

Національна Академія наук України  
Академія технологічних наук України  
Інженерна академія України  
Державний науково-дослідний інститут випробувань і сертифікації озброєння та  
військової техніки, Україна  
Університет Гліндор, м. Рексхем, Великобританія  
Військова дослідницька лабораторія США, м. Аделфі, США  
Інститут оборони ім. С. Лазарова, м. Софія, Болгарія  
Технічний університет Лодзі, Польща  
Технічний університет м. Рига, Латвія  
Технологічний університет м. Таллінн, Естонія  
Університет Екстрамадура, м. Бадахос, Іспанія  
Гомельський державний університет ім. Ф. Скорини, Білорусь  
Інститут проблем математичних машин і систем (ІПММС) НАН України  
Національний технічний університет України «Київський політехнічний  
інститут ім. І. Сікорського»  
Полтавський національний технічний університет імені Ю. Кондратюка  
Черкаський національний університет ім. Б. Хмельницького  
Чернігівський національний технологічний університет

## П'ЯТНАДЦЯТА МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

### МАТЕМАТИЧНЕ ТА ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ СИСТЕМ МОДС 2020

Тези доповідей



Чернігів 2020

Отже, досліджений метод дозволяє не тільки прогнозувати рівень загроз для корпоративної комп'ютерної мережі, але й досліджувати послідовність їх виникнення, адресу джерела та призначення, тип загрози, тощо. Алгоритм є адаптивним, оскільки його робота не залежить від конфігурації корпоративної комп'ютерної мережі.

## Література

1. The Mayhem Cyber Reasoning System / Thanassis Avgerinos, David Brumley, John Davis та ін.] // Security&Privacy / Thanassis Avgerinos, David Brumley, John Davis та ін.], 2018. – С. 52-60.
2. Cyber Reasoning Systems: Automating Cyber Warfare [Електронний ресурс] // Medium. – 2016. – Режим доступу до ресурсу: [https://medium.com/@joey\\_rideout/cyber-reasoning-systems-automating-cyber-warfare-3329f339edeb](https://medium.com/@joey_rideout/cyber-reasoning-systems-automating-cyber-warfare-3329f339edeb) .
3. Martin Husák. Predictions of Network Attacks in Collaborative Environment : дис. докт. / Martin Husák. – Brno, 2019. – 144 с.
4. O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing. “Automated generation and analysis of attack graphs”. / Security and privacy, 2002. Proceedings. 2002 IEEE Symposium on. IEEE. 2002, С. 273-284.
5. Z. t. Li, J. Lei, L. Wang, and D. Li. “A Data Mining Approach to Generating Network Attack Graph for Intrusion Prediction”. / Fuzzy Systems and Knowledge Discovery, 2007. FSKD 2007. Fourth International Conference on. Vol. 4. Aug. 2007, С. 307-311

УДК 004.056.55: 004.032: 004.93

## SIMULATING AND RESEARCH OF BLOCK PARAMETRIC MATRIX AFFINE-PERMUTATION CIPHERS (BP\_MAPCS) FOR CRYPTOGRAPHIC TRANSFORMATIONS

V.G. Krasilenko, A.A. Lazarev, D.V. Nikitovich  
*Vinnitsia National Technical University*

**Introduction, analysis of recent publications, formulation of the problems.** In the era of electronic communications, the need to transmit and cryptographic transformations (CTs) specific text and graphic documents (TGDs) in the form of table data, 2-D, 3-D, 4-D arrays, drawings, diagrams, resolutions has essentially increased [1-7]. Many TGDs contain restricted access information that in encrypted form, to transmit over communication channels, providing only access with their digital signatures. For security purposes technologies of cryptography, tools for CTs [1-7] and protocols for the formation of keys and their exchange [8, 9] are used, but only small part is devoted to methods oriented on matrix models (MM) [2, 3] and tools. That is why the search and research of new matrix models (MM) of CT, improvement of matrix ciphers are actual strategic task. In works [1, 2] generalized algorithms for CTs, so-called matrix affine-permutation ciphers

(MAPCs) [3] based matrix affinity ciphers (MACs), as modifications of known affine ciphers [2], were proposed. The results of simulation [1-7] of processes of CTs of images on the basis of such models have shown their significant advantages such as: greater stability, increase in speed. In work [2] on the basis of MACs the algorithm for creating a digital blind signature (DBS) is proposed. The results of modeling algorithms for creating a 2D key are also known [8]. One of main components of MAPCs [3] is matrix permutation model (MM\_P), which has obvious simplicity. Further improvement of matrix-type ciphers based on such MM\_P is highlighted in papers [6, 7]. Their basic operations are elemental multiplication, matrix addition and matrix permutation models (MM\_P) with multiplication matrices. However, as shown in papers [4], the CTs on their basis, without additional operations, do not modify histograms of TGDs. For most of works, there is a common significant disadvantage, especially for work related to MAC [1, 5], MAPCs [3] and the like [2, 4, 6, 7], which requires the use of at least two MK, if implemented multiplicative and additive components. Therefore, the search to improve especially the multi-step MAPCs [7] while maintaining stability and other characteristics, in order to reduce the number of MKs to one, and their experimental verification is a necessary urgent task. The emergence of multi-processors requires creation of appropriate matrix-algebraic models (MAM), matrix-type systems (MT) for CT. The promise of the MAM for the CT is evidenced by the ability to check the integrity of the cryptograms and the presence of distortions in them, increasing the cryptostability and expanding their functionality, as experimentally shown in [6]. The generalization of the MAM to a matrix-block view is necessary in terms of the versatility of block algorithms and independence on data volumes. Thus, the actual purpose is development of block modifications of the MAPCs with the possibility of choosing its parameters, cyclic/block keys, their simulation on real information objects (IO), demonstration of their possibilities and advantages.

**Presentation of research results.** The CT algorithm for encryption based on BP\_MAPCs consists of the following steps: 1) the partition of IO into blocks in the form of matrices with a dimension  $2^m \times 2^m$ , where  $m = 4, 5, 6, \dots$  and with element-bytes in a digital format that at  $m = 4$  is equivalent to the length of the block  $256 \times 8 = 2024$  bits; 2) the permutation of the bytes of each block using the current key (CK), which is formed synchronously from the main key by the selected procedure according to the parametric model, the argument of which is index of block, 3) matrix affine/affine-permutation transformations (MAPTs) of bytes in block using the CK, the same as on stage 2 or similar, but according to parametric model, 4) concatenation of received blocks for formation of cryptogram of IO. The decryption process has the following steps: 1) decomposing the cryptograms on blocks, 2) using MAPT for reversing of blocks based on the reversed CKs; 3) reversing the permutation of bytes of blocks by CKs; 4) concatenating the transformed blocks into the restored IO. The steps of permutations and affine CTs can change and repeat in different sequences. Modeling of BP\_MAPC was done

with Mathcad. Windows for CT modeling by BP\_MAPCs are shown in Fig. 1-5. The essence of MAPT is to apply to blocks, as set of bytes (PIC\_S, images), procedures pixel by pixel modulo multiplication/additions by corresponding 8-bit MKs (direct/inverse) of same dimensions, depending on the parameters, formation modules, which are shown in Fig. 2. As can be seen from the figures, the simulation Results of the processes of direct and reverse CT TGD, images confirm the correct operation of the models. As it was shown by researches, several iterative multiplications of the data (MD) on the MK P (permutations) to may not be sufficient with the application of the same MK for TGDs. In order to improve the algorithm, we propose applying various current MKs to blocks and increasing the dimension of MK and blocks do 256x256 bytes. Thus, the idea and essence of BP\_MAP-ciphers of CTs consists in using the functional dependencies of their parameters on block indices and additional vector keys (VK). The MP in the generally accepted form should be square with  $N \times N$  elements ("0" or "1"), where  $N = 2^{16}$ . The power of the set of MPs, that is, their number is estimated as  $N!$ , which gives huge values. Each address of a block can be represented using 2 bytes, indicate two coordinates (row and column) of the block. This enables to represent any permutation P by 2 blocks (256 x 256 elements) of bytes, putting in each identical address of these blocks the corresponding high byte (in first block) and the least significant byte (in second block) the coordinates of the new address of the byte for permutation. The Mathcad module for generating the main MK (MP) and of its components KeyA, KeyB in format of 2 gray images is shown in Fig. 2. We will show Mathcad windows with modules, formulas for calculating entropy and plotting a histogram, with parametric modules of forward and reverse CTs (qw-multiple permutations of block F bytes) and stream-MKs (larger MP) in isomorphic representation.

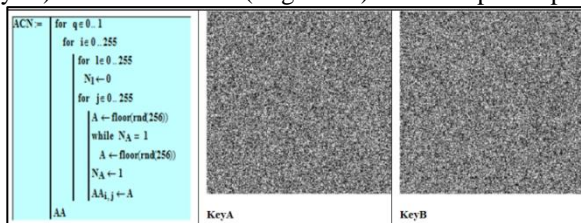


Fig. 1. The module for the generation of the head MP (KeyA and KeyB).

The analysis of histograms before/after the CTs confirms that the proposed models give better results. The TGD entropy was 0.738, and the cryptogram entropy increased 10.6–10.8 times and became equal to 7.82–7.999. The entropy of cryptogram has become almost equal to 8 bits per element: 7,999 (- 0.009 %!). Without knowledge of MK it is impossible to restore MD. As was shown in [2], already with dimension of 32x32 MK (P), the stability is ensured. The power of possible keys set has increased by many orders of magnitude with dimension 256x256 8-bit elements of key (power of keys set is estimated  $256^2$  !!). Therefore, stability has increased significantly.

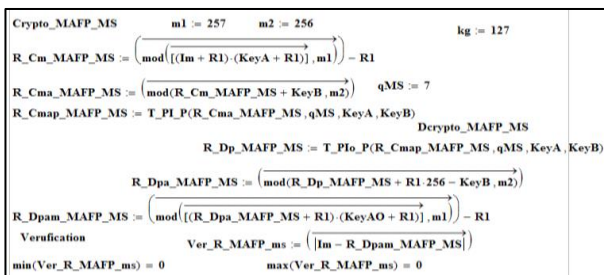


Figure 2. Mathcad window with BP\_MAPC of forward/reverse CTs (pixel-by-pixel affine encryption/decryption and multiple permutations).

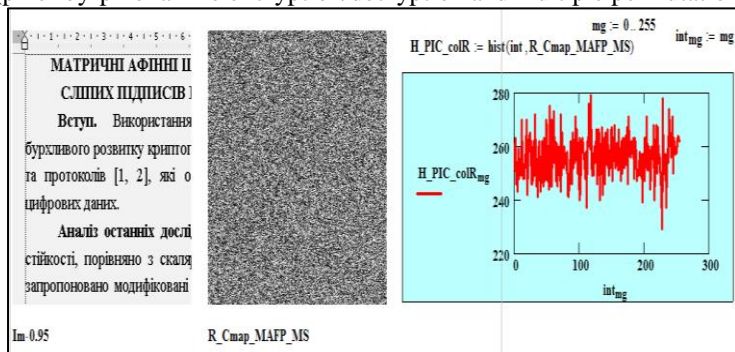


Figure 3. The results of cryptographic image Im conversion using BP\_MAPC: the original image, cryptogram and histogram of cryptogram.

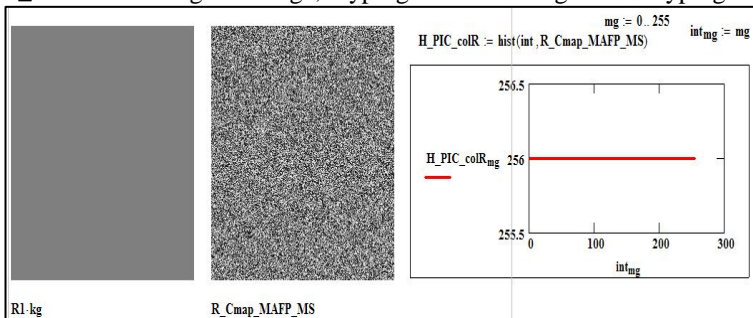


Figure 4. The results of cryptographic conversion of single-level image R1 using BP\_MAPC.

For MAM, it is urgently necessary to form a whole series of permutation matrices (MP) from main MK (MMK). Previously considered only MMK of general type was considered, but not the MP series. The aim of the work is to study the processes of formation of the MP flow for CTs and to check their properties. And in [9], questions were considered of creating by the parties a secret main MK of type P with isomorphic representations and the synthesis of set number of sub-keys of a similar type from it, therefore they are not considered in detail here, but will be covered in the report.

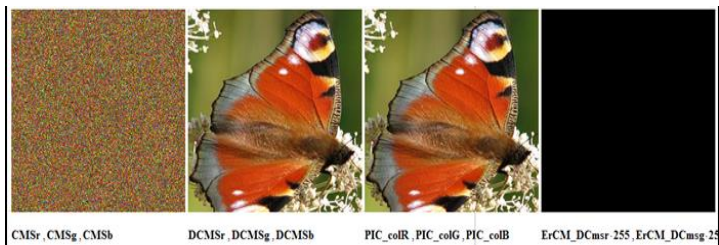


Figure 5. Forward and reverse CT color images using BP\_MAPC.

**The conclusions:** New block parametric matrix-algebraic models and matrix affine-permutation ciphers for CTs are proposed and modulated. The results of their modeling are presented using direct and inverse CT scans over images as an example, which indicates their correct operation and effectiveness. The entropy-histogram analysis of the obtained cryptograms, the advantages of the proposed modifications of ciphers with an increased permutation matrix are shown. The aspects of creating existing MKs are considered. Models can be implemented on matrix processors and have high speed, stability of transformations, and are more resistant to attacks.

## References

1. Krasilenko V.G. Modeling of Matrix Cryptographic Protection Algorithms / V.G. Krasilenko, Y.A. Flavitskaya // Bulletin "Computer Systems and Networks". - 2009. - No. 658. - pp. 59-63.
2. Krasilenko V.G., Matrix Affine Ciphers for the Creation of Digital Blind Signatures for Text-Graphic Documents / V.G. Krasilenko, S.K. Grabovlyak // Systems of information processing. - Kh.: KhUPPS, 2011. - Vol. 7 (97). - pp. 60 - 63.
3. Krasilenko V.G. Matrix affine and permutation ciphers for encryption and decryption of images / V.G Krasilenko, S.K. Grabovlyak // Systems of information processing. - Kh., 2012. - Vo. 3 (101). - t. 2. - pp. 53-62.
4. Krasilenko V.G. Cryptographic transformations of images based on matrix models of permutations with matrix-bit-map decomposition and their modeling / V.G. Krasilenko, V.M. Dubchak // Bulletin of Khm. National University. Technical sciences. - 2014. - No. 1. - pp. 74-79.
5. Krasilenko, V.G. Modeling of Matrix Affine Algorithms for the Encryption of Color Images / V.G. Krasilenko, K.V. Ogorodnik, Yu.A. Flavitskaya // Computer technologies: science and education: abstracts of reports v VseUkr. sci. conf. - K., 2010. - pp. 120-124.
6. Krasilenko V.G. Modeling and research of cryptographic transformations of images based on their matrix-bit-map decomposition and matrix models of permutations with verification of integrity / V.G. Krasilenko, D.V. Nikitovich // Electronics and Information Technologies. - Lviv: National University, 2016. - Vo. 6. – pp. 111-127.
7. Krasilenko V.G. Simulation of cryptographic transformations of color images based on matrix models of permutations with spectral and bit-

map decompositions / V.G. Krasilenko, D.V. Nikitovich // Computer-integrated technologies: education, science, production: sciences, - Lutsk: Lutsk Nat Tech Un., - 2016. - No. 23. - pp. 31-36.

8. Krasilenko V.G. Modeling Protocols for Matching a Secret Matrix Key for Cryptographic Transformations and Matrix-type Systems / V.G. Krasilenko, D.V. Nikitovich // Systems of information processing. - 2017 - Vo. 3 (149). – pp. 151-157.

9. Krasilenko VG Modeling of methods for generating flows of matrix permutations of significant dimension for cryptographic transformations of images // V.G. Krasilenko, D.V. Nikitovich // Abstracts of the II All-Ukrainian STC Computer Technologies: Innovations, Problems, Solutions. - Zhytomyr: Zhytomyr Polytechnic, 2019. - P. 67-77.

UDC 528.852.6(528.831.1):004.932.2

## MULTIFRAME REMOTE SENSED IMAGERY SUPERRESOLUTION

Sergey A. Stankevich, Artem A. Andreiev, Artur R. Lysenko  
*Scientific Centre for Aerospace Research of the Earth, Ukraine*

### Introduction

Spatial resolution is the most important criterion of remote sensing capabilities. Regardless of the continuous improvement of remote sensing imaging systems, in many cases a lack of spatial resolution is evident. Spatial resolution enhancement makes remote sensing applications more successful, so such enhancement is important and relevant now. However, the possible resolution of the remote sensing imagers' hardware is limited by the microminaturization technology of semiconductor sensor arrays on the one hand and the maximum allowable size of the lens on the other hand. However, the superresolution can be engaged too by joint processing of several subpixel-shifted images of the same scene [1].

### Method

The general image processing dataflow for a subpixel superresolution includes three stages: 1) acquiring several subpixel-shifted input images; 2) assigning a joint subpixel grid for all input images; 3) restoring the superresolution image from the input ones on the subpixel grid.

The first stage is done by co-registering and cutting the input images. The usual correlation method is used:

$$(\Delta x^*, \Delta y^*)_{II} = \operatorname{argmax} r[I(x, y), J(x+\Delta x, y+\Delta y)] \quad (1)$$

where  $I, J$  are overlapped images with grid coordinates  $x$  and  $y$ ,  $\Delta x, \Delta y$  are integer pixel shifts between images,  $r[\cdot]$  is the mutual correlation operator,  $\Delta x^*, \Delta y^*$  are optimal pixel shifts corresponding to image stacking.

The joint subpixel grid **Fig. 1** of co-registered images is determined in the second stage so that as the minimum possible number of pixels of the input images overlap each subpixel of grid.

## ЗМІСТ

<b>В. В. Вишневецький</b> УПРАВЛІННЯ ЖИТТЄВИМ ЦИКЛОМ ІНФОРМАЦІЙНИХ СИСТЕМ .....	17
<b>Фу Хун</b> ПЕРСПЕКТИВИ КИТАЙСКО-УКРАЇНСЬКОГО НАУКОВО-ТЕХНІЧНОГО СПІВРОБІТНИЦТВА.....	19
<b>С.Ф. Теленик, І.В. Стеценко, О.Г. Жданова</b> ВАЛЕНТИН МИКОЛАЙОВИЧ ТОМАШЕВСЬКИЙ – ПРОФЕСОР, НАУКОВЕЦЬ, ДІЯЧ ОСВІТИ.....	25

### СЕКЦІЯ 1

#### СУЧАСНІ АСПЕКТИ МАТЕМАТИЧНОГО ТА ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ СИСТЕМ В ЕКОЛОГІЇ ТА ГЕОЛОГІЇ

<b>ZATSERKOVNYI V.I., PAMPUKHA I.V., LEVINSKOVA N.V., SYNIAVSKA I.K., ТКАЧЕНКО А.А.</b> ANALYSIS OF APPROACHES FOR SOLVING GEOGRAPHIC INFORMATION PROCESSING AND SUBMISSION TASKS IN COMBAT VISUALIZATION SYSTEM.....	30
<b>НОМА V.V., VEZUHLYI V.M., TSYBA M.M., CHUKHLEV O.V., DRYZHYNIN V.A.</b> THE IMPLEMENTATION OF GEOINFORMATION SYSTEMS IN JOINT COMBAT TRAINING OF TACTICAL GROUPS.....	34
<b>С. Ю. Даншина, А. С. Нечаусов</b> ГІС У СОЦІАЛЬНИХ ПРОЕКТАХ МІСТА: АНАЛІЗ МЕРЕЖІ МЕДИЧНИХ ЗАКЛАДІВ.....	39



<b>О.О. Кряжич, О.В. Коваленко</b> ВИБІР ІНТЕРВАЛІВ АПРОКСИМАЦІЇ ФУНКЦІЇ ДЛЯ ВИРІШЕННЯ ЗАДАЧ ОПИСУ ЗАБРУДНЕНОЇ ТЕРИТОРІЇ .....	43
<b>Д.В. Кушнір, Ю.С. Тучковенко</b> МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ РІЧНОЇ МІНЛИВОСТІ ГІДРОЛОГІЧНИХ ХАРАКТЕРИСТИК У ЛИМАНІ САСИК ЗА УМОВ ВІДНОВЛЕННЯ ВОДООБМІНУ З МОРЕМ .....	47
<b>Терлецька К., Мадерич В., Бровченко І.</b> ТРАНСФОРМАЦІЯ ВНУТРІШНІХ УСАМІТНЕНИХ ХВИЛЬ НАД ПІДВОДНОЮ СХОДИНКОЮ У ТРИШАРОВІЙ СТРАТИФІКАЦІЇ.....	51
<b>О. РYЛУРЕНКО, М. ЗНЕЛЕЗНУАК, М. SOROKIN, S. KIVVA</b> МОДИФІКАЦІЯ ГІДРОЛОГІЧНОГО БЛОКУ СППР RODOS ДЛЯ КОМПЛЕКСНОГО МОДЕЛЮВАННЯ ВОДНИХ ОБ'ЄКТІВ.....	54
<b>М.В. Талах, С.В. Голуб</b> ІНФОРМАЦІЙНА СИСТЕМА КЛІМАТИЧНОГО МОНІТОРИНГУ .....	56
<b>С.О. Заїка, А.Т. Лобурець</b> ЗАСТОСУВАННЯ ДИНАМІКИ ЛАНЖЕВЕНА ДЛЯ МОДЕЛЮВАННЯ ПОШИРЕННЯ ВІРУСНИХ ІНФЕКЦІЙ НА ПРИКЛАДІ COVID-19 .....	60
<b>В.В. Бегун, Т.В. Полщук</b> АНАЛІЗ МОДЕЛЕЙ ВИЗНАЧЕННЯ РИЗИКУ КРИТИЧНО ВАЖЛИВОЇ ІНФРАСТРУКТУРИ .....	64
<b>С.Я. Майстренко, А.А. Полонский, А.В. Халченков, Т.А. Донцов-Загреба, К.В. Хурцилава, О.И. Удовенко, И.В. Ковалец</b> ВЕБ-СЕРВИС МОДЕЛИРОВАНИЯ АТМОСФЕРНЫХ ЗАГРЯЗНЕНИЙ В ОБЛАЧНОЙ ИНФРАСТРУКТУРЕ.....	67

**В.В. Кулик, О.І. ЯСТРЕМСЬКИЙ**  
ОЦІНКА ЗАБРУДНЕННЯ АТМОСФЕРНОГО ПОВІТРЯ  
ЗАЛЕЖНО ВІД ОБСЯГІВ КІНЦЕВОГО ПОПИТУ .....71

**В.В. Тютюник, О.О. Тютюник, Т.Х. АГАЗАДЕ**  
РЕЗУЛЬТАТИ НЕЙРОМЕРЕЖЕВОГО  
МОДЕЛЮВАННЯ ТА ПРОГНОЗУВАННЯ КІЛЬКОСТІ  
ЗЕМЛЕТРУСІВ З МАГНІТУДОЮ  $\geq 5$  ПО ЗЕМНІЙ КУЛІ .....74

## **СЕКЦІЯ 2**

### **СУЧАСНІ АСПЕКТИ МАТЕМАТИЧНОГО ТА ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ СИСТЕМ У ВИРОБНИЦТВІ**

**A.S. CHUMAK, L.Y. BUIVAL, A.M. HUMENNYI,  
O.G. GREBENIKOV, D. KONYSHEV**  
TRANSPORT CATEGORY AIRPLANE FUSELAGE  
MASTER GEOMETRY PARAMETRICAL  
MODELING METHOD .....80

**BOGDAN KORNIYENKO, LESYA LADIEVA, LILIYA GALATA**  
MATHEMATICAL MODEL OF HEAT TRANSFER  
PROCESS OF PRODUCTION OF GRANULATED  
FERTILIZERS IN FLUIDIZED BED .....84

**D. LEONTIEV, S. SHUKLINOV,  
V. MAKAROV, V. VERBYTSKIYI, A. GUBIN**  
STUDIES OF THE RECTILINEAR MOTION OF THE  
AXIS OF THE LOCKED WHEEL AFTER BRAKING  
THE CAR ON UPHILL .....87

**РЕУТСЬКА С.В., БАКЛАН І.В., ОЛІЙНИК Ю.О., ЛІЩУК К.І.**  
ПІДХІД ДО ВИЯВЛЕННЯ АНОМАЛІЙ В ДАНИХ ЕКГ .....91

**АЛЕКСИКОВ І.О., ДОЛІННА Є.О.**  
МОДЕЛЮВАННЯ СИСТЕМИ ПЕРЕДБАЧЕННЯ  
ПРОСТОЇВ НА ВИРОБНИЦТВІ ДЛЯ  
ТЕРМОПЛАСТАВТОМАТУ .....95

**ЛАКТИОНОВ О.І.**  
МЕТОДИ ТА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ  
ВИЗНАЧЕННЯ ЯКОСТІ ВИГОТОВЛЕНОЇ ПРОДУКЦІЇ ..... 99

**ГОДУН Р.Л., САВЕЛЬЕВ М.В.,**  
**ВИСОТСЬКИЙ Є.Д., СУЩЕНКО К.О., СКІТЕР І.С.**  
АНАЛІЗ НЕЙТРОННОЇ АКТИВНОСТІ НА ПЕРИФЕРІЇ  
ЛОКАЛІЗОВАНИХ В НБК-ОУ НАКОПИЧЕНЬ  
ПАЛИВОВМІСНИХ МАТЕРІАЛІВ ..... 103

### **СЕКЦІЯ 3**

#### **СУЧАСНІ АСПЕКТИ МАТЕМАТИЧНОГО ТА ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ СИСТЕМ В ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЯХ**

**ANDRIY BOYCHENKO, DMYTRO LANDE**  
GENERATION OF INFORMATION IMPACTS  
SCENARIOS IN MANAGEMENT DECISION  
SUPPORT SYSTEMS ..... 110

**Y.O. HORONOVYCH**  
NETWORK SECURITY CONFIGURATION  
ALGORITHM FOR LINUX SERVERS ..... 111

**L. PETROV, N. STOIANOV**  
ANALYSIS OF CRITICAL INFORMATION  
INFRASTRUCTURE PROTECTION MODEL (СІРМ) ..... 116

**Ю.М. ЛИСЕЦКИЙ, Д.И. КАЛБАЗОВ**  
ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА  
ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ ..... 117

**МІЩЕНКО М.В., ГРЕБЕННИК А.Г., ТРУНОВА О.В.**  
ПРОГНОЗУВАННЯ РІВНЯ ЗАГРОЗ  
З ВИКОРИСТАННЯМ МЕРЕЖ БАЙССА ..... 120

<b>V.G. KRASILENKO, A.A. LAZAREV, D.V. NIKITOVICH</b> SIMULATING AND RESEARCH OF BLOCK PARAMETRIC MATRIX AFFINE-PERMUTATION CIPHERS (BP_MAPCS) FOR CRYPTOGRAPHIC TRANSFORMATIONS .....	123
<b>SERGEY A. STANKEVICH, ARTEM A. ANDREIEV, ARTUR R. LYSENKO</b> MULTIFRAME REMOTE SENSED IMAGERY SUPERRESOLUTION .....	128
<b>JOHN N. DAVIES, MARIYA VEROVKO, OLEKSANDR VEROVKO, IRYNA SOLOMAKHA</b> INTEGRATING AI-ALGORITHMS INTO CHATBOT DEVELOPMENT USING AWS SERVICES .....	132
<b>O.F. VOLOSHYN, D.I. KOVALIOV</b> USING NATURAL LANGUAGE PROCESSING IN EVALUATING OPEN QUESTIONS .....	134
<b>М.В. Сорокин</b> МОДЕЛИРОВАНИЕ КОРАБЕЛЬНЫХ ВОЛН С ИСПОЛЬЗОВАНИЕМ УРАВНЕНИЙ МЕЛКОЙ ВОДЫ НА GPU .....	137
<b>N.T. STOIANOV, M.G. BOZHILOVA</b> EXPERT'S STUDY ON SITUATIONAL AWARENESS OF OPERATIONS DIRECTED AT THE WIDE DISSEMINATION OF MALICIOUS INFORMATION .....	141
<b>N.T. STOIANOV, M.G. BOZHILOVA, G.R. VELEV</b> HONEYPOT TYPES AS A POSSIBLE DATA SOURCE FOR THE CYRADARS PROJECT .....	144
<b>D.V. LANDE, O.O. DMYTRENKO, O.V. ANDRIICHUK, V.V. TSYGANOK, Y.V. PORPLENKO</b> BUILDING OF DIRECTED WEIGHTED NETWORKS OF TERMS FOR DECISION-MAKING SUPPORT DURING INFORMATION OPERATIONS RECOGNITION .....	147

<b>А.М. Хошаба, В.В. Литвинов, В.Ф. Гречанинов, К.С. Завертайло</b> МЕТОДЫ ОБЕСПЕЧЕНИЯ НАДЕЖНОСТИ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ СТРУКТУР В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ.....	148
<b>Ібнұхсейін І., Суворова В.Є.</b> ЗАДАЧА СКЛАДАННЯ РОЗКЛАДУ МЕТОДОМ ПРОМЕНЕВОГО ПОШУКУ .....	152
<b>BAKRI MADON, GARY LOH CHEE WYAI, A.V. JURCHENKO, Y.M. TKACH, M.E. SHELEST</b> DEVELOPMENT OF SARAWAK ENCRYPTION STANDARD TO SECURE SARAWAK DIGITAL ECONOMY INFRASTRUCTURE AND ENABLE UBIQUITOUS DEPLOYMENT OF IOT DEVICES AND SOLUTIONS .....	155
<b>И.В. Богдан, А.А. Задорожний</b> МЕТОДЫ ПРИОРИТЕЗАЦИИ ЗАДАЧ В ГИБКИХ МЕТОДОЛОГИЯХ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ.....	158
<b>ALYOSHIN S., НАІТАН О.</b> NEURAL NETWORK TECHNOLOGY OF RECOGNITION OF HACKER APPLICATIONS FOR TRAFFIC INTERCEPTION AND ANALYSIS.....	162
<b>П.Д. СЕСПЕДЕС Гарсия, Н.В. СЕСПЕДЕС Гарсия</b> АТРИБУТЫ И МЕТРИКИ ГАРАНТОСПОСОБНОГО ПРОГРАМНОГО ОБЕСПЕЧЕНИЯ .....	164
<b>Голуб С.В., Куницька С.Ю.</b> ІНТЕЛЕКТУАЛЬНІ АГЕНТИ МОНІТОРИНГОВИХ ІНФОРМАЦІЙНИХ СИСТЕМ.....	167
<b>Голуб С.В., Толбатов Д.В.</b> ПРОТЕКЦІЯ АРГУМЕНТІВ ПРИ СИНТЕЗІ ПРОГНОЗНИХ МОДЕЛЕЙ В МОНІТОРИНГОВИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ .....	169

<b>Курто О.С.</b> МОДЕЛЮВАННЯ КЛАСІВ ТЕКСТОВИХ ДОКУМЕНТІВ ПРИ ВИЗНАЧЕННІ ЇХ ПРИКЛАДНОЇ НАПРАВЛЕНОСТІ.....	171
<b>С.М. Лапач</b> ОЦІНКА СТРУКТУРНОЇ СТІЙКОСТІ РЕГРЕСІЙНОЇ МОДЕЛІ .....	174
<b>Медведніков Д.С., Олійник Ю.О.</b> АНАЛІЗ СУЧАСНИХ ЗАСОБІВ ТА МЕТОДІВ СЕНТИМЕНТ АНАЛІЗУ З ПІДТРИМКОЮ УКРАЇНОМОВНИХ ТЕКСТІВ.....	178
<b>Гончаров К.О., Онуфрієва А.О., Попенко В.Д., Сперкач М.О.</b> СКЛАДАННЯ РОЗКЛАДУ ВИВЧЕННЯ ТЕМ ПРИ ПІДГОТОВЦІ ДО ІСПИТУ ЗА УМОВИ ОБМЕЖЕНОГО ЧАСУ.....	181
<b>Оксанич І.М., Лопушанський А.В.</b> ПОБУДОВА МОДЕЛІ ІНФОРМАЦІЙНОЇ ВЗАЄМОДІЇ В РОЗРІЗНЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ.....	185
<b>О.С. Тарасов, А.Г. Гребенник, Трунова О.В.</b> ВИКОРИСТАННЯ МУЛЬТИАГЕНТНИХ СИСТЕМ ДЛЯ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ.....	186
<b>Кудряшова О.В., Блюус І.В.</b> ІНФОРМАЦІЙНА СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ПРО ВІДРЯДНУ ОПЛАТУ ПРАЦІ НА ПІДПРИЄМСТВАХ АВТОТРАНСПОРТУ .....	190
<b>Ровник О.С., Трунова О.В.</b> ІНФОРМАЦІЙНА СИСТЕМА РОЗПІЗНАВАННЯ ТА ОБРОБКИ ПЕРВИННОЇ ПРОЕКТНОЇ ІНФОРМАЦІЇ .....	194
<b>Н.О. Абрашина</b> КОНЦЕПТ СИСТЕМИ ВІРТУАЛЬНОГО ТИРУ НА ОСНОВІ ВІДЕО-ВВОДУ .....	196

<b>КОВАЛЕНКО М.А., Дорощ М.С.</b> СТВОРЕННЯ MLOPS ІНФРАСТРУКТУРИ ЗА ДОПОМОГОЮ ХМАРНИХ РІШЕНЬ.....	198
<b>АНДРУСЕНКО Б.Г., МАМЧУРОВСЬКИЙ В.С., ТРУНОВА О.В.</b> ПОРІВНЯННЯ МОВ ПРОГРАМУВАННЯ PYTHON TA R B DATA SCIENCE .....	201
<b>А.В. ЯРМІЛКО, І.О. РОЗЛОМІЙ, Г.В. КОСЕНЮК</b> МЕТОДИ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ ПОТОКІВ ІЗ ЗАСТОСУВАННЯМ ХЕШУВАННЯ.....	205
<b>КАЧАНОВСЬКИЙ П.П.</b> ІНФОРМАЦІЙНА СИСТЕМА ВИЗНАЧЕННЯ АВТОРСТВА ТЕКСТУ НА ОСНОВІ СИНТЕЗУ ФОРМАЛЬНИХ МЕТОДІВ АТРИБУЦІЇ.....	208
<b>С.В. ГРИБКОВ, В.А. ЛИТВИНОВ, А.В. ОЛЕЙНИК</b> ІНСТРУМЕНТАЛЬНА МОДЕЛЬ ПОДСИСТЕМИ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ.....	212
<b>ФЕДОРОВ В.В., ЛУДАНИК Р.В.</b> РОЗРОБКА МОБІЛЬНОЇ ГРИ “PHOTO HUNTER”.....	215
<b>МУХА АР.А.</b> АТРИБУТИВНА МОДЕЛЬ ГАРАНТОСПОСОБНОСТІ КОМПЬЮТЕРНОЇ СИСТЕМИ.....	217
<b>ЖУРКО Д.О., БЛОУС І.В.</b> МОДЕЛЮВАННЯ РОБОТИ СЛУЖБИ ПІДТРИМКИ ЗА ДОПОМОГОЮ МЕРЕЖ МАСОВОГО ОБСЛУГОВУВАННЯ ....	219
<b>Т.З. ФИДАРОВ</b> СТРУКТУРА И ОРГАНИЗАЦИЯ ВЕБ-СЛОВАРЯ ДЛЯ ИССЛЕДОВАНИЙ В ОБЛАСТЯХ РАЗРАБОТКИ, МОДЕЛИРОВАНИЯ И ПОДДЕРЖКИ ФУНКЦИОНИРОВАНИЯ ГАРАНТОСПОСОБНЫХ СИСТЕМ .....	221

<b>Н.О. Ткачук</b> МОРФОЛОГІЧНІ ПІДХОДИ ОБРОБКИ ПРИРОДНОЇ МОВИ ДЛЯ РОБОТИ З ПОШУКОВИМИ ЗАПИТАМИ.....	225
<b>Філон А.А., Гребенник А.Г.</b> АДАПТИВНЕ УПРАВЛІННЯ ЗАХИЩЕНІСТЮ КОРПОРАТИВНОЇ МЕРЕЖИ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ.....	229
<b>Ю.В. Бугай, З.М. Веремей</b> 3D-МОДЕЛЮВАННЯ В ОСВІТНЬОМУ ПРОЦЕСІ ВНЗ В УКРАЇНІ.....	233
<b>BOGDAN KORNIYENKO, LESYA LADIEVA, LILIYA GALATA</b> MATHEMATICAL MODEL OF HEAT TRANSFER PROCESS OF PRODUCTION OF GRANULATED FERTILIZERS IN FLUIDIZED BED.....	236
<b>Н. SARYВОНА, Y. YAMNENKO</b> REAL-TIME MOTION CONTROL SYSTEM FOR CAMERA CRANE BASED ON PID CONTROLLER AND INERTIAL MEASUREMENT UNIT .....	239
<b>М.І. Грищенко, В.О. Бойко, М.С. Дорош</b> ВИКОРИСТАННЯ НЕЙРОМЕРЕЖ ДЛЯ ВИЗНАЧЕННЯ ПОБАЖАНЬ СПОЖИВАЧІВ ЗАКЛАДІВ ХАРЧУВАННЯ .....	246
<b>В.Ф. ГРЕЧАНИНОВ, А.В. ЛОПУШАНСЬКИЙ</b> ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ БЕЗПЕКИ ТА ОБОРОНИ .....	249
<b>ANDRIY DEMYDENKO</b> WHAT TYPE OF MODELLING COULD BE USED FOR EFFECTIVE WATER SUSTAINABLE DEVELOPMENT GOAL 6 ACHIEVEMENT? .....	253



<b>A.M. ISKRYZHITSKYI, O.K. ISKRYZHITSKA, O.V. TRUNOVA, L.K. SVETENOK</b> DEVELOPING AND DEPLOYING OF CNTU COMMUNICATION SYSTEM CALLED “STU&TGRAM” .....	253
<b>N.D. PANKRATOVA, V.A. PANKRATOV</b> EVALUATION OF INFORMATION RELIABILITY SENSORS OF CYBER-PHYSICAL SYSTEM.....	256
<b>МАКСИМОВ А.Є., ТИМЧЕНКО А.А.</b> ЦИФРО-АНАЛІТИЧНА ТЕХНОЛОГІЯ СИСТЕМНИХ ДОСЛІДЖЕНЬ ПРОЦЕСІВ КЕРОВАНОГО РУХУ .....	260
<b>А.О. ЗАВОРОТНИЙ, В.В. НЕХАЙ</b> ПЛАГІН ВІДЕОПЛЕЄРА ДЛЯ ІНТЕРПОЛЯЦІЇ КАДРІВ .....	262
<b>КУЧЕРЯВЕНКО М.О., ГРЕБЕННИК А.Г.</b> ПРОГРАМНА РЕАЛІЗАЦІЯ ВІЗУАЛЬНОЇ МОДЕЛІ РУХУ НЕБЕСНИХ ТІЛ.....	267
<b>В.І. САЛАПАТОВ</b> ОПИС, МОДЕЛЮВАННЯ ТА РОЗРОБКА ПРОГРАМ .....	269
<b>В.А. УМАНСЬКИЙ</b> РОЗВ’ЯЗУВАННЯ ЗАДАЧІ ПІДТРИМКИ ПРАВЦІВНИКА МОБІЛЬНОЇ ГРУПИ З УРАХУВАННЯМ ЧАСОВИХ ВІКОН ....	272
<b>А.В. ФЕДУХИН</b> ЭФФЕКТ ДИХОТОМИИ В СТРУКТУРНОЙ НАДЕЖНОСТИ ДУБЛИРОВАННЫХ СИСТЕМ .....	275
<b>N.R. BALYK, I.M. GROD, S.V. MARTYNUK, Y.P. VASYLENKO, V.P. OLEKSIUK</b> WEB-SERVICE FOR NETWORK GRAPH BUILDING FOR WORKS PLANNING .....	277
<b>О.О. ДРУЖИНИН</b> ДЕТЕКТУВАННЯ ІНТЕРЕСІВ КОРИСТУВАЧІВ СОЦІАЛЬНИХ МЕРЕЖ .....	280

**Секція 4**  
**Сучасні аспекти математичного та імітаційного**  
**моделювання зразків техніки спеціального**  
**призначення**

<b>SAVKOV P.A., STORUBLOV O.I., SYNAVSKA I.K., ZATSERKOVNYI V.I., OLSHEVSKIY YU.V.</b> THE USE OF THE TILE STRUCTURE OF SPATIAL DATA IN NETWORK-CENTRIC ARMED FORCES MANAGEMENT SYSTEMS .....	286
<b>HEORHADZE O.A., KHARABARA V.I., VYNOKUROV D.V., HAKHOVICH S.V., SAVCHENKO T.V.</b> METHODICAL APPROACH TO EVALUATE THE YOUNGER SPECIALISTS COMPETENCE LEVEL IN THE SPECIALIZATION OF “TOPO-GEODESIC AND NAVIGATION SUPPORT OF TROOPS (FORCES)” IN THE TRAINING CENTER.....	291
<b>М.А. Закалад, М.Ю. Голобородько, В.Б. Полщук</b> АСПЕКТИ СТВОРЕННЯ АРХІТЕКТУРИ ІНФОРМАЦІЙНОЇ СИСТЕМИ ЛОГІСТИКИ ЗБРОЙНИХ СИЛ УКРАЇНИ.....	296
<b>М.А. Закалад, А.С. Мулявка, В.Б. Полщук</b> ПІДХОДИ ДО РОЗРОБКИ ІТ-АРХІТЕКТУРИ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ІТ-СТРАТЕГІЇ МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ .....	300
<b>В.Б. Полщук, І.С. Нетесін, В.Ф. Гречанинов, В.М. Закалад</b> ПІДХІД ДО ПОРЯДКУ ПРОЕКТУВАННЯ АРХІТЕКТУРИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЛОГІСТИЧНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ЗБРОЙНИХ СИЛ УКРАЇНИ.....	304

<b>Олійник Р.М., Цілина С.В., Єрмоленко О.В.</b> МЕТОДИКА ОЦІНЮВАННЯ ЖИВУЧОСТІ СИСТЕМИ УПРАВЛІННЯ ВОГНЕМ ЗЕНІТНОГО ПІДРОЗДІЛУ (ЧАСТИНИ) З ВИКОРИСТАННЯМ МОДЕЛЮВАННЯ .....	308
<b>Москалець С.В., Живець Ю.М., Шумигай О.В.</b> МОДЕЛЮВАННЯ РАДІОЛОКАЦІЙНИХ ХАРАКТЕРИСТИК РОЗСІЮВАННЯ АРТИЛЕРІЙСЬКИХ БОЄПРИПАСІВ .....	309
<b>С.П. Корнієнко, І.В. Корнієнко, В.А. Дмитрієв, А.Г. Павленко, Д.О. Камак</b> ДОСЛІДЖЕННЯ НЕРІВНОМІРНОСТІ ПОТОКУ ВИМОГ НА ВИПРОБУВАННЯ ОЗБРОЄННЯ І ВІЙСЬКОВОЇ ТЕХНІКИ .....	310
<b>О. VARABASH, V. TYURIN, P. OPEN'KO, N. DAKHNO, H. SHEVCHENKO, A. PAVLENKO</b> THE PROBLEM OF TRAJECTORY CONTROL WITH MINIMUM FUEL COST .....	314
<b>О.О. Акимов, В.Т. Бояров, М.М. Жданюк</b> ПРО ВИЗНАЧЕННЯ ПЛАВНОСТІ ХОДУ БРОНЕАВТОМОБІЛІВ.....	317
<b>П.Л. Аркушенко, В.В. Борщ, О.І. Вервейко, А.В. Коваленко</b> ДЕЯКІ ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ВІРТУАЛЬНИХ ВИМІРЮВАЛЬНИХ ПРИЛАДІВ ПРИ ВИПРОБУВАННЯХ ВІДБИТТЯ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ.....	321
<b>А.Г. Артикула, Д.М. Бритов, Д.М. Крючков, Р.В. Титаренко</b> ОБґРУНТУВАННЯ СТРУКТУРИ МЕТОДУ ПРОГНОЗУВАННЯ ТА ДІАГНОСТУВАННЯ ТЕХНІЧНОГО СТАНУ РАДІОТЕХНІЧНИХ ЗАСОБІВ .....	324

<b>О.І. ДЕНИСОВ, Ю.О. ДЕНИСОВ, О.О. БУРСАЛА</b> ПОХІБКА РЕГУЛЮВАННЯ ПРОЦЕСОМ СТАБІЛІЗАЦІЇ ФАЗИ РОБОЧОГО ОРГАНУ РОБОТОТЕХНІЧНОГО КОМПЛЕКСУ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ .....	328
<b>С.В. КУКОБКО, О.Г. ВЕТОШКІН,</b> <b>С.В. ГЕРАСИМОВ, О.В. ГРЕЧКА</b> МОДЕЛЮВАННЯ ВПЛИВУ НЕСТАБІЛЬНОСТІ ХАРАКТЕРИСТИК ЗАСОБІВ КОНТРОЛЮ НА ЕФЕКТИВНІСТЬ ФУНКЦІОНУВАННЯ РАДІОТЕХНІЧНИХ СИСТЕМ.....	331
<b>С.В. КУКОБКО, О.Г. ВЕТОШКІН,</b> <b>Є.С. РОЩУПКІН, В.В. ДЖУС</b> АВТОМАТИЗОВЕ ТЕХНІЧНЕ ОБСЛУГОВУВАННЯ РОЗНЕСЕНИХ ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ СИСТЕМ .....	335
<b>І.М. ЛАППО, О.В. ЧЕРВОТОКА, М.О. ГЕРАЩЕНКО</b> ВЗАЄМНИЙ ВПЛИВ ТЕПЛОВИХ ДЖЕРЕЛ НА ТЕМПЕРАТУРНИЙ СТАН ПІД ЧАС ОБРОБЛЕННЯ ОТВОРІВ КОМБІНОВАНИМ ІНСТРУМЕНТОМ .....	339
<b>О.О. САУТІН, С.В. РУДНІЧЕНКО,</b> <b>М.М. ГЕРАЩЕНКО, М.О. СОЛОДЧУК</b> БЕЗПЕКА ПУСКУ БЕЗПЛОТНОГО ЛІТАЛЬНОГО АПАРАТУ ПРИ ВИКОРИСТАННІ СТАРТОВОЇ ГУМОВОЇ КАТАПУЛЬТИ .....	343
<b>В.М. ЧУПРИНА</b> СУЧАСНІ МЕТОДИ МОДЕЛЮВАННЯ ПРИ ВИПРОБУВАННЯХ СПЕЦІАЛЬНОЇ АВТОМОБІЛЬНОЇ ТЕХНІКИ.....	344
<b>В.Г. ШАПОРЕНКО, В.А. ДМИТРІЄВ</b> МОДЕЛЮВАННЯ ПРОЦЕСУ ПОВІТРЯНОГО ДЕСАНТУВАННЯ З МЕТОЮ ОЦІНКИ ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ ПАРАШУТНИХ СИСТЕМ .....	347

## Секція 5

### Сучасні аспекти математичного та імітаційного моделювання систем в управленні проектами

<b>А.В. Казмірчук, М.О. Сперкач, О.Г. Жданова</b> МОДЕЛЮВАННЯ СТРАТЕГІЙ НАРАХУВАННЯ БОНУСІВ СПІВРОБІТНИКАМ КОМПАНІЇ.....	352
<b>О.В. Малишев</b> МОДЕЛЮВАННЯ ДІЯЛЬНОСТІ У ПРОЦЕСАХ УПРАВЛІННЯ ЖИТТЄВИМ ЦИКЛОМ СИСТЕМ (ЕСКІЗ ФОРМАЛЬНОГО ПІДХОДУ).....	356
<b>О.М. Кношова, L.O. NIKIFOROVA, A.A. SHYIAN</b> MODEL FOR CALCULATION OF MANAGEMENT EFFICIENCY FOR HIGH STAFF OFFICERS.....	360
<b>Ю.Ю. Мартинюк, М.О. Сперкач</b> ІНФОРМАЦІЙНА СИСТЕМА ПЛАНУВАННЯ РЕСУРСІВ ІТ- ПРОЕКТІВ .....	363
<b>Т.К. Єременко, Ю.Г. Пилипенко</b> ОСОБЛИВОСТІ МОДЕЛЮВАННЯ ПРОЦЕСІВ ВИПРОБУВАННЯ СИСТЕМ УПРАВЛІННЯ ДІЯЛЬНІСТЮ У ЦАРИНІ ВІЙСЬКОВОГО УПРАВЛІННЯ.....	367