

# ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ

## НАУЧНЫЙ РЕЦЕНЗИРУЕМЫЙ ЖУРНАЛ

№3 (67) 2025 г.

Выходит 6 раз в год

Журнал выходит с 2013 г. (Свидетельство о регистрации ПИ № ФС77-75239). Перерегистрировано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций 07.03.2019.

Журнал входит в рейтинг научных изданий ВАК в категории К1, индексируется в RSCI, публикует статьи по специальностям 1.2.4 и 2.3.6 – физ.-мат. науки; 2.2.15, 2.3.1, 2.3.5, 2.3.6 – техн. науки

### Главный редактор

**МАРКОВ Алексей Сергеевич**, д. т. н., с. н. с., Москва

### Председатель Редакционного совета

**ШЕРЕМЕТ Игорь Анатольевич**, академик РАН, д. т. н., профессор, Москва

### Шеф-редактор

**МАКАРЕНКО Григорий Иванович**, с. н. с., шеф-редактор, Москва

### Редакционный совет

**БАСАРАБ Михаил Алексеевич**, д. ф.-м. н., Москва

**КАЛАШНИКОВ Андрей Олегович**, д. т. н., Москва

**КРУГЛИКОВ Сергей Владимирович**, д. в. н., к. т. н., профессор, Минск, Беларусь

**ПЕТРЕНКО Сергей Анатольевич**, д. т. н., профессор, Иннополис

**СТАРОДУБЦЕВ Юрий Иванович**, д. в. н., профессор, Санкт-Петербург

**ЯЗОВ Юрий Константинович**, д. т. н., профессор, Воронеж

### Редакционная коллегия

**БАБЕНКО Людмила Климентьевна**, д. т. н., профессор, Таганрог

**БАРАНОВ Александр Павлович**, д. ф.-м. н., профессор, Москва

**ГАРБУК Сергей Владимирович**, к. т. н., с. н. с., Москва

**ГАЦЕНКО Олег Юрьевич**, д. т. н., с. н. с., Санкт-Петербург

**ЗЕГЖДА Дмитрий Петрович**, член-корреспондент РАН, д. т. н., профессор, Санкт-Петербург

**ЗУБАРЕВ Игорь Витальевич**, к. т. н., доцент, Москва

**КОЗАЧОК Александр Васильевич**, д. т. н., Орел

**МАКСИМОВ Роман Викторович**, д. т. н., профессор, Краснодар

**ПАНЧЕНКО Владислав Яковлевич**, академик РАН, д. ф.-м. н., профессор, Москва

**ПУДОВКИНА Марина Александровна**, д. ф.-м. н., профессор, Москва

**ЦИРЛОВ Валентин Леонидович**, к. т. н., доцент, Москва

**ШАХАЛОВ Игорь Юрьевич**, ответственный секретарь, Москва

**ШУБИНСКИЙ Игорь Борисович**, д. т. н., профессор, Москва

### Учредитель и издатель

АО «Научно-производственное  
объединение «Эшелон»

Над номером работали:

Г. И. Макаренко – шеф-редактор, И. Ю. Шахалов – отв. секретарь,  
С. С. Игнатов – верстка, Ю. С. Логинова – зам. главного редактора

Подписано к печати 20.06.2025 г.

Общий тираж 120 экз. Цена свободная

Адрес: 107023, Москва, ул. Электrozаводская, д. 24, стр. 1.

E-mail: editor@cyberrus.info, тел.: +7 (985) 939-75-01.

Требования, предъявляемые к рукописям,  
размещены на сайте: <https://cyberrus.info/>

Подписка на журнал осуществляется в почтовых отделениях по каталогу «Пресса России». Подписной индекс 40707

# СОДЕРЖАНИЕ

ОБРАЗОВАТЕЛЬНОМУ ЦЕНТРУ «СИРИУС» – 10 ЛЕТ

Гусев А. С. .... 2

ПРЕДСТАВЛЕНИЕ ТЕМАТИЧЕСКОГО ВЫПУСКА ЖУРНАЛА

Ширяев М. В. .... 4

ТИПОВЫЕ УРАВНЕНИЯ ВЕРИФИКАЦИИ  
В АЛГЕБРАИЧЕСКИХ СХЕМАХ ЭЦП  
С ДВУМЯ СКРЫТЫМИ ГРУППАМИ

Молдовян Н. А., Петренко А. С. .... 8

МЕТОДЫ ЗАЩИТЫ ОТ АТАК ПО ПОБОЧНЫМ КАНАЛАМ  
АППАРАТНОЙ РЕАЛИЗАЦИИ СХЕМ ПОСТКВАНТОВОЙ  
ПОДПИСИ, ПОСТРОЕННЫХ НА ОСНОВЕ ПРОТОКОЛА  
ИДЕНТИФИКАЦИИ ШТЕРНА

Смирнов Д. К., Чижов И. В. .... 21

О ПРИМЕНИМОСТИ ПОСТКВАНТОВОГО  
СТАНДАРТА ЭЛЕКТРОННОЙ ПОДПИСИ SLH-DSA  
В СМАРТ-КАРТАХ

Панасенко С. П. .... 29

УСКОРЕНИЕ АЛГОРИТМОВ ПРИВЕДЕНИЯ ЧИСЕЛ  
ПО МОДУЛЮ В ПОСТКВАНТОВОЙ СХЕМЕ  
ЭЦП FALCON

Фиошин М. А., Иванова И. Д., Жуков И. Ю. .... 38

АЛГОРИТМ ЭЦП НА АЛГЕБРЕ МАТРИЦ  $3 \times 3$ ,  
ИСПОЛЬЗУЮЩИЙ ДВЕ СКРЫТЫЕ ГРУППЫ

Захаров Д. В., Костина А. А., Морозова Е. В., Молдовян Д. Н. .... 45

КВАНТОВО-УСИЛЕННЫЙ СИММЕТРИЧНЫЙ  
КРИПТОАНАЛИЗ S-AES

Моисеевский А. Д., Манько С. Д. .... 55

О ВЛИЯНИИ КРИПТОГРАФИЧЕСКОЙ СТОЙКОСТИ  
ФУНКЦИЙ ХЕШИРОВАНИЯ НА УСТОЙЧИВОСТЬ  
СОВРЕМЕННЫХ БЛОКЧЕЙН-ЭКОСИСТЕМ  
И ПЛАТФОРМ

Ищуклова Е. А. .... 63

МОДЕЛЬ БЛОКЧЕЙН-ПЛАТФОРМЫ  
С КИБЕРИММУНИТЕТОМ В УСЛОВИЯХ  
КВАНТОВЫХ АТАК

Балябин А. А., Петренко А. А. .... 72

ФУНКЦИОНАЛЬНАЯ УСТОЙЧИВОСТЬ  
РАСПРЕДЕЛЕННОГО РЕЕСТРА В УСЛОВИЯХ  
ПОЯВЛЕНИЯ НОВОЙ КВАНТОВОЙ УГРОЗЫ

Сундеев П. В. .... 83

КВАНТОВЫЕ СЕТИ: РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ  
ЧЕРЕЗ НЕДОВЕРЕННЫЕ УЗЛЫ

Кулик С. П., Молотков С. Н. .... 90

КВАНТОВЫЙ КРИПТОАНКЛАВ ДЛЯ РЕАЛИЗАЦИИ  
НЕКОМПРОМЕТИРУЕМЫХ ДОВЕРЕННЫХ ЦЕНТРОВ  
ОБРАБОТКИ ДАННЫХ

Елисеев В. Л. .... 99

ОПРЕДЕЛЕНИЕ ДОСТОВЕРНОСТИ ОДНОКУБИТНЫХ  
ОПЕРАЦИЙ МЕТОДОМ РАНДОМИЗИРОВАННОГО  
БЕНЧМАРКИНГА

Бантыш Б. И., Заливако И. В., Колачевский Н. Н., Федоров А. К. .... 105

НОВЫЕ ПОДХОДЫ К ОЦЕНКАМ ИНФОРМАЦИИ  
ПЕРЕХВАТЧИКА В ПРОБЛЕМАХ КВАНТОВОЙ  
КРИПТОГРАФИИ

Кронберг Д. А., Холево А. С. .... 110