

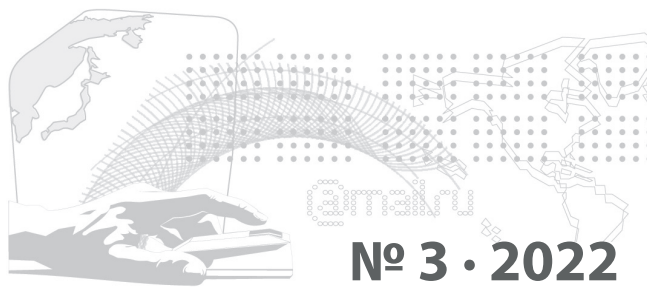
ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КОМПЬЮТЕРНЫЕ СИСТЕМЫ

№ 3 • 2022

РАЗДЕЛЫ ВЫПУСКА:

Методы и средства обеспечения информационной безопасности	9
Практические аспекты криптографии	45
Безопасность критических информационных инфраструктур	55
Безопасность киберфизических систем	80
Исследование, контроль и оптимизация автоматизированных систем управления	90
Системы машинного обучения и управления базами знаний	143



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

<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, д-р техн. наук, проф. 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 НЕ, д-р наук, Шеньчженьский университет, 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., зав. кафедрой «Информа-
тика и информационная безопасность» ПГУПС;

СИКАРЕВ И. А., д-р техн. наук, проф., зав. кафедрой Морских ин-
формационных систем ФГБОУ ВО «Российский государственный
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., чл.-кор. РАН, заместитель
директора по науке РФФИ;

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

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

Выпускающий редактор **Д. А. КЛУБНИЧКИНА**

Ответственный секретарь **Н. Ю. ЛОВЧИНОВСКАЯ**



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.

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.

Организатор конференции



Соучредители



Комитет
по информатизации
и связи
Правительства
Санкт-Петербурга



Комитет
по науке и высшей
школе
Правительства
Санкт-Петербурга



Санкт-Петербургский
политехнический
университет
Петра Великого

При участии

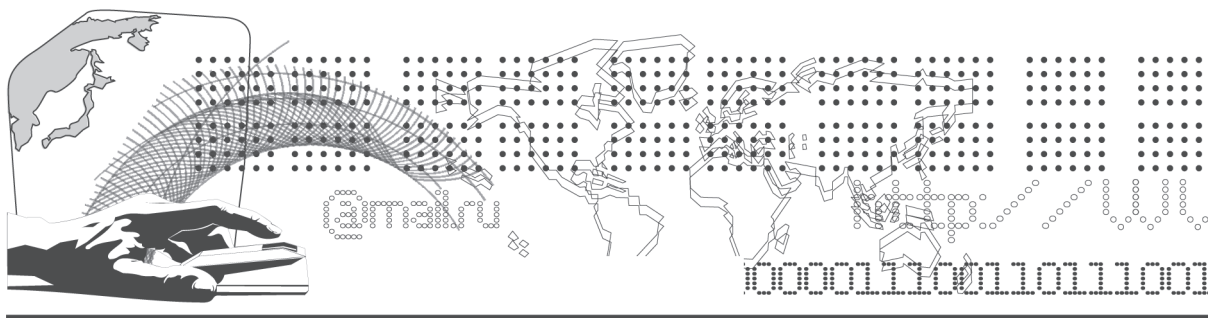
Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю, Управления специальной связи и информации ФСО России в СЗФО, Федеральной службы по финансовому мониторингу.

Подробная информация — на сайте конференции www.mitsobi.ru.

Контактные лица:

**Селиванова Анна Юрьевна — 8 (800) 222-28-06 (звонок бесплатный);
+7 (812) 535-28-06.**

E-mail: mitsobi@neobit.ru.



СОДЕРЖАНИЕ

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- 9** Ручкин В. Н., Костров Б. В., Фулин В. А.
**ИНТЕЛЛЕКТУАЛЬНАЯ СТРАТЕГИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
ПОСРЕДСТВОМ ВЫБОРА АРХИТЕКТУРЫ ВЫЧИСЛИТЕЛЬНЫХ И НЕЙРОННЫХ СЕТЕЙ**
- 24** Соколов М. В., Чечин И. В., Новиков П. А., Самойленко Д. В.
**МАТЕМАТИЧЕСКАЯ МОДЕЛЬ И АЛГОРИТМ КОНТРОЛЯ ЦЕЛОСТНОСТИ ДАННЫХ
НА ОСНОВЕ ПРАВИЛ ПОСТРОЕНИЯ КОДА С НЕРАВНОЙ ЗАЩИТОЙ СИМВОЛОВ**
- 36** Павленко Е. Ю., Еременко И. С., Фатин А. Д.
**МЕТОДЫ КЛАСТЕРИЗАЦИИ КОМПЬЮТЕРНЫХ СЕТЕЙ
В ЗАДАЧАХ КИБЕРБЕЗОПАСНОСТИ**

ПРАКТИЧЕСКИЕ АСПЕКТЫ КРИПТОГРАФИИ

- 45** Ниткин И. С., Таранов С. В.
**ОЦЕНКА КРИПТОГРАФИЧЕСКОЙ СТОЙКОСТИ ШИФРА КУЗНЕЧИК
ПРИ АТАКАХ МЕТОДОМ НЕВОЗМОЖНЫХ ДИФФЕРЕНЦИАЛОВ**

БЕЗОПАСНОСТЬ КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУР

- 55** Павленко Е. Ю.
**СИСТЕМАТИЗАЦИЯ КИБЕРУГРОЗ КРУПНОМАСШТАБНЫМ СИСТЕМАМ
С АДАПТИВНОЙ СЕТЕВОЙ ТОПОЛОГИЕЙ**
- 68** Павленко Е. Ю.
**МОДЕЛЬ ФУНКЦИОНИРОВАНИЯ АДАПТИВНОЙ СЕТЕВОЙ ТОПОЛОГИИ
КРУПНОМАСШТАБНЫХ СИСТЕМ НА ОСНОВЕ ДИНАМИЧЕСКОЙ ТЕОРИИ ГРАФОВ**

БЕЗОПАСНОСТЬ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

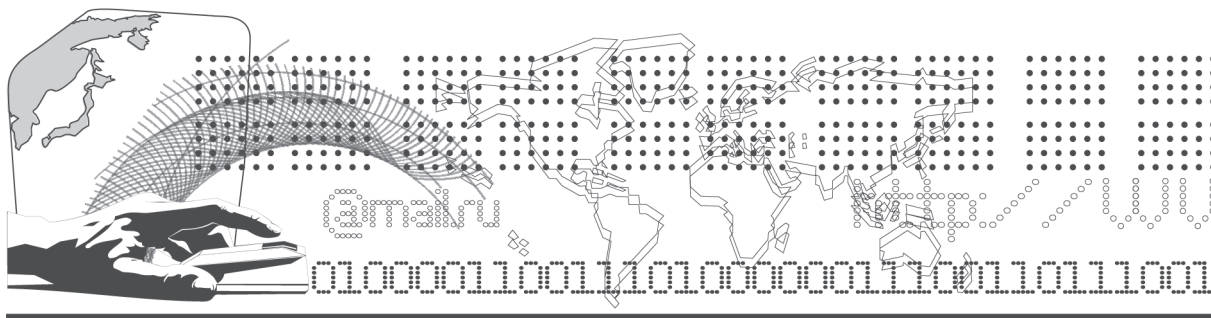
- 80** Александрова Е. Б., Штыркина А. А.
**ОЦЕНКА БЕЗОПАСНОСТИ УМНЫХ СИСТЕМ ЭНЕРГОСНАБЖЕНИЯ
НА ОСНОВЕ АНАЛИЗА СТРУКТУРНЫХ СВОЙСТВ МОДЕЛИРУЮЩИХ ГРАФОВ**

ИССЛЕДОВАНИЕ, КОНТРОЛЬ И ОПТИМИЗАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

- 90** Журавлев Д. А., Грибунин В. Г., Неустроев А. В., Полешенков Д. Д.
**МИКРОАРХИТЕКТУРНЫЕ УЯЗВИМОСТИ ПРОЦЕССОРА
В КОНТЕКСТЕ СОВМЕСТНОГО ПРИМЕНЕНИЯ АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ
ИНФОРМАЦИИ И ТЕХНОЛОГИЙ ВИРТУАЛИЗАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ**
- 96** Беззатеев С. В., Федоров И. Р., Федосенко М. Ю.
**ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ ТЕХНОЛОГИИ БЛОКЧЕЙН
В ПРОИЗВОДСТВЕННЫЕ ПРОЦЕССЫ ОТЕЧЕСТВЕННЫХ КОМПАНИЙ**
- 121** Куракин А. С.
**МОДЕЛЬ РАЗГРАНИЧЕНИЯ ПРАВ ДОСТУПА ВИРТУАЛЬНОГО ОТРЯДА
БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ**
- 130** Барышников С. О., Сахаров В. В., Сикарев И. А.
СИНТЕЗ НАБЛЮДАТЕЛЯ ДЛЯ СИСТЕМЫ УПРАВЛЕНИЯ КУРСОМ СУДНА

СИСТЕМЫ МАШИННОГО ОБУЧЕНИЯ И УПРАВЛЕНИЯ БАЗАМИ ЗНАНИЙ

- 143** Шниперов А. Н., Потылицина Ю. В.
**МЕТОД ИДЕНТИФИКАЦИИ ЧЕЛОВЕКА ПО ГОЛОСУ
С ИСПОЛЬЗОВАНИЕМ МАШИННОГО ОБУЧЕНИЯ**
- 155** Беззатеев С. В., Елина Т. Н., Красников Н. С.
**ИССЛЕДОВАНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ
ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
В РОЗНИЧНЫХ ТОРГОВЫХ ОПЕРАЦИЯХ**



CONTENTS

INFORMATION SECURITY APPLICATION

- 9** *Ruchkin V. N., Kostrov B. V., Fulin V. A.*
**INTELLECTUAL STRETEGY OF SECURITY ON BASE CHOSING
OF ARCHITECTURE COMPUTING AND NEUROPROCESSING NETS**
- 24** *Sokolov M. V., Chechin I. V., Novikov P. A., Samoylenko D. V.*
**MATHEMATICAL MODEL AND ALGORITHM FOR DATA INTEGRITY CONTROL
BASED ON THE RULES OF CODE CONSTRUCTION
WITH UNEQUAL CHARACTER PROTECTION**
- 36** *Pavlenko E. Yu., Eremenko I. S., Fatin A. D.*
**METHODS OF COMPUTER NETWORK CLUSTERING
IN CYBERSECURITY TASKS**

APPLIED CRYPTOGRAPHY

- 45** *Nitkin I. S., Taranov S. V.*
**AN ASSESSMENT OF CIPHER KUZNYECHIK CRYPTOGRAPHIC STABILITY
IN CASE OF IMPOSSIBLE DIFFERENTIALS METHOD ATTACKS**

CRITICAL INFORMATION INFRASTRUCTURE SECURITY

- 55** *Pavlenko E. Yu.*
**SYSTEMATIZATION OF CYBER THREATS TO LARGE-SCALE SYSTEMS
WITH ADAPTIVE NETWORK TOPOLOGY**
- 68** *Pavlenko E. Yu.*
**A FUNCTIONING MODEL OF ADAPTIVE NETWORK TOPOLOGY
OF LARGE-SCALE SYSTEMS BASED ON DYNAMIC GRAPH THEORY**

CYBER PHYSICAL SYSTEMS SECURITY

- 80** *Aleksandrova E. B., Shtyrkina A. A.*
**THE SECURITY OF SMART GRID SYSTEMS
BASED ON THE GRAPH STRUCTURAL PROPERTIES**

RESEARCH, MONITORING AND OPTIMIZATION OF AUTOMATED PROCESS CONTROL SYSTEMS

- 90** *Zhuravlev D. A., Gribunin V. G., Neustroev A. V., Poleshenkov D. D.*
**CPU MICROARCHITECTURAL VULNERABILITIES IN THE CONTEXT OF JOINT APPLICATION
OF HARDWARE FOR INFORMATION PROTECTION AND VIRTUALIZATION TECHNOLOGIES
IN AUTOMATED SYSTEMS**
- 96** *Bezzateev S. V., Fedorov I. R., Fedosenko M. Y.*
**THE PERSPECTIVE FOR INTRODUCTION OF BLOCKCHAIN TECHNOLOGY
INTO THE PRODUCTION PROCESSES OF RUSSIAN COMPANIES**
- 121** *Kurakin A. S.*
**A MODEL OF DIFFERENTIATION OF ACCESS RIGHTS
FOR A VIRTUAL SQUAD OF UNMANNED AERIAL VEHICLES**
- 130** *Baryshnikov S. O., Sakharov V. V., Sikarev I. A.*
SYNTHESIS OF AN OBSERVER FOR THE SHIP'S COURSE CONTROL SYSTEM

MACHINE LEARNING AND KNOWLEDGE CONTROL SYSTEMS

- 143** *Shniperov A. N., Potylitsina Y. V.*
VOICE IDENTIFICATION METHOD BASED ON MACHINE LEARNING
- 155** *Bezzateev S. V., Yelina T. N., Krasnikov N. S.*
**STUDY OF MACHINE LEARNING METHODS TO ENSURE INFORMATION SECURITY
IN RETAIL TRADING OPERATIONS**