

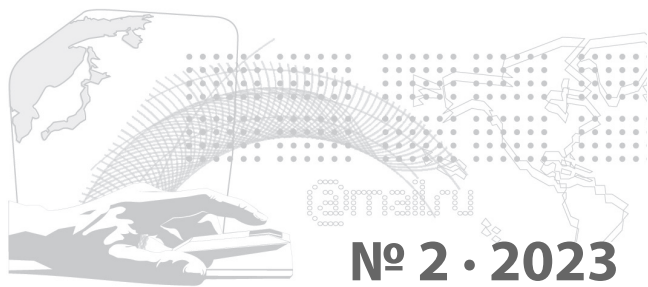
ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КОМПЬЮТЕРНЫЕ СИСТЕМЫ

№ 2 • 2023

РАЗДЕЛЫ ВЫПУСКА:

Методы и средства обеспечения информационной безопасности	9
Безопасность программного обеспечения	37
Безопасность распределенных систем и телекоммуникаций	61
Практические аспекты криптографии	82
Безопасность критических информационных инфраструктур	92
Безопасность киберфизических систем	107
Моделирование технологических систем, алгоритмизация задач и объектов управления	183
Системы машинного обучения и управления базами знаний	191



№ 2 • 2023

Журнал является органом Совета
Регионального Северо-Западного
учебно-научного центра
информационной безопасности

Журнал включен в перечень изданий,
утвержденных ВАК, для публикации
основных результатов
диссертационных исследований

Целью Журнала является популяризация
результатов актуальных научных
исследований в сфере обеспечения
безопасности информационных
инфраструктур, исследования
автоматизированных систем управления
технологическими процессами
и производствами, а также оценки
качества и сопровождения программных
продуктов.

АДРЕС РЕДКОЛЛЕГИИ:

195251, Санкт-Петербург,
ул. Политехническая, 29.
ФГАОУ ВО «Санкт-Петербургский
политехнический университет
Петра Великого».

Тел. (812) 552-76-32

e-mail: kafedra@ibks.ftk.spbstu.ru
ojs@ic.spbstu.ru

<http://jisp.ru/kontakty>

Свидетельство о регистрации
№ 018607 от 17.03.99 г. выдано
Государственным комитетом Российской
Федерации по печати

С 1 января 2019 г. подписка
на журнал «Проблемы информационной
безопасности. Компьютерные системы»
осуществляется через объединенный
каталог «Пресса России»

<https://www.pressa-rf.ru>

Подписной индекс — Т18237

РЕДАКЦИОННЫЙ СОВЕТ:

ЗЕГЖДА Д. П. — главный редактор, чл.-кор. РАН, д-р техн. наук,
проф., директор Института кибербезопасности и защиты
информации СПбПУ

ЧЛЕНЫ РЕДАКЦИОННОГО СОВЕТА:

АБДЫКАППАР АШИМОВ, акад. Национальной академии наук РК,
д-р техн. наук, проф., Институт проблем информатики и управ-
ления Министерства образования и науки РК, Казахстан;

АТИЛЛА ЭЛЧИ, д-р наук, проф. кафедры «Электроэлектронная
инженерия», инженерный факультет, Аксарайский университет,
Турция;

БАРАНОВ А. П., д-р физ.-мат. наук, проф., зав. кафедрой комплексной
безопасности критически важных объектов РГУ нефти и газа
(НИУ) имени И. М. Губкина;

БУДЗКО В. И., д-р техн. наук, зам. директора Института проблем
информатики ФИЦ ИУ РАН, академик Академии криптографии
РФ;

ВЭЙ НИ, д-р наук, профессор Наньчанского университета, Китай;

ЖУКОВ И. Ю., д-р техн. наук, профессор кафедры стратегических
информационных исследований Института интеллектуаль-
ных кибернетических систем НИЯУ «МИФИ»

МАРКОВ А. С., д-р техн. наук, профессор кафедры «Информаци-
онная безопасность» МГТУ им. Н. Э. Баумана, член Экспертно-
го совета при Правительстве РФ;

МОДРИС ГРЕЙТАНС, д-р техн. наук, гл. ред. журн. «Автоматика
и вычислительная техника», директор по науке Института
электроники и компьютерных наук, Рига, Латвия;

КНЯЗЕВ А. В., д-р физ.-мат. наук, проф., генеральный директор
АО «Институт точной механики и вычислительной техники
им. С. А. Лебедева Российской академии наук»;

КОРНИЕНКО А. А., д-р техн. наук, проф., проф. кафедры «Информа-
тика и информационная безопасность» ПГУПС;

СИКАРЕВ И. А., д-р техн. наук, проф., ФГБОУ ВО «Российский госу-
дарственный гидрометеорологический университет»;

СОКОЛОВ И. А., д-р техн. наук, академик РАН, профессор, декан
факультета Вычислительной математики и кибернетики МГУ
им. М. В. Ломоносова;

ФРАНК ЛЕПРЕВО, д-р, проф., вице-президент по международным
связям Университета Люксембурга;

МАЛЮК А. А., канд. техн. наук, проф. кафедры № 41 «Кибербез-
опасность» НИЯУ «МИФИ»;

ОСТАПЕНКО А. Г., д-р техн. наук, проф., зав. кафедрой «Системы
информационной безопасности» ВГТУ;

ВАСИЛЬ СГУРЕВ, акад. Болгарской академии наук, д-р техн. наук,
проф., Болгария;

ХАРИН Ю. С., академик НАН Беларуси, д-р физ.-мат. наук, проф., дирек-
тор НИИ прикладных проблем математики и информатики БГУ;

ЧАНДАН ТИЛАК БХУНИЙ, д-р наук, директор Национального тех-
нологического института, Министерство развития человеческих
ресурсов Правительства Индии, Аруначал-Прадеш, Индия;

ШЕРЕМЕТ И. А., д-р техн. наук, проф., академик РАН, заместитель
директора по науке РФФИ;

ШЕЛУПАНОВ А. А., д-р техн. наук, проф., президент ТУСУР;

ЮСУПОВ Р. М., чл.-кор. РАН, д-р техн. наук, проф., директор
СПИИРАН.

Выпускающий редактор **М. В. ДЕВЕЙКИС**

Ответственный секретарь **Н. Ю. ЛОВЧИНОВСКАЯ**



МитСОБИ

Конференция «**Методы и технические средства обеспечения безопасности информации**» (МитСОБИ) — это встреча профессионалов информационной безопасности, единственная и старейшая конференция, с 1991 года ежегодно проходящая в Санкт-Петербурге.

32-я научно-техническая конференция МитСОБИ имени Петра Дмитриевича Зегжды в 2023 году пройдет в Санкт-Петербурге с 26 по 29 июня.

МитСОБИ — это возможность узнать самые современные направления и поделиться опытом, это интересные доклады и горячие дискуссии, в которых молодые разработчики имеют возможность узнать мнение мэтров информационной безопасности, а руководители — выяснить, как на практике решать самые острые вопросы, оценить важность и действенность этих решений для обеспечения информационной безопасности как страны в целом, так и для каждого участника киберпространства. Особенность конференции — это диалог на пересечении теории и практики, науки и бизнеса.

Ежегодное количество участников — до 300 человек, среди которых руководство и специалисты органов государственной власти РФ, вузов, академических учреждений, разработчики и молодые ученые, представители научно-исследовательских организаций и коммерческих предприятий из различных регионов России.

Организаторы конференции



НеоБИТ



Комитет
по информатизации
и связи
Правительства
Санкт-Петербурга



Комитет
по науке и высшей
школе
Правительства
Санкт-Петербурга



СЗРО УМО
по ИБ
при СПбПУ

При участии

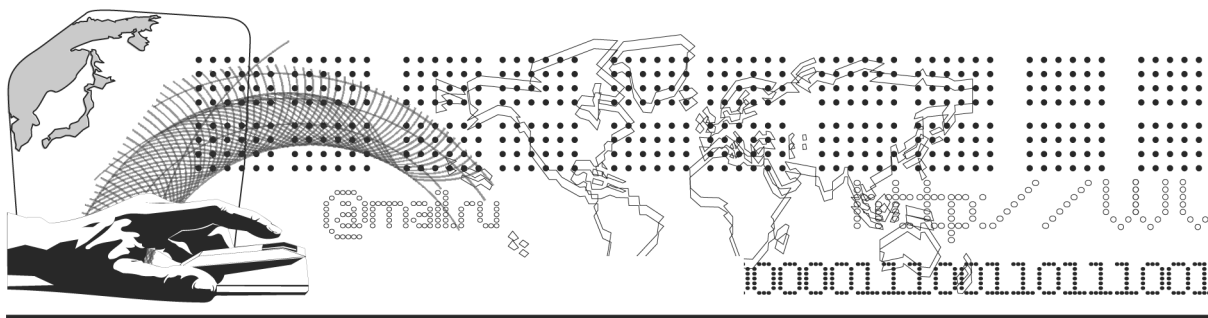
Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю, Управления специальной связи и информации ФСО России в СЗФО, Федеральной службы по финансовому мониторингу.

Подробная информация — на сайте конференции www.mitsobi.ru

8 (800) 222-28-06

+7 (812) 535-28-06

mitsobi@neobit.ru



СОДЕРЖАНИЕ

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- 9 *Шакурский М. В., Караулова О. А.*
ОЦЕНКА МАСКИРОВКИ СИГНАЛА ДВУХКОМПОНЕНТНОЙ
СТЕГАНОГРАФИЧЕСКОЙ СИСТЕМОЙ ПРИ ОКОННОЙ ОБРАБОТКЕ ИНФОРМАЦИИ
- 17 *Логинов З. Г., Соловей Р. С., Дахнович А. Д.*
ИСПОЛЬЗОВАНИЕ МЕТОДА ОБНАРУЖЕНИЯ КООРДИНАЦИИ БОТ-СЕТЕЙ
ДЛЯ ДЕТЕКТИРОВАНИЯ ИНФОРМАЦИОННЫХ КАМПАНИЙ В СОЦИАЛЬНЫХ СЕТЯХ
- 27 *Карпова И. Л., Курилов А. В., Супрун А. Ф., Иванова Л. А.*
УЧЁТ ВЛИЯНИЯ ЧЕЛОВЕЧЕСКОГО ФАКТОРА В МОДЕЛЯХ КИБЕРБЕЗОПАСНОСТИ

БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

- 37 *Югай П. Э., Жуковский Е. В., Семенов П. О.*
ОСОБЕННОСТИ ОБНАРУЖЕНИЯ ВРЕДНОСНЫХ УСТАНОВОЧНЫХ ФАЙЛОВ
С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМОВ МАШИНОГО ОБУЧЕНИЯ
- 47 *Грибков Н. А., Овасапян Т. Д., Москвин Д. А.*
АНАЛИЗ ВОССТАНОВЛЕННОГО ПРОГРАММНОГО КОДА
С ИСПОЛЬЗОВАНИЕМ АБСТРАКТНЫХ СИНТАКСИЧЕСКИХ ДЕРЕВЬЕВ

БЕЗОПАСНОСТЬ РАСПРЕДЕЛЕННЫХ СИСТЕМ И ТЕЛЕКОММУНИКАЦИЙ

- 61 *Коломойцев В. С.*
МЕТОДЫ КОНТРОЛЯ ИСПОЛНЕНИЯ СЦЕНАРИЯ БЕЗОПАСНОСТИ
В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ
- 73 *Орел Е. М., Москвин Д. А., Аношкин И. А.*
АНАЛИЗ УСТОЙЧИВОСТИ АРХИТЕКТУРЫ СИСТЕМ ОБМЕНА СООБЩЕНИЯМИ
С ДЕЦЕНТРАЛИЗОВАННОЙ УЗЛОВОЙ СТРУКТУРОЙ

ПРАКТИЧЕСКИЕ АСПЕКТЫ КРИПТОГРАФИИ

- 82 *Семьянов П. В., Грезина С. В.*
АНАЛИЗ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ КРИПТОКОШЕЛЬКА BITCOIN CORE

БЕЗОПАСНОСТЬ КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУР

- 92** *Васинев Д. А., Семенов А. К.*
**АНАЛИЗ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ И ПЕРСПЕКТИВНЫЕ ВАРИАНТЫ
ПРИМЕНЕНИЯ МЕЖСЕТЕВОГО ЭКРАНА НОВОГО ПОКОЛЕНИЯ
ДЛЯ ЗАЩИТЫ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ**

БЕЗОПАСНОСТЬ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

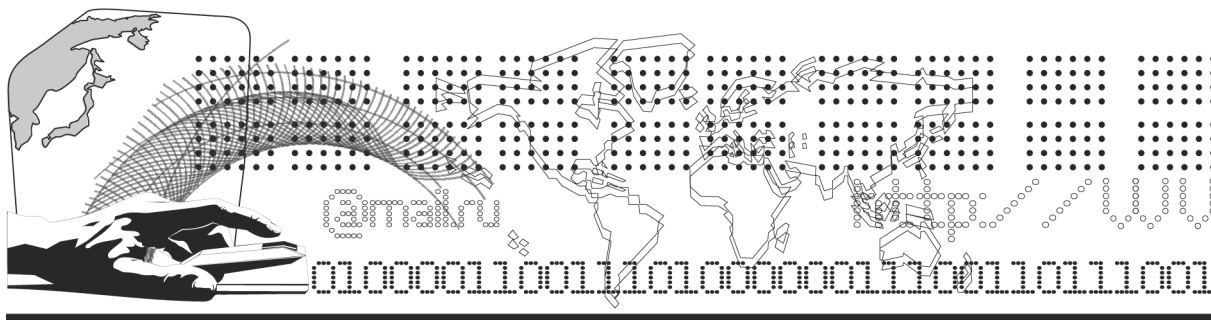
- 107** *Завадский Е. В., Калинин М. О.*
**ПОДДЕРЖАНИЕ КИБЕРУСТОЙЧИВОСТИ
НА БАЗЕ МЕТОДОВ АНАЛИЗА ГРАФОВ И ВИРТУАЛИЗАЦИИ ФУНКЦИОНАЛЬНОЙ СЕТИ**
- 123** *Богина В. М., Лаврова Д. С., Зегжда Д. П., Павленко Е. Ю.*
**ВЕРОЯТНОСТНЫЙ ПОДХОД К ОЦЕНКЕ КИБЕРУСТОЙЧИВОСТИ
МОБИЛЬНЫХ СЕТЕЙ НА ОСНОВЕ ИХ СВЯЗНОСТИ**
- 140** *Марков Г. А.*
**ПРИМЕНЕНИЕ МОДЕЛИ НЕОКОРТЕКСА ДЛЯ ВЫЯВЛЕНИЯ КОНТЕКСТУАЛЬНЫХ
АНОМАЛИЙ В СЕТЕВОМ ТРАФИКЕ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ**
- 150** *Зегжда Д. П., Зубков Е. А., Москвин Д. А.*
**ОЦЕНКА ЗАЩИЩЕННОСТИ КИБЕРФИЗИЧЕСКОЙ СИСТЕМЫ
НА ОСНОВЕ АНАЛИЗА СИГНАТУР ВРЕДОНОСНОГО ПО**
- 163** *Марков Г. А., Крундышев В. М., Калинин М. О., Зегжда Д. П., Бусыгин А. Г.*
**ОБНАРУЖЕНИЕ КОМПЬЮТЕРНЫХ АТАК В СЕТЯХ ПРОМЫШЛЕННОГО ИНТЕРНЕТА
ВЕЩЕЙ НА ОСНОВЕ ВЫЧИСЛИТЕЛЬНОЙ МОДЕЛИ ИЕРАРХИЧЕСКОЙ ВРЕМЕННОЙ ПАМЯТИ**
- 173** *Штыркина А. А.*
**МЕТОД РЕКОНФИГУРАЦИИ ТОПОЛОГИИ КИБЕРФИЗИЧЕСКОЙ СИСТЕМЫ
НА ОСНОВЕ ГРАФОВОЙ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ**

МОДЕЛИРОВАНИЕ ТЕХНОЛОГИЧЕСКИХ СИСТЕМ, АЛГОРИТМИЗАЦИЯ ЗАДАЧ И ОБЪЕКТОВ УПРАВЛЕНИЯ

- 183** *Сухов А. М.*
**ПОДХОДЫ К РЕШЕНИЮ ЗАДАЧИ СИНТЕЗА
ЭФФЕКТИВНОГО ПРОЦЕССА ФУНКЦИОНИРОВАНИЯ ВОЕННО-ТЕХНИЧЕСКИХ СИСТЕМ**

СИСТЕМЫ МАШИННОГО ОБУЧЕНИЯ И УПРАВЛЕНИЯ БАЗАМИ ЗНАНИЙ

- 191** *Миляков Д. Ф., Сикарев И. А., Травин С. В.*
**ИСКУССТВЕННЫЕ НЕЙРОННЫЕ СЕТИ В СИСТЕМЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
МОРЕПЛАВАНИЯ АВТОНОМНЫХ БЕЗЭКИПАЖНЫХ СУДОВ**
- 202** *Калинин М. О., Ткачева Е. И.*
**ДЕЦЕНТРАЛИЗОВАННЫЙ ПОДХОД К ОБНАРУЖЕНИЮ ВТОРЖЕНИЙ
В ДИНАМИЧЕСКИХ СЕТЯХ ИНТЕРНЕТА ВЕЩЕЙ НА БАЗЕ МНОГОАГЕНТНОГО ОБУЧЕНИЯ
С ПОДКРЕПЛЕНИЕМ И МЕЖАГЕНТНЫМ ВЗАИМОДЕЙСТВИЕМ**



CONTENTS

INFORMATION SECURITY APPLICATION

- 9 *Shakurskiy M. V., Karaulova O. A.*
**EVALUATION OF SIGNAL MASKING
BY A TWO-COMPONENT STEGANOGRAPHIC SYSTEM
IN WINDOWED INFORMATION PROCESSING**
- 17 *Loginov Z. G., Solovey R. S., Dakhnovich A. D.*
**USING BOTNET COORDINATION DETECTION
TO DETECT SOCIAL INFORMATION CAMPAIGNS**
- 27 *Karpova I. L., Kurilov A. V., Suprun A. F., Ivanova L. A.*
**ACCOUNTING FOR THE IMPACT
OF THE HUMAN FACTOR IN CYBER SECURITY MODELS**

SOFTWARE SECURITY

- 37 *Yugay P. E., Zhukovsky E. V., Semenov P. O.*
**ASPECTS OF DETECTING MALICIOUS INSTALLATION FILES
USING MACHINE LEARNING ALGORITHMS**
- 47 *Gribkov N. A., Ovasapyan T. D., Moskvina D. A.*
**ANALYSIS OF DECOMPILED PROGRAM CODE
USING ABSTRACT SYNTAX TREES**

NETWORK AND TELECOMMUNICATION SECURITY

- 61 *Kolomoitcev V. S.*
**METHODS OF MONITORING THE EXECUTION
OF THE SECURITY PATTERN IN INFOCOMMUNICATION SYSTEMS**
- 73 *Orel M. E., Moskvina D. A., Anoshkin I. A.*
**DECENTRALIZED MESSAGING SYSTEMS
ARCHITECTURE STABILITY ANALYSIS**

APPLIED CRYPTOGRAPHY

- 82 *Semyanov P. V., Grezina S. V.*
BITCOIN CORE CRYPTOCURRENCY WALLET CRYPTOGRAPHIC SECURITY ANALYSIS

CRITICAL INFORMATION INFRASTRUCTURE SECURITY

- 92** *Vasinev D. A., Semenov A. K.*
**ANALYSIS OF FUNCTIONALITY AND FUTURE OPTIONS FOR THE APPLICATION
OF A NEW GENERATION FIREWALL TO PROTECT CRITICAL INFORMATION
INFRASTRUCTURE FACILITIES**

CYBER-PHYSIC SYSTEMS SECURITY

- 107** *Zavatskii E. V., Kalinin M. O.*
**CYBER RESILIENCY SUPPORT BASED ON METHODS
OF GRAPH ANALYSIS AND FUNCTIONAL NETWORK VIRTUALIZATION**
- 123** *Bogina V. M., Lavrova D. S., Zegzhda D. P., Pavlenko E. Yu.*
**A PROBABILISTIC APPROACH TO ASSESSING THE CYBER RESILIENCE
OF MOBILE NETWORKS BASED ON THEIR CONNECTIVITY**
- 140** *Markov G. A.*
**APPLICATION OF THE NEOCORTEX MODEL TO DETECT CONTEXTUAL ANOMALIES
IN NETWORK TRAFFIC OF THE INDUSTRIAL INTERNET OF THINGS**
- 150** *Zegzhda D. P., Zubkov E. A., Moskvina D. A.*
**CYBERSECURITY ASSESSMENT OF CYBER-PHYSICAL SYSTEM
BASED ON ANALYSIS OF MALWARE SIGNATURES**
- 163** *Markov G. A., Krundyshev V. M., Kalinin M. O., Zegzhda D. P., Busygin A. V.*
**DETECTION OF COMPUTER ATTACKS IN NETWORKS OF INDUSTRIAL INTERNET
OF THINGS BASED ON THE COMPUTING MODEL OF HIERARCHICAL TEMPORARY MEMORY**
- 173** *Shtyrkina A. A.*
**METHOD OF CYBERPHYSICAL SYSTEM TOPOLOGY RECONFIGURATION
BASED ON GRAPH ARTIFICIAL NEURAL NETWORK**

TECHNOLOGICAL SYSTEMS, ALGORITHMIZATION OF TASKS AND CONTROL OBJECTS MODELING

- 183** *Sukhov A. M.*
**APPROACHES TO SOLVING THE PROBLEM OF SYNTHESIS
OF AN EFFECTIVE PROCESS OF FUNCTIONING OF MILITARY-TECHNICAL SYSTEMS**

MACHINE LEARNING AND KNOWLEDGE CONTROL SYSTEMS

- 191** *Milyakov D. F., Sikarev I. A., Travin S. V.*
**ARTIFICIAL NEURAL NETWORKS IN THE NAVIGATION
SAFETY SYSTEM OF AUTONOMOUS UNMANNED VESSELS**
- 202** *Kalinin M. O., Tkacheva E. I.*
**DECENTRALIZED APPROACH TO INTRUSION DETECTION IN DYNAMIC NETWORKS
OF THE INTERNET OF THINGS BASING ON MULTI-AGENT
REINFORCEMENT LEARNING AND INTER-AGENT COMMUNICATION**