problems in cybersecurity, a modified method will be developed that combines strengths and compensates for the weaknesses of several artificial intelligence methods.

- Task 3.1 Development of a modified method
- Task 3.2 Experimental testing of the modified method
- Task 3.3 Preparation of scientific articles and participation in national and international scientific conferences

WP 4: Dissemination of the results

To disseminate the results, the project team will develop a specific plan including the following activities:

- Task 4.1 Creating a project website and project presentation
- Task 4.2 Organizing seminars to disseminate research results from the project
- Task 4.3 Publication of scientific articles in scientific journals, refereed and indexed in worldwide secondary literary sources, and/or in publications with Impact Factor IF (Web of Science) and / or Impact Rank SJR (SCOPUS)
- Task 4.4 Preparation of a report on the recommended use of artificial intelligence methods to increase the cybersecurity level of industrial systems

Published, accepted or submitted scientific articles in proceedings or in journals with Impact Factor and/or Impact Rank will provide new knowledge from the basic research on the project to the wider scientific community by accessing refereed and indexed worldwide secondary literature sources publications with/without IF (Web of Science) and/or Impact Rank SJR (SCOPUS), as well as the presentation of the special prepared at the end of the project report on the recommended use of intelligent methods to increase the level of cybersecurity in industrial systems will guide scientists and interested business experts on the possibility for future potential development of real-world, latest-generation application systems using intelligent methods in cybersecurity of industrial systems.

