

## ЗМІСТ

<i>Степан Винничук, Евгений Максименко, Виталий Мисько</i>	
Оценка вычислительных затрат р-метода Полларда в зависимости от выбора отображения и начального приближения для малых факторизуемых чисел.....	263
<i>Сергій Родін</i>	
Дослідження моделей розповсюдження радіохвиль всередині приміщення для проектування живучих систем охорони побудованих на стандарті ZIGBEE...	268
<i>Анатолій Белецкий</i>	
Примитивные матрицы Гауа в криптографических приложениях.....	274
<i>Александр Корченко, Бахытжан Ахметов, Светлана Казмирчук, Андрей Гололобов, Нургуль Сейлова</i>	
Метод n-кратного понижения числа термов лингвистических переменных в задачах анализа и оценивания рисков.....	284
<i>Анна Корченко</i>	
Метод $\alpha$ -уровневой номинализации нечетких чисел для систем обнаружения вторжений.....	292
<i>Владислав Ковтун, Олексій Кінзерявий,</i>	
Експериментальне дослідження стійкості методу побітового приховування даних відносно атак на основі афінних перетворень....	304
<i>Анатолій Шиян, Юрій Яремчук</i>	
Модель та методи захисту структурованої соціальної групи від негативного інформаційно-психологічного впливу.....	311
<i>Гулом Туйчиев</i>	
О сети PES16–8, состоящей из восьми раундовых функций.....	318
<i>Дмитро Домарев, Яна Милокум</i>	
Модель конфліктних ситуацій в управлінні інформаційною безпекою.....	323
<i>Anton Alekseychuk, Sergey Gryshakov</i>	
On the computational security of randomized stream ciphers proposed by Mihaljević and Imai....	328
<i>Эмиль Фауре, Валерий Швыдкий, Валентина Шчерба</i>	
Метод формирования имитовставки на основе перестановок.....	334

## CONTENTS

<i>Stepan Vynnychuk, Evhenyy Maksymenko, Vitaliy Misko</i>	
Inequality of computational effort of Pollard p-method according to dispaaly selection and initial estimate for small-scale factorizable amounts.....	263
<i>Sergey Rodin</i>	
Research indoor radio propagation models for design survivability security systems built on the ZIGBEE standard.....	268
<i>Anatoliy Beletsky</i>	
Primitive matrix Galois in cryptographic application.....	274
<i>Oleksandr Korchenko, Bakhytzhān Akhmetov, Svitlana Kazmirchuk, Andrew Gololobov, Nurgul Seilova</i>	
The n-fold decrease method of terms number of linguistic variables in risk assessment and task analysis.....	284
<i>Anna Korchenko</i>	
The method of $\alpha$ -level of nominalization for intrusion detection systems.....	292
<i>Vladislav Kovtun, Oleksiy Kinzeryavyy</i>	
An experimental study of the stability of the bitwise data hiding method, relative to attacks, based on affine transformations.....	304
<i>Anatoliy Shyan, Iurii Iaremchyk</i>	
Model and methods for protection of structured social group from negative information- psychological impact.....	311
<i>Gulom Tuiychiev</i>	
About the network PES 16-8, consisting of eight round function.....	318
<i>Dmitry Domarev, Yana Mylokum</i>	
Model of a conflict situation in information security management.....	323
<i>Anton Alekseychuk, Sergey Gryshakov</i>	
On the computational security of randomized stream ciphers proposed by Mihaljević and Imai....	328
<i>Emil Faure, Valerii Shvydkii, Valentina Shcherba</i>	
Method of message authentication code formation based on permutations.....	334