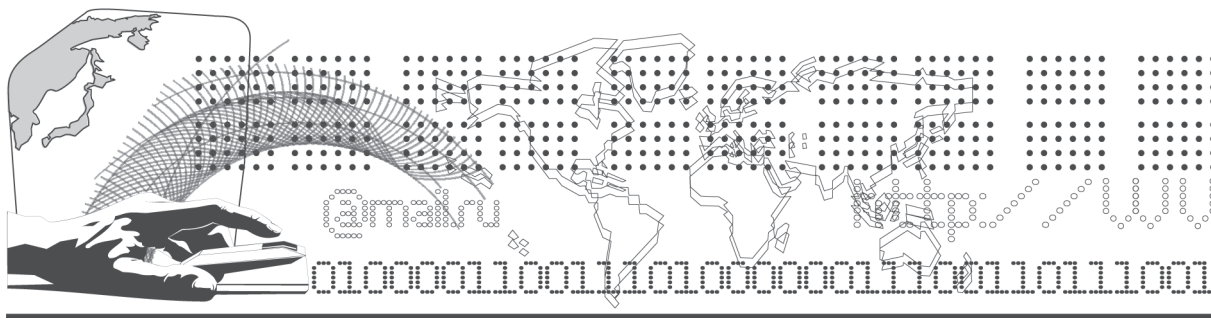




CONTENTS

INFORMATION SECURITY APPLICATION

- 9 *Sokolov A. S., Chernov A. Y., Konoplev A. S.*
**MITIGATION OF SPECULATIVE EXECUTION ATTACKS
BY INTEL DAL TECHNOLOGY APPLICATION**
- 20 *Sopin K. Yu., Povchun I. O., Dichenko S. A., Samoylenko D. V.*
**ENSURING DATA INTEGRITY BASED ON
NUMBER-THEORETICAL GAUSS TRANSFORMATIONS**

APPLIED CRYPTOGRAPHY

- 30 *Belim S. V., Munko S. N.*
**ALGORITHM FOR EMBEDDING DIGITAL WATERMARK
IN DYNAMIC MEMORY OF EXECUTABLE CODE**
- 35 *Berezovskaya O. I., Chuprov S. S., Neverov E. A., Sadreev E. R.*
**REVIEW AND COMPARISON OF AES LIGHTWEIGHT MODIFICATIONS
FOR A LOW-POWER DEVICES NETWORK**

CRITICAL INFORMATION INFRASTRUCTURE SECURITY

- 51 *Krudyshchev V. M., Kalinin M. O.*
**ADAPTIVE CONTROL SYSTEM FOR DETECTING COMPUTER ATTACKS
ON OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE**
- 65 *Pavlenko E. Yu., Fatin A. D.*
**IMMUNIZATION OF COMPLEX NETWORKS:
A SYSTEM OF DIFFERENTIAL EQUATIONS AND DYNAMIC VARIATION**
- 73 *Krudyshchev V. M.*
**MATHEMATICAL MODEL OF SPREAD OF COMPUTER ATTACKS
ON CRITICAL INFORMATION INFRASTRUCTURE**

RESEARCH, MONITORING AND OPTIMIZATION OF AUTOMATED PROCESS CONTROL SYSTEMS

- 82 *Sikarev I. A., Ivanyuk V. Yu., Sakharov V. V.*
DIGITALIZATION AND IDENTIFICATION OF ECG SIGNALS USING WAVELET TECHNOLOGIES

- 98** *Zabirov I. I., Mashkina I. V.*
**APPLYING OF IDENTIFICATION AND ACCESS CONTROL MANAGEMENT SYSTEM
IN INDUSTRIAL CONTROL SYSTEM**
- 106** *Sukhov A. M., Krupenin A. V., Yakunin V. I.*
**THE METHOD OF MODELING THE PROCESS OF FUNCTIONING
OF AN AUTOMATED SYSTEM OF SPECIAL PURPOSE
IN CONDITIONS OF DESTRUCTIVE INFLUENCES**

MACHINE LEARNING AND KNOWLEDGE CONTROL SYSTEMS

- 125** *Lebedev I. S., Sukhoparov M. E.*
**INFLUENCING FACTORS INFORMATION USAGE FOR SPLITTING DATA SAMPLES
IN MACHINE LEARNING METHODS TO ASSESS IS STATE**
- 135** *Gololobov N. V., Pavlenko E. Y.*
**COMPARISON OF THE EFFECTIVENESS OF ANOMALY DETECTION
BY MACHINE LEARNING ALGORITHMS WITHOUT A TEACHER**
- 148** *Rudnitskaya E. A., Poltavtseva M. A.*
**PROTECTION AGAINST ATTACKS ON MACHINE LEARNING SYSTEMS
ON THE EXAMPLE OF EVADIATION ATTACKS IN MEDICAL IMAGE ANALYSIS**