



CONTENTS

NETWORK AND CYBER-PHYSIC SYSTEMS SECURITY

- 13** *Pahomov M. A., Pavlenko E. Y., Sobolev H. V.*
ANALYSIS OF METHODS FOR ENSURING INFORMATION SECURITY OF WIRELESS AD-HOC NETWORKS
- 25** *Shtyrkina A. A., Aleksandrova E. B.*
CYBER PHYSICAL ATTACKS DETECTION BASED ON GRAPH FOURIER TRANSFORM
- 34** *Danilov V. D., Gribkov N. A., Ivanov D. V.*
ANALYSIS OF METHODS FOR DETECTING ARTIFICIALLY SYNTHESIZED CONTENT
- 45** *Zagal'skii D. S., Kashkarov O. E., Moskvina D. A., Solov'ev R. S., Loginov Z. G.*
DEVELOPMENT OF A METAVERSE MODEL FOR USER ACCESS CONTROL TO METAVERSE RESOURCES
- 54** *Izotova O. A., Lavrova D. S.*
EARLY DETECTION OF NETWORK ATTACKS BASED ON WEIGHT AGNOSTIC NEURAL NETWORKS
- 65** *Berko A. S., Poltavtseva M. A.*
A FRAMEWORK FOR SECURITY POLICIES MODELING FOR BIG DATA SYSTEMS
- 77** *Skokov N. S., Krundyshev V. M.*
ENSURING THE SECURITY OF WEB RESOURCES BASED ON INTELLIGENT ANALYSIS OF NETWORK TRAFFIC

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING SYSTEMS SECURITY

- 86** *Gololobov N. V., Pavlenko E. Y.*
CLASSIFICATION OF METHODS TO COUNTERACT A DATA POISONING ATTACK DURING NEURAL NETWORK TRAINING
- 95** *Soshnev M. D., Kalinin M. O.*
PROTECTION AGAINST THE THREAT OF THE MACHINE LEARNING MODELS EXTRACTION

- 108** *Rudnitskaya E. A., Poltavtseva M. A.*
PRIVACY OF MACHINE LEARNING MODELS
- 120** *Gololobov N. V., Zegzhda D. P.*
**A SET-THEORETIC MODEL OF DATA POISONING ATTACK TECHNIQUES
IN ARTIFICIAL INTELLIGENCE SYSTEMS**
- 130** *Dakhnovich A. D., Solovei R. S., Loginov Z. G., Zagalskii D. S., Moskvina D. A., Zegzhda D. P.*
**CAVIATS OF DETECTING UNFAIRNESS BIASES
IN RESULTS OF RECOMMENDER SYSTEMS**
- 139** *Ognev R. A., Zegzhda D. P.*
**AN EMPIRICAL STUDY OF THE ROBUSTNESS
OF A LINEAR FILTER BUILT ON THE NEYMAN-PEARSON CRITERION
TO A CHANGE IN THE MEAN VALUES**

SOFTWARE SECURITY

- 145** *Kubrin G. S., Zegzhda D. P.*
**VULNERABILITY DETECTION WITH AN ENSEMBLE
OF ANALYSIS ALGORITHMS FOR CODE GRAPH REPRESENTATION**
- 159** *Suprun A. F., Sobolev N. V.*
**A METHOD FOR DETECTING ATTACKS ON WEB APPLICATIONS
USING A WEB APPLICATION FIREWALL BASED ON AN ARTIFICIAL NEURAL NETWORK**

APPLIED CRYPTOGRAPHY

- 173** *Kuzmina K. A., Yarmak A. V., Aleksandrova E. B.*
PROXY SIGNATURE BASED ON GOST 34.10-2018
- 183** *Kostin S. O., Aleksandrova E. B.*
**RESEARCH OF THE ISOGENY GRAPH STRUCTURE
OF SUPERSINGULAR CURVES FOR POST-QUANTUM CRYPTOGRAPHY PROTOCOLS**