

# ИЗВЕСТИЯ ЮФУ. ТЕХНИЧЕСКИЕ НАУКИ IZVESTIYA SFedU. ENGINEERING SCIENCES

Свидетельство о регистрации средства массовой информации

ПИ № ФС77-28889 от 12.07.2007

Научно-технический и прикладной журнал

Издается с 1995 года

Подписной индекс 41970

№ 2 (151). 2014 г.

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

---

Журнал включен в «Перечень российских рецензируемых научных журналов, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученых степеней доктора и кандидата наук».

Журнал включен в Реферативный журнал и Базы данных ВИНТИ. Сведения о журнале ежегодно публикуются в международной справочной системе по периодическим и продолжающимся изданиям «Ulrich`s Periodicals Directory».

### *Редакционный совет*

Каляев И.А. (председатель); Курейчик В.М. (зам. председателя); Моськин В.Н. (ученый секретарь); Абрамов С.М.; Агеев О.А.; Бабенко Л.К.; Вагин В.Н.; Веселов Г.Е.; Гонкальвес Ж.; Колесников А.А.; Коноплев Б.Г.; Курейчик В.В.; Левин И.И.; Макаревич О.Б.; Маркович И.И.; Микрин Е.А.; Никитов С.А.; Обуховец В.А.; Осипов Г.С.; Панатов Г.С.; Панич А.Е.; Петров В.В.; Петровский А.Б.; Пшихопов В.Х.; Редько В.Г.; Румянцев К.Е.; Саламах М.; Солдатов А.В.; Стемпковский А.Л.; Сухинов А.И.; Сысоев В.В.; Тарасов С.П.; Федотов А.А.; Фрадков А.Л.; Хашемипур М.; Чаплыгин Ю.А.; Чердниченко Д.И.; Четверушкин Б.Н.; Чичков Б.Н.

*Рецензент номера* д.т.н., профессор Румянцев К.Е.

*Учредитель* Южный федеральный университет.

*Издатель* Технологический институт Южного федерального университета  
в г. Таганроге.

*Ответственный за выпуск* Макаревич О.Б.

*Главный редактор* Ярошевич Н.В.

*Оригинал-макет выполнен* Ярошевич Н.В.

ЛР № 020565 от 23.06.1997 г. Подписано к печати 27.02.2014 г.

Формат 70×108  $\frac{1}{8}$ . Бумага офсетная.

Офсетная печать. Усл. печ. л. – 32,1. Уч.-изд. л. – 32,0.

Заказ № . Тираж 250 экз.

*Адрес издателя:* 347928, г. Таганрог, ГСП 17А, Некрасовский, 44.

*Адрес типографии:* 347928, г. Таганрог, ГСП 17А, Энгельса, 1.

*Адрес редколлегии:* 347928, г. Таганрог, ГСП 17А, пер. Некрасовский, 44,

ТТИ ЮФУ, Д-211, телефон/факс: +7 8634 371-071.

e-mail: [onti@tgn.sfedu.ru](mailto:onti@tgn.sfedu.ru), <http://izv-tn.tti.sfedu.ru/>.

ISSN 1999-9429 (Print)

© Технологический институт

ISSN 2311-3103 (Online)

Южного федерального университета в г. Таганроге, 2014

## СОДЕРЖАНИЕ

### РАЗДЕЛ I. КОНЦЕПТУАЛЬНЫЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

<b>В.И. Васильев, Б.Г. Ильясов, Т.А. Иванова</b> МЕТОДОЛОГИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В СЛОЖНЫХ ОРГАНИЗАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ ТРИАДНОГО ПОДХОДА....	7
<b>А.Ю. Гуфан, К.И. Полюшкина</b> КУМУЛЯТИВНЫЙ ПОДХОД К ИСПОЛЬЗОВАНИЮ ВЕРОЯТНОСТНЫХ МЕТОДОВ ОБНАРУЖЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	16

### РАЗДЕЛ II. БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ И СЕТЕЙ

<b>А.Т. Алиев</b> ПРОАКТИВНЫЕ СИСТЕМЫ ЗАЩИТЫ ОТ ВРЕДНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ.....	26
<b>Ю.А. Брюхомицкий</b> ИММУНОЛОГИЧЕСКИЙ ПОДХОД К ОРГАНИЗАЦИИ КЛАВИАТУРНОГО МОНИТОРИНГА .....	33
<b>Е.А. Пакулова</b> АЛГОРИТМ РАСПРЕДЕЛЕНИЯ ПОТОКОВОГО ТРАФИКА И ТРАФИКА РЕАЛЬНОГО ВРЕМЕНИ В ГЕТЕРОГЕННОЙ БЕСПРОВОДНОЙ СЕТИ.....	42
<b>А.А. Бешта, А.М. Цыбулин</b> АЛГОРИТМ ОБНАРУЖЕНИЯ ВНУТРЕННЕГО НАРУШИТЕЛЯ НА ОСНОВЕ МЕХАНИЗМА ОЦЕНКИ ДОВЕРИЯ .....	50
<b>В.И. Васильев, И.В. Шарабыров</b> ОБНАРУЖЕНИЕ АТАК В ЛОКАЛЬНЫХ БЕСПРОВОДНЫХ СЕТЯХ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ .....	57
<b>В.М. Федоров, Д.П. Рублев</b> ИДЕНТИФИКАЦИЯ НАБИРАЕМОГО НА КЛАВИАТУРЕ ТЕКСТА ПО ВИБРОАКУСТИЧЕСКИМ ШУМАМ .....	67
<b>А.Ю. Оладько, В.С. Аткина</b> МОДЕЛЬ ЗАЩИТЫ ИНТЕРНЕТ-МАГАЗИНА .....	74
<b>А.В. Никишова, Р.Ф. Рудиков, Е.А. Калинина</b> НЕЙРОСЕТЕВОЙ АНАЛИЗ СОБЫТИЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ.....	80
<b>И.Ю. Половко, О.Ю. Пескова</b> АНАЛИЗ ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ К СИСТЕМАМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ.....	86
<b>Е.С. Абрамов, М.А. Кобилев, Л.С. Крамаров, Д.В. Мордвин</b> ИСПОЛЬЗОВАНИЕ ГРАФА АТАК ДЛЯ АВТОМАТИЗИРОВАННОГО РАСЧЕТА МЕР ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТИ.....	92
<b>Е.С. Абрамов, Е.С. Басан, Виджай Лакшми</b> РАЗРАБОТКА ЗАЩИЩЕННОГО ПРОТОКОЛА УПРАВЛЕНИЯ МОБИЛЬНОЙ КЛАСТЕРНОЙ СЕНСОРНОЙ СЕТЬЮ .....	101

### РАЗДЕЛ III. ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

<b>Е.А. Максимова, Т.А. Омельченко, В.В. Алексеенко</b> ПРОБЛЕМЫ РАЗРАБОТКИ ЧАСТНОЙ ПОЛИТИКИ МЕНЕДЖМЕНТА ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ .....	108
<b>А.М. Цыбулин, В.А. Балдаев, А.А. Бешта</b> АУТСОРСИНГ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ .....	114
<b>Е.П. Соколовский, О.А. Финько</b> ИНФОРМАЦИОННАЯ ПОДДЕРЖКА УПРАВЛЕНИЯ ЗАПАСАМИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ .....	120

#### РАЗДЕЛ IV. МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИИ И СТЕГАНОГРАФИИ

<b>Л.К. Бабенко, Е.А. Ищукова</b> АНАЛИЗ АЛГОРИТМА ГОСТ 28147-89: ПОИСК СЛАБЫХ БЛОКОВ.....	129
<b>Л.К. Бабенко, Е.А. Ищукова</b> ИСПОЛЬЗОВАНИЕ СЛАБЫХ БЛОКОВ ЗАМЕНЫ ДЛЯ ЛИНЕЙНОГО КРИПТОАНАЛИЗА БЛОЧНЫХ ШИФРОВ.....	138
<b>А.В. Бессалов, А.А. Дихтенко, О.В. Цыганкова</b> ПЛОТНОСТЬ КАНОНИЧЕСКИХ ЭЛЛИПТИЧЕСКИХ КРИВЫХ СО СВОЙСТВОМ ИЗОМОРФИЗМА К ФОРМЕ ЭДВАРДСА.....	146
<b>Л.К. Бабенко, Е.А. Маро</b> АЛГОРИТМЫ ОЦЕНКИ СТОЙКОСТИ МЕТОДАМИ АЛГЕБРАИЧЕСКОГО АНАЛИЗА .....	153
<b>А.С. Елисеев, А.Р. Тикиджи-Хамбурьян</b> СТАТИСТИЧЕСКИЙ СТЕГАНОГРАФИЧЕСКИЙ АНАЛИЗ ИСТОЧНИКОВ КОНТЕЙНЕРОВ ОДИНАКОВОГО ТИПА С ИСПОЛЬЗОВАНИЕМ БАЗОВОГО МЕТОДА АНАЛИЗА ОТДЕЛЬНЫХ КОНТЕЙНЕРОВ НЕИЗВЕСТНОЙ СТРУКТУРЫ.....	158
<b>Ю.Е. Рябинин, О.А. Финько</b> УСТОЙЧИВАЯ К АТАКАМ СТЕГАНОГРАФИЧЕСКАЯ СИСТЕМА В РАСШИРЕННОМ МОДУЛЯРНОМ КОДЕ .....	167
<b>Л.К. Бабенко, Д.А. Беспалов, О.Б. Макаревич, Р.Д. Чесноков, Я.А. Трубников</b> РАЗРАБОТКА И ИССЛЕДОВАНИЕ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА ШИФРОВАНИЯ ПО АЛГОРИТМУ PRESENT ДЛЯ РЕШЕНИЯ ЗАДАЧ МАЛОРЕСУРСНОЙ КРИПТОГРАФИИ.....	174

#### РАЗДЕЛ V. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

<b>И.А. Калмыков, О.В. Вельц, М.И. Калмыков, Д.О. Науменко</b> АЛГОРИТМ ИМИТОЗАЩИТЫ ДЛЯ СИСТЕМ УДАЛЕННОГО МОНИТОРИНГА И УПРАВЛЕНИЯ КРИТИЧЕСКИМИ ТЕХНОЛОГИЯМИ.....	181
<b>С.В. Котенко</b> ИДЕНТИФИКАЦИОННЫЙ АНАЛИЗ ПРОЦЕССОВ ТЕЛЕКОММУНИКАЦИИ НЕПРЕРЫВНЫХ СООБЩЕНИЙ В ЦИФРОВЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ .....	187
<b>В.М. Деундяк, Ю.В. Косолапов</b> ОБ ОДНОМ МЕТОДЕ СНЯТИЯ НЕОПРЕДЕЛЕННОСТИ В КАНАЛЕ С ПОМЕХАМИ В СЛУЧАЕ ПРИМЕНЕНИЯ КОДОВОГО ЗАШУМЛЕНИЯ.....	197
<b>А.Ф. Чипига</b> АНАЛИЗ ЭНЕРГЕТИЧЕСКОЙ СКРЫТНОСТИ НИЗКОЧАСТОТНЫХ СИСТЕМ СПУТНИКОВОЙ СВЯЗИ ОТ ОБНАРУЖЕНИЯ СИГНАЛОВ .....	209

#### РАЗДЕЛ VI. ПРИКЛАДНЫЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

<b>И.А. Калмыков, А.Б. Саркисов, А.В. Макарова, М.И. Калмыков</b> РАСШИРЕНИЕ МЕТОДОВ ЗАЩИТЫ СИСТЕМ ЭЛЕКТРОННОЙ КОММЕРЦИИ НА ОСНОВЕ МОДУЛЯРНЫХ АЛГЕБРАИЧЕСКИХ СХЕМ.....	218
<b>Л.В. Толмачёва, Е.Н. Каменская</b> АНАЛИЗ ВОЗДЕЙСТВИЙ ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ НА СТУДЕНТА ТЕХНИЧЕСКОГО ВУЗА .....	225
<b>Н.Д. Абасов</b> ОРГАНИЗАЦИЯ ЖУРНАЛА ТРАНЗАКЦИИ OLTP-СИСТЕМЫ, ФУНКЦИОНИРУЮЩЕГО В ИЗБЫТОЧНОМ МОДУЛЯРНОМ КОДЕ.....	231

<b>О.Ю. Пескова, И.Ю. Половко, С.В. Фатеева</b> ОБЗОР ПОДХОДОВ К ОРГАНИЗАЦИИ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ.....	237
<b>К.А. Катков, Е.К. Катков</b> ПОВЫШЕНИЕ ИНФОРМАЦИОННОЙ ЗАЩИЩЕННОСТИ СПУТНИКОВЫХ РАДИОНАВИГАЦИОННЫХ СИСТЕМ ПРИ ИСКУССТВЕННЫХ ИОНОСФЕРНЫХ ВОЗМУЩЕНИЯХ .....	247

## CONTENTS

### SECTION I. CONCEPTUAL ISSUES OF INFORMATION SECURITY

<b>V.I. Vasilyev, B.G. Ilyasov, T.A. Ivanova</b> METHODOLOGY OF PROVIDING OF COMPLEX ORGANIZATIONAL SYSTEMS SECURITY ON BASIS OF TRIAD APPROACH .....	7
<b>A.Y. Gufan, K.I. Polyushkina</b> CUMULATIVE APPROACH USING PROBABILISTIC METHODS FOR DETECTION INFORMATION SECURITY THREATS .....	17

### SECTION II. SECURITY OF INFORMATION SYSTEMS AND NETWORKS

<b>A.T. Aliev</b> PROACTIVE MALWARE PROTECTION SYSTEMS .....	26
<b>Yu.A. Bryukhomitsky</b> THE IMMUNOLOGIC APPROACH TO KEYBOARD MONITORING ORGANIZATION .....	34
<b>E.A. Pakulova</b> SENDER-SIDE PATH-SCHEDULING ALGORITHM FOR VIDEO STREAM ALLOCATION IN HETEROGENEOUS WIRELESS NETWORK.....	42
<b>A.A. Beshta, A.M. Tsybulin</b> ALGORITHM OF INSADERS DETECTION BASED ON CONFIDENCE EVALUATION.....	51
<b>V.I. Vasilyev, I.V. Sharabyrov</b> LOCAL WIRELESS NETWORKS ATTACKS DETECTION BASED ON INTELLIGENT DATA ANALYSIS.....	58
<b>V.M. Fedorov, D.P. Rublev</b> IDENTIFICATION OF TEXT TYPED ON KEYBOARD BY VIBROACOUSTICS NOISES.....	67
<b>A.Yu. Oladko, V.S. Atkina</b> MODEL OF ONLINE STORE PROTECTION.....	74
<b>A.V. Nikishova, R.F. Rudikov, E.A. Kalinina</b> NEURAL NETWORK ANALYSIS OF SECURITY EVENTS IN INFORMATION SYSTEM.....	81
<b>I.Y. Polovko, O.Y. Peskova</b> ANALYSIS OF THE FUNCTIONAL REQUIREMENTS FOR INTRUSION DETECTION SYSTEMS .....	87
<b>E.S. Abramov, M.A. Kobilev, L.S. Kramorov, D.V. Mordvin</b> DESIGN OF COUNTERMEASURES FOR SECURITY RISKS OF ENTERPRISE NETWORKS BY USING ATTACK GRAPHS .....	92
<b>E.S. Abramov, E.S. Basan, Vijay Laxmi</b> DEVELOPMENT OF SECURE PROTOCOL FOR MOBILE CLUSTER SENSOR NETWORK MANAGEMENT .....	101

### SECTION III. SECURITY OF COMPLEX FACILITIES

<b>E.A. Maksimova, T.A. Omelchenko, V.V. Alekseenko</b> PROBLEMS OF PRIVATE POLICY OF INFORMATION SECURITY OF ENTERPRISE INCIDENTS MANAGEMENT DEVELOPMENT .....	108
<b>A.M. Tsybulin, V.A. Baldaev, A.A. Beshta</b> OUTSOURCE AND INFORMATION SECURITY .....	114
<b>E.P. Sokolovsky, O.A. Finko</b> INFORMATION SUPPORT OF STOCKPILE MANAGEMENT OF MEANS OF PROTECTION OF INFORMATION IN THE CONDITIONS OF UNCERTAINTY .....	121

## SECTION IV. METHODS AND MEANS OF CRYPTOGRAPHY AND STEGANOGRAPHY

<b>L.K. Babenko, E.A. Ischukova</b>	ANALYSIS OF ALGORITHM GOST 28147-89: RESEARCH OF WEAK S-BOXES .....	129
<b>L.K. Babenko, E.A. Ischukova</b>	USING OF WEAK BLOCKS OF REPLACEMENT FOR LINEAR CRYPTOANALYSIS OF BLOCK CIPHERS.....	139
<b>A.V. Bessalov, A.A. Dikhtenko, O.V. Tsygankova</b>	DENSITY OF THE CANONICAL ELLIPTIC CURVES HAVING A PROPERTY OF THE ISOMORPHISM TO AN EDWARDS FORM.....	146
<b>L.K. Babenko, E.A. Maro</b>	ALGORITHMS OF RESISTANCE EVALUATION CIPHERS BY ALGEBRAIC CRYPTANALYSIS METHOD .....	153
<b>A.S. Eliseev, A.R. Tikidzhi-Khamburian</b>	STATISTICAL STEGANALYSIS OF IMAGES SOURCES, BASED ON OPAQUE SEPARATE IMAGES STEGANALYSIS TECHNIQUE.....	158
<b>Ju.E. Ryabinin, O.A. Finko</b>	STEGANOGRAPHIC SYSTEM RESISTANT TO ATTACK IN THE EXTENDE MODULAR ARITHMETIC .....	167
<b>L.K. Babenko, D.A. Bessalov, O.B. Makarevich, R.D. Chesnokov, Y.A. Trubnikov</b>	SOFTWARE AND HARDWARE DEVELOPMENT AND RESEARCH OF ENCRYPTION ALGORITHM PRESENT FOR SOLVING PROBLEMS OF THE LIGHTWEIGHT CRYPTOGRAPHY .....	175

## SECTION V. SECURITY OF TELECOMMUNICATIONS

<b>I.A. Kalmykov, O.V. Velts, M.I. Kalmykov, D.O. Naumenko</b>	DEVELOPMENT OF AN ALGORITHM IMITATION RESISTANCE FOR OF REMOTE MONITORING AND CONTROL CRITICAL TECHNOLOGIES .....	181
<b>S.V. Kotenko</b>	IDENTIFICATION ANALYSIS OF PROCESSES TELECOMMUNICATIONS OF CONTINUOUS REPORTS IN DIGITAL INFORMATION SYSTEMS.....	188
<b>V.M. Deundyak, Yu.V. Kosolapov</b>	ONE METHOD OF REMOVING THE UNCERTAINTY IN THE CHANNEL WITH ERRORS IN THE CASE OF CODE NOISING .....	197
<b>A.F. Chipiga</b>	STEALTH ENERGY ANALYSIS OF LOW FREQUENCY SYSTEM OF SATELLITE COMMUNICATIONS FROM SIGNAL DETECTION .....	209

## SECTION VI. APPLICATIONS OF INFORMATION SECURITY

<b>I.A. Kalmykov, A.B. Sarkisov, A.V. Makarova, M.I. Kalmykov</b>	ENHANCED PROTECTION METHODS OF ELECTRONIC COMMERCE ON THE BASIS OF MODULAR ALGEBRAIC SCHEME .....	218
<b>L.V. Tolmacheva, E.N. Kamenskaya</b>	IMPACT ANALYSIS OF INFORMATION EDUCATIONAL ENVIRONMENT FOR A STUDENT OF A TECHNICAL UNIVERSITY .....	225
<b>N.D. Abasov</b>	ORGANISATION OF TRANSACTION LOG OLTP-SYSTEM FUNCTIONING IN SURPLUS MODULAR CODE .....	231
<b>O.Yu. Peskova, I.Yu. Polovko, S.V. Fateeva</b>	REVIEW OF APPROACHES TO THE ORGANIZATION OF ELECTRONIC VOTING .....	237
<b>K.A. Katkov, E.K. Katkov</b>	IMPROVING THE INFORMATION SECURITY OF THE SATELLITE RADIO NAVIGATION SYSTEMS WITH ARTIFICIAL IONOSPHERIC DISTURBANCES.....	248