2.1. 01-01-00108
2.2. Kotenko Igor Vitalevich
2.3. Mathematical models of information security assurance in computer networks based on multi-agent technologies and their experimental evaluation.
2.4. 2004
2.5. 1
2.6. The project is devoted to solution of a fundamental scientific problem of information assurance in computer networks that is founded on new approaches based on multi-agent technologies. The main results of the project are mathematical frameworks, architectures, operation models and methods, realization principles and software prototypes of components of the vulnerabilities analysis, intrusion detection and intrusion detection learning systems, as well as the results of exploratory computer simulation of their operation and the recommendations on elaboration of perspective computer network security systems. Within the project the following particular results are developed. The analysis and classification of external and internal computer attacks were fulfilled. The scenario-based specifications of a representative set of remote network attacks were developed. The models and techniques of recovery of the formal grammars specifying attack models were offered. A set of the formal models for imitation of the distributed attacks on computer networks (including models of attack generation by team of malefactors and models of an attacked computer network) was created. The architecture of the multi-agent security system was developed (The main attention was given to intrusion detection components). The models and methods of operation of particular components (agents) of the multi-agent security system were offered. The ontology of computer network security domain was developed. The model of distributed knowledge base of the security system was constructed (as a set of models of the security agents' distributed knowledge, believes and intentions). The model of the agents' interaction was developed. The formal model of the agents' communication language and appropriate protocols of their interaction were elaborated. The ontology for tasks of the computer network intrusion detection learning was developed. The distribution of learning tasks between typical learning agents was made and the architecture of the multi-agent intrusion detection learning system was developed. The mathematical methods for realization of typical learning agents' functions were chosen and developed. To check the main theoretical results the object-oriented projects and prototypes of the multi-agent systems of computer network attack simulation, intrusion detection and intrusion detection learning were developed. To evaluate the quality of the models

and methods developed, computer simulation of the prototypes operation was conducted.

2.7. Saint-Petersburg Institute for informatics and automation of RAS

Project Principal Investigator
Ph.D. Professor

I.V.Kotenko