Brief information about the project

Name of the project	AP19174716 «Development of a decision support system based on Bayesian networks to improve the effectiveness of detecting intrusions into computer systems» (0123PK00972)
Relevance	Analysis of existing intrusion detection systems and event collection and correlation systems (Security Information and Event Management, SIEM) shows a tendency to intellectualize data analysis processes that are used to identify the actions of potential violators of information security (IS) and cybersecurity (CS) of informatization objects (IO). This has become especially noticeable in the context of an increase in the number and quality of malicious actions aimed at destabilizing the functioning of computer and information systems. The analysis of mathematical methods for modern intrusion detection systems (IDS) in the information and communication networks of the IO has revealed several both their advantages and disadvantages. To date, existing IDS are not always ineffective against new types of intrusions, especially in situations that are characterized by poorly structured data on signs of attacks or vaguely defined criteria in the corresponding task of recognizing new threats. Therefore, the development of appropriate methods for identifying abnormal states for IDS by integrating intelligent decision support systems (DSS) into their composition to expand the functionality of the protection side, will allow these IDS to be more effective in identifying new types of cyber-attacks. Based on the existing apparent contradiction between an increase in the level of cybernetic threats to the security of the IO and an increase in the intensity of external malicious influences with a simultaneous increase in the requirements for CS, an important scientific and technical task is to further develop existing and develop new methods and models for intelligent DSS in conditions of poorly structured data on signs and identified anomalies in the IS. As shown by many theorists in the field of IS and CS studies, one of the most promising areas of abuse identification are methods adapted to the analysis of situations that are associated with the recognition of long-term cyber-attacks that are not accompanied by obvious signs. Such methods fully include methods based on Bayesian networks (BN) and Bayesian classifiers, which determines the relevance of the topic of our study.
Purpose	The aim of the project is to improve the quality of estimates of the probability of the implementation of threats of an IO attacker by developing an approach based on the use of Bayesian networks in complex formalized atypical situations of multi–stage targeted cyber attacks on the IO.
Objectives	To achieve this goal , the following interrelated tasks must be solved: 1) analyze existing intrusion detection systems and event collection and correlation systems (Security Information and Event Management, SIEM)

	2) to develop BN templates and new models for the DSS computing core during the prediction of threats and stages of intrusion into information and communication networks (ICS) of informatization objects; 3) supplement probabilistic models for detecting network intrusions based on the use of dynamic BN; 4) develop and test the DSS in data analysis tasks based on the use of BN.
Expected and achieved results	The BN templates developed within the framework of the project for the computing core of the DSS in the course of forecasting threats and stages of intrusion into the ICS OI will allow information security analysts to operate with a variety of random variables using the DSS and determine the probability of the implementation of threats or a specific stage of intrusion into the ICS OI under specified conditions. In comparison with similar works, our project will supplement probabilistic models for detecting network intrusions based on the use of dynamic base systems. In addition, the proposed approach makes it possible not only to take into account the main stages of intrusions, but also to make more informed decisions based on the use of both standard intrusion templates and newly synthesized templates. All templates and models make up the computational core of the decision support system during the intrusion detection process, which is.
Research team members with their identifiers (Scopus Author ID, Researcher ID, ORCID, if available) and links to relevant profiles	1. Ydyryshbayeva Moldir Bazarkhankyzy, The Hirsch Index is – 1, ORCID: https://orcid.org/0000-0002-5680-5444, Scopus Author ID: 57222863896 2. Akhmetov Bakhytzhan Srazhatdinovich, Doctor of Technical Sciences, Professor, The Hirsch Index is – 7, ResearcherID: ABI-3310-2020, ORCID: https://orcid.org/0000-0001-5622-2233, Scopus Author ID: 56829370400
List of publications with links to them	
Patents	-