

№ 1 • 2025

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

Цель журнала – 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

УЧРЕДИТЕЛЬ И ИЗДАТЕЛЬ

Санкт-Петербургский политехнический
университет Петра Великого

КОНТАКТЫ:

195251, Санкт-Петербург,
ул. Политехническая, 29
Тел. +7 (812) 552-76-32
E-mail: ojs@ibks.spbstu.ru
Сайт журнала: <http://jisp.ru/>

Свидетельство о регистрации
№ 018607 от 17.03.99

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. – д-р техн. наук, проф., чл.-кор. РАН, чл.-кор.
Академии криптографии РФ, главный редактор, директор
Института компьютерных наук и кибербезопасности
СПбПУ

ЧЛЕНЫ РЕДАКЦИОННОГО СОВЕТА

АШИМОВ АБДЫКАППАР, д-р техн. наук, проф., акад. НАН РК, Инсти-
тут информационных и вычислительных технологий Комитета
науки Министерства образования и науки РК, Казахстан

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, акад. Академии криптографии РФ,
Национальный исследовательский ядерный университет
«МИФИ»

ВЭЙ НЕ, д-р наук, Шеньчженьский университет, Китай

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

ГРИБОВА В. В., д-р техн. наук, проф., чл.-кор. РАН, Институт
автоматики и процессов управления Дальневосточного
отделения РАН

ГРУШО А. А., д-р физ.-мат. наук, проф., Московский государствен-
ный университет имени М. В. Ломоносова

ЖУКОВ И. Ю., д-р техн. наук, проф., Национальный исследова-
тельский ядерный университет «МИФИ»

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., Петербургский государ-
ственный университет путей сообщения Императора Алек-
сандра I

ЛЕПРЕВО ФРАНК, д-р наук, проф., вице-президент по междуна-
родным связям Университета Люксембурга

МАЛЮК А. А., канд. техн. наук, проф., Национальный исследова-
тельский ядерный университет «МИФИ»

МАРКОВ А. С., д-р техн. наук, проф., член Экспертного совета при
Правительстве РФ, Национальный исследовательский ядер-
ный университет «МИФИ»

ОСТАПЕНКО А. Г., д-р техн. наук, проф., Воронежский государ-
ственный технический университет

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

СИКАРЕВ И. А., д-р техн. наук, проф., Российский государствен-
ный гидрометеорологический университет

СОКОЛОВ И. А., д-р техн. наук, проф., акад. РАН, Московский
государственный университет имени М. В. Ломоносова

ХАРИН Ю. С., д-р физ.-мат. наук, проф., акад. НАН Беларуси,
Белорусский государственный университет, Беларусь

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

ШЕЛУПАНОВА А., д-р техн. наук, проф., Томский государственный
университет систем управления и радиоэлектроники

ШЕРЕМЕТ И. А., д-р техн. наук, проф., акад. РАН, Российский фонд
фундаментальных исследований

ЭЛЧИ АТИЛЛА, д-р наук, проф. кафедры электроэлектронной
инженерии, инженерный факультет, Аксарайский университет,
Турция

Выпускающий редактор **В. Е. ФИЛИППОВА**

Ответственный секретарь **Н. Ю. ЛОВЧИНОВСКАЯ**

© Санкт-Петербургский политехнический
университет Петра Великого, 2025

No. 1 • 2025

The journal is a body of the Council of the Regional North-West Educational and Scientific Center for Information Security

The journal is included in the list of editions approved by the Higher Attestation Commission for the publication of the main results of dissertation research

The purpose of the journal is to popularize the results of current scientific research in the field of information infrastructure security, research of automated process and production control systems, as well as quality assessment and maintenance of software products

FOUNDER AND PUBLISHER

Peter the Great
St. Petersburg Polytechnic University

CONTACTS:

29, Polytechnicheskaya str.,
St. Petersburg, 195251
Tel. +7 (812) 552-76-32
E-mail: ojs@ibks.spbstu.ru
Journal website: <http://jisp.ru/>

Registration Certificate
No. 018607 dated 17.03.99

From January 1, 2019 subscription to the journal "Problems of Information Security. Computer Systems" is available through the united catalog "Press of Russia"
<https://www.pressa-rf.ru>
Subscription index – T18237

EDITORIAL COUNCIL

ZEGZHDA D. P. – Doctor of Engineering Sciences, Professor, Corresponding Member RAS, Corresponding Member Academy of Cryptography of the Russian Federation, Chief Editor, Director of the Institute of Computer Science and Cybersecurity SPbPU

EDITORIAL COUNCIL MEMBERS

ASHIMOV ABDYKAPPAR, Doctor of Engineering Sciences, Professor, Academician of the National Academy of Sciences of the Republic of Kazakhstan, Institute of Information and Computational Technologies CS MSHE RK, Kazakhstan

BARANOV A. P., Doctor of Physics and Mathematics, Professor, Head of Department of Integrated Security of Critical Facilities, Gubkin Russian State University of Oil and Gas

BUDZKO V. I., Doctor of Engineering Sciences, Academician of the Russian Academy of Cryptography, National Research Nuclear University MEPhI (Moscow Engineering Physics Institute)

WEI NE, PhD, Shenzhen University, China

GREITANS MODRIS, Doctor of Engineering Sciences, Chief Editor journal "Automatic Control and Computer Sciences", Director of Science at the Institute of Electronics and Computer Science, Riga, Latvia

GRIBOVA V. V., Doctor of Engineering Sciences, Professor, Corresponding Member of the RAS, Institute of Automation and Control Processes Far Eastern Branch of the RAS

GRUSHO A. A., Doctor of Physics and Mathematics, Professor, Lomonosov Moscow State University

ZHUKOV I. YU., Doctor of Engineering Sciences, Professor, National Research Nuclear University MEPhI (Moscow Engineering Physics Institute)

KNYAZEV A. V., Doctor of Physics and Mathematics, Professor, General Manager of the Lebedev Institute of Precise Mechanics and Computer Engineering

KORNIENKO A. A., Doctor of Engineering Sciences, Professor, Emperor Alexander I St. Petersburg State Transport University

LEPREVOST FRANC, PhD, Professor, Vice President for International Relations at the University of Luxembourg

MALYUK A. A., Candidate of Engineering Sciences, Professor, National Research Nuclear University MEPhI (Moscow Engineering Physics Institute)

MARKOV A. S., Doctor of Engineering Sciences, Professor, Member of the Expert Council under the Government of the Russian Federation, National Research Nuclear University MEPhI (Moscow Engineering Physics Institute)

OSTAPENKO A. G., Doctor of Engineering Sciences, Professor, Voronezh State Technical University

SGUREV VASIL, Doctor of Engineering Sciences, Professor, Academician of the Bulgarian Academy of Science, Bulgaria

SIKAREV I. A., Doctor of Engineering Sciences, Professor, Russian State Hydrometeorological University

SOKOLOV I. A., Doctor of Engineering Sciences, Professor, Academician of the RAS, Lomonosov Moscow State University

KHARIN YU. S., Doctor of Physics and Mathematics, Professor, Academician of the National Academy of Sciences of Belarus, Belarusian State University, Belarus

CHANDAN TILAK BHUNIA, PhD, Director of the National Institute of Technology (University), Arunachal Pradesh, India

SHELUPANOV A. A., Doctor of Engineering Sciences, Professor, Tomsk State University of Control Systems and Radioelectronics

SHEREMET I. A., Doctor of Engineering Sciences, Professor, Academician of the RAS, Russian Foundation for Basic Research

ELCI ATILLA, Professor of the Department of Electronic Engineering, Faculty of Engineering, Aksaray University, Turkey

Executive editor **V. E. FILIPPOVA**

Executive secretary **N. YU. LOVCHINOVSKAYA**

© Peter the Great
St. Petersburg Polytechnic University, 2025



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.

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

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- 9 Чижевский М. А., Серпенинов О. В., Лапсарь А. П.
**ОПТИМИЗАЦИЯ ИСПОЛЬЗОВАНИЯ ИНДИКАТОРОВ КОМПРОМЕТАЦИИ
В ЗАДАЧАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

СИСТЕМЫ МАШИННОГО ОБУЧЕНИЯ И УПРАВЛЕНИЯ БАЗАМИ ЗНАНИЙ

- 21 Безбородов П. Д., Лаврова Д. С.
**ЗАЩИТА НЕЙРОСЕТЕВЫХ МОДЕЛЕЙ ОТ УГРОЗ НАРУШЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ
В ФЕДЕРАТИВНОМ ОБУЧЕНИИ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ ОПТИМИЗАЦИИ**
- 30 Бирюков Д. Н., Супрун А. Ф.
**ОТ «ЧЕРНОГО ЯЩИКА» К ПРОЗРАЧНОСТИ:
ФИЛОСОФСКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ОБЪЯСНИМОСТИ
И ИНТЕРПРЕТИРУЕМОСТИ В ИСКУССТВЕННОМ ИНТЕЛЛЕКТЕ**
- 43 Величко И. С., Беззатеев С. В.
ОТ ЭКСПЛУАТАЦИИ К ЗАЩИТЕ: АНАЛИЗ АТАК НА БОЛЬШИЕ ЯЗЫКОВЫЕ МОДЕЛИ
- 59 Кириллов Р. Б., Калинин М. О.
**ВЫЯВЛЕНИЕ ИСКАЖАЮЩИХ ДАННЫХ В СИСТЕМАХ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ,
ИСПОЛЬЗУЮЩИХ ВЫЧИСЛИТЕЛЬНЫЕ МОДЕЛИ МАШИННОГО ОБУЧЕНИЯ**

БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

- 69 Бугаев В. А., Жуковский Е. В., Лырчиков А. А.
**ОБНАРУЖЕНИЕ ПОТЕНЦИАЛЬНО ВРЕДОНОСНОЙ АКТИВНОСТИ
В КОНВЕЙЕРАХ CI/CD НА ОСНОВЕ АНАЛИЗА ПОВЕДЕНИЯ СБОРЩИКА**
- 83 Ломако А. Г., Исаев Н. Э., Менисов А. Б., Сабиров Т. Р.
**ПОДХОД К ВЫЯВЛЕНИЮ УЯЗВИМОСТЕЙ ПРОГРАММНОГО КОДА
НА ОСНОВЕ АДАПТАЦИИ С ПОДКРЕПЛЕНИЕМ
ПРЕДОБУЧЕННЫХ МОДЕЛЕЙ МАШИННОГО ОБУЧЕНИЯ**

ПРАКТИЧЕСКИЕ АСПЕКТЫ КРИПТОГРАФИИ

- 97 Костин С. О., Александрова Е. Б.
**МНОЖЕСТВЕННАЯ ПОДПИСЬ НА ИЗОГЕНИЯХ ЭЛЛИПТИЧЕСКИХ КРИВЫХ
С МАСКИРОВАНИЕМ И АУТЕНТИФИКАЦИЕЙ УЧАСТНИКОВ**

- 106** Шенец Н. Н., Александрова Е. Б., Коноплев А. С., Гололобов Н. В.
**ОБЩЕЕ РЕШЕНИЕ ЗАДАЧИ СПЕЦИАЛЬНОГО РАСПРЕДЕЛЕНИЯ
ЧАСТИЧНЫХ СЕКРЕТОВ С ИСПОЛЬЗОВАНИЕМ
СХЕМЫ РАЗДЕЛЕНИЯ СЕКРЕТА ШАМИРА**

БЕЗОПАСНОСТЬ РАСПРЕДЕЛЕННЫХ СИСТЕМ И ТЕЛЕКОММУНИКАЦИЙ

- 121** Новиков П. А., Диченко С. А., Лукьянов Р. В., Поликаренков С. В., Мартынов М. Л.
**МАТЕМАТИЧЕСКАЯ МОДЕЛЬ И МЕТОДИКА ОЦЕНИВАНИЯ ЭФФЕКТИВНОСТИ
СЕТЕВОГО МОНИТОРИНГА БЕЗОПАСНОСТИ СЕТИ ПЕРЕДАЧИ ДАННЫХ**
- 132** Пахомов М. А.
**МОДЕЛЬ ВЗАИМОДЕЙСТВИЯ УЗЛОВ МОБИЛЬНОЙ САМООРГАНИЗУЮЩЕЙСЯ СЕТИ
С УЧЕТОМ ЗАЩИТЫ ОТ АКТИВНЫХ СЕТЕВЫХ АТАК**
- 145** Скрыпников А. К., Крундышев В. М., Калинин М. О.
**АНОНИМИЗАЦИЯ СЕТЕВОГО ТРАФИКА В БЛОКЧЕЙН-СИСТЕМАХ
НА ОСНОВЕ ЧЕСНОЧНОЙ МАРШРУТИЗАЦИИ**

МОДЕЛИРОВАНИЕ ТЕХНОЛОГИЧЕСКИХ СИСТЕМ, АЛГОРИТМИЗАЦИЯ ЗАДАЧ И ОБЪЕКТОВ УПРАВЛЕНИЯ

- 155** Сикарев И. А., Абрамов В. М., Простакевич К. С., Абрамова А. Л., Честнов А. И.
**АВТОМАТИЗАЦИЯ АРХИВИРОВАНИЯ ИЗМЕРИТЕЛЬНОЙ ИНФОРМАЦИИ
ОБ АТМОСФЕРНЫХ ОСАДКАХ**

Contents

INFORMATION SECURITY ASPECTS

- 9 Chizhevsky M. A., Serpeninov O. V., Lapsar A. P.
**OPTIMIZATION OF INDICATOR OF COMPROMISE UTILIZATION
IN INFORMATION SECURITY TASKS**

MACHINE LEARNING AND KNOWLEDGE CONTROL SYSTEMS

- 21 Bezborodov P. D., Lavrova D. S.
**PROTECTING NEURAL NETWORK MODELS FROM PRIVACY VIOLATION THREATS
IN FEDERATED LEARNING USING OPTIMIZATION METHODS**
- 30 Biryukov D. N., Suprun A. F.
**FROM “BLACK BOX” TO TRANSPARENCY:
PHILOSOPHICAL AND METHODOLOGICAL FOUNDATIONS OF EXPLAINABILITY
AND INTERPRETABILITY IN ARTIFICIAL INTELLIGENCE**
- 43 Velichko I. S., Bezzateev S. V.
FROM EXPLOITATION TO PROTECTION: A DEEP DIVE INTO ADVERSARIAL ATTACKS ON LLMS
- 59 Kirillov R. B., Kalinin M. O.
**DETECTING ADVERSARIAL SAMPLES IN INTRUSION DETECTION SYSTEMS
USING MACHINE LEARNING MODELS**

SOFTWARE SECURITY

- 69 Bugaev V. A., Zhukovskii E. V., Lyrchikov A. A.
**DETECTION OF POTENTIALLY MALICIOUS ACTIVITY IN CI/CD PIPELINES
BASED ON ANALYSIS OF RUNNER BEHAVIOR**
- 83 Lomako A. G., Isaev N. E., Menisov A. B., Sabirov T. R.
**AN APPROACH TO IDENTIFYING SOFTWARE CODE VULNERABILITIES
BASED ON ADAPTATION WITH REINFORCEMENT LEARNING
OF MACHINE LEARNING MODELS**

APPLIED CRYPTOGRAPHY

- 97 Kostin S. O., Aleksandrova E. B.
**MULTIPLE SIGNATURES ON ELLIPTIC CURVE ISOGENIES
WITH MASKING AND PARTICIPANT AUTHENTICATION**

- 106** Shenets N. N., Aleksandrova E. B., Konoplev A. S., Gololobov N. V.
**GENERAL SOLUTION TO THE SPECIAL PROBLEM
OF DISTRIBUTING SHARES USING SHAMIR'S SECRET SHARING SCHEME**

NETWORK AND TELECOMMUNICATION SECURITY

- 121** Novikov P. A., Dichenko S. A., Lukyanov R. V., Polikarenkov S. V., Martynov M. L.
**A MATHEMATICAL MODEL AND METHODOLOGY
FOR EVALUATING THE EFFECTIVENESS OF NETWORK MONITORING
OF DATA TRANSMISSION NETWORK SECURITY**
- 132** Pahomov M. A.
**MODEL OF NODE INTERACTION IN A MOBILE AD-HOC NETWORK
CONSIDERING PROTECTION AGAINST ACTIVE NETWORK ATTACKS**
- 145** Skrypnikov A. K., Krundyshev V. M., Kalinin M. O.
**ANONYMIZATION OF NETWORK TRAFFIC IN BLOCKCHAIN SYSTEMS
BY USING GARLIC ROUTING**

TECHNOLOGICAL SYSTEMS, ALGORITHMIZATION OF TASKS AND CONTROL OBJECTS MODELING

- 155** Sikarev I. A., Abramov V. M., Prostakevich K. S., Abramova A. L., Chestnov A. I.
**AUTOMATION OF ARCHIVING FOR ATMOSPHERIC PRECIPITATION
MEASUREMENT INFORMATION**