

Предисловие

Данный тематический выпуск журнала посвящен рассмотрению некоторых проблем информационной безопасности в условиях современных вызовов и угроз, а также способов предупреждения и предотвращения информационно-технической и информационно-психологической агрессии. Ряд статей представляет оригинальные результаты в области защиты организационно-технических систем критически важной инфраструктуры с возможностями активного противодействия, включая защиту персонала от вредоносного информационно-психологического воздействия. Предлагаются новые подходы к обеспечению безопасности, основанные на моделировании сценариев поведения сторон в конфликте и синтезе интеллектуальных систем противоборства в киберпространстве. В их числе: упреждающее противоборство, маскирование и сетевая контрразведка, управление информационным контентом и семантический контроль целостности.

Рассмотрены технологии разработки автоматизированных систем в защищенном исполнении с учетом информационных рисков и развиваемые для усложненной модели нарушителя. Представлены оригинальные технологии обнаружения и предупреждения воздействий в сетях связи различных операторов с учетом возможных сценариев поведения нарушителя. Приведены механизмы выявления и пресечения массовых вредоносных воздействий на информационно-телекоммуникационные системы и способы адаптивного управления целевым активным сетевым оборудованием для нейтрализации массивированного возмущения и восстановления параметров штатного функционирования. Предлагается система непрерывного контроля целостности средств защиты информации и последующего восстановления эталонного состояния системы безопасности.

В выпуске представлены также оригинальные методы и технологии многоуровневой фильтрации потенциально вредоносного контента в мультимедийных потоках данных. Детализированы технологии защиты от скрытой передачи вредоносной видео- и аудиоинформации, призванных снижать риск возможного негативного влияния на индивидуальное и групповое психофизиологическое состояние персонала критической инфраструктуры. Обсуждается подход к созданию теории построения интеллектуальных киберсистем, способных порождать упреждающие стратегии поведения в

киберпространстве по аналогии с антиципирующим поведением биоорганизмов. Предлагаются решения по организации «доверительных сред» функционирования информационно-вычислительных комплексов, использующих потенциально опасные аппаратно-программные комплекты. В данном тематическом выпуске журнала представлены большей частью статьи сотрудников Военно-космической академии имени А.Ф. Можайского, являющейся в настоящее время системообразующим политехническим ВУЗом Министерства Обороны Российской Федерации в области военно-космической деятельности, инфотелекоммуникационных технологий, а также технологий сбора и обработки специальной информации.

Директор СПИИРАН,
член-корреспондент РАН
Р.М. ЮСУПОВ

Профессор кафедры систем
сбора и обработки информации
Военно-космическая академия
имени А.Ф. Можайского,
доктор технических наук, профессор
А.Г. ЛОМАКО

Preface

This topical issue of the journal is dedicated to some specific aspects of information security emerging under actual threats and challenges, as well as to approaches aimed at preventing and averting of information-technical and information-psychological aggression. Many presented articles deliver original solutions intended for the protection of organization-technical systems of critical infrastructure capable of active counteraction, including protection of the personnel against malicious information-psychological impacts. New approaches are proposed to the security assurance based on modeling the scenarios of the conflict parties' behavior and on the synthesis of intelligent counteraction systems in cyberspace. Namely: anticipatory counteraction, masking and network counterintelligence, information content management and integrity's semantic control.

The technologies for development of secure automated systems that account for the information risks and the sophisticated malefactor model are considered. Original technologies are presented that are meant for detecting and averting the effects in communication networks of different operators with regard to possible scenarios of malefactor's behavior. Mechanisms developed in order to detect and suppress mass malicious effects upon the information and telecommunication systems as well as methods for adaptive control of active target network equipment for neutralization of mass disturbance and recovery of regular functioning parameters are represented. The system of continuous monitoring of the information securities' integrity and subsequent recovering of the reference security state is proposed.

Also this issue presents the original methods and technologies of multilevel filtration of potentially malicious content in multimedia data streams. Technologies of protection against hidden malicious video and audio information transfer meant for decreasing risks of the possible negative influence on the individual and group psycho-physiological condition of the critical infrastructure personnel are given in detail. An approach to developing a theory of designing the intelligent cyber systems capable of generating the proactive behavioral strategies in cyberspace similar to the anticipatory behavior of biological organisms is discussed. Solutions that consider a construct of "confidence environment" for functioning of information and computing systems that use potentially dangerous firmware components are suggested. Most of the articles published in this topical issue of the journal were submitted by the scientists

of the Military Space Academy named after A.F. Mozhaysky that currently is a backbone higher education polytechnic institution at the Russian Federation Ministry of Defense in the area of military-space activities, information telecommunication technologies, as well as technologies of special information gathering and processing.

St. Petersburg Institute for Informatics and Automation of the
Russian Academy of Sciences (SPIIRAS)

Director

Corresponding Member of the Russian Academy of Sciences

Doctor of Technical Sciences, Professor

R.M. YUSUPOV

Military Space Academy named after A. F. Mozhaysky

Department of the Systems for

Data Collection and Processing

Professor

Doctor of Technical Sciences, Professor

A.G. LOMAKO