



004.056  
Д 81



В. І. Дужий

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ  
ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ  
БЕЗПЕКИ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧИХ  
СИСТЕМ З АРХІТЕКТУРНО-  
ТЕХНОЛОГІЧНОЮ ДИВЕРСНІСТЮ

За редакцією В. С. Харченка

№ 3 (33), 2015

V. I. Duzhyi

INFORMATION TECHNOLOGY  
TO ENSURE FUNCTIONAL SAFETY  
OF INFORMATION AND CONTROL  
SYSTEMS WITH ARCHITECTURE  
AND TECHNOLOGY DIVERSITY

Edited by V. S. Kharchenko



**GREENCO**  
GREEN COMPUTING & COMMUNICATIONS



European Commission  
**TEMPUS**

Міністерство освіти і науки України  
Національний аерокосмічний університет  
ім. М. Є. Жуковського «ХАІ»

В. І. Дужий

**ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ  
ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ  
ІНФОРМАЦІЙНО-УПРАВЛЯЮЧИХ СИСТЕМ  
З АРХІТЕКТУРНО-ТЕХНОЛОГІЧНОЮ ДИВЕРСІСТІЮ**

За редакцією В. С. Харченка

V. I. Duzhyi

**INFORMATION TECHNOLOGIES TO ENSURE  
FUNCTIONAL SAFETY  
INFORMATION AND CONTROL SYSTEMS  
WITH ARCHITECTURE AND TECHNOLOGY  
OF DIVERSITY**

Edited by V. S. Kharchenko

Проект  
*TEMPUS-GREENCO 530270-TEMPUS-1-2012-1-UK-TEMPUS-  
JPCR*  
*Green Computing and Communication*

2015

УДК 004.056.5:681.518  
ББК 32.973-018.2+32.965  
Д81

The monograph is based on the PhD thesis and results of a dissertation research in area of green and safe computing and communication (specialty 05.13.06 - information technologies). Research was conducted at the National Aerospace University named after N. E. Zhukovsky «Kharkiv Aviation Institute», Department of Computer Systems and Networks. The book is dedicated to the development of information technology to ensure functional safety of information and control systems (IC&S), which is based on creating a new model and method of rational selection attributes of the architectural and technological diversity (ADT). It proposed the model architectural and technological diversity of multi-version IC&S using normalized metrics of the diversity on direct and indirect metrics. Also offered an information technology to ensure functional safety of multi-version ICS. Results of the research were implemented within the project TEMPUS-GREENCO Green Computing and Communication (530270-TEMPUS-1-2012-1-UK-TEMPUS-JPCR), Work Package WP4 Establishment of the PhD incubators.

This book is intended for MSc- and PhD-students, university lecturers, engineers and researchers in the area of energy saving and safe information and communication technologies and systems.

Ref. -153 items, figures - 30, tables - 16.

**Рецензенти:** **Краснобаєв Віктор Анатолійович**, завідувач кафедри комп'ютерної інженерії Полтавського національного технічного університету імені Юрія Кондратюка, доктор технічних наук, професор, заслужений винахідник України;  
**Мищенко Віктор Олегович**, професор кафедри моделювання систем і технологій Харківського національного університету імені В. Н. Каразіна, доктор технічних наук, доцент;  
**Сидоренко Микола Федорович**, головний інженер НТ СКБ «Полісвіт» (Харків, Україна), заслужений винахідник України, кандидат технічних наук, доцент.

**Дужий В. І.**

**Інформаційна технологія забезпечення функціональної безпеки інформаційно-управляючих систем з архітектурно-технологічною диверсністю: моногр.** / за ред. В. С. Харченка. – Міністерство освіти і науки України, Національний аерокосмічний університет ім. М. С. Жуковського «ХАІ», 2015. – 216 с.

ISBN 978-617-7361-16-8.

Монографія базується на результатах дисертаційного дослідження на здобуття наукового ступеня кандидата технічних наук (PhD) у галузі зеленого і безпечного комп'ютерного і комунікацій (спеціальність 05.13.06-інформаційні технології). Виконана в Національному аерокосмічному університеті ім. М. С. Жуковського «Харківський авіаційний інститут», кафедра комп'ютерних систем і мереж. Присвячена розробленню інформаційної технології забезпечення функціональної безпеки інформаційно-управляючих систем (ІУС), яка базується на створенні нової моделі та методу вибору раціональних варіантів використання архітектурно-технологічної диверсності (АТД). Пропонується модель АТД багатoversійних ІУС і удосконалений метод оцінювання диверсності ІУС шляхом використання нормованих метрик диверсності за прямими і непрямими ознаками, а також інформаційна технологія забезпечення функціональної безпеки багатoversійних ІУС. Результати впроваджені у проект TEMPUS-GREENCO Green Computing and Communication (530270-TEMPUS-1-2012-1-UK-TEMPUS-JPCR). Робочий пакет WP4 Створення і впровадження PhD-інкубаторів.

Для студентів, аспірантів та викладачів університетів, інженерів та дослідників у сфері енергоефективних і безпечних інформаційних і комунікаційних технологій та систем.

Бібл. - 153 найменувань, рисунків - 30, таблиць - 16.

Рекомендовано до видання Вченою радою Національного аерокосмічного університету ім. М. О. Жуковського «Харківський авіаційний інститут» (протокол № 1 від 23 вересня 2015 року).

УДК 004.056.5:681.518  
ББК 32.973-018.2+32.965

ISBN 978-617-7361-16-8

© Дужий В. І.

© Национальный аэрокосмический университет имени Н. Е. Жуковского «ХАИ», 2015

## TABLE OF CONTENTS

SUMMARY (Ukrainian).....	11
SUMMARY (English).....	14
LIST OF ABBREVIATIONS.....	16
INTRODUCTION.....	17
<b>PART 1 MODELS ANALYSIS AND METHODS ASSESSMENT OF MULTI-VERSION INFORMATION AND CONTROL SYSTEMS.....</b>	<b>24</b>
1. 1 Requirements analysis for the usage of the diversity principle in IC&S.....	24
1.1.1 Requirements analysis to safety systems.....	24
1.1.2 Analysis of the functional safety standards for IC&S.....	26
1.1.3 Analysis of the functional safety requirements for IC&S.....	28
1.1.4 Normative profile of functional safety.....	30
1.1.5 Analysis of the diversity principle usage.....	32
1.1.6 Analysis of problems usage diversity for IC&S.....	33
1.1.7 Analysis of regulations on the diversity usage.....	33
1.2 Analysis of classifications and models of multi-version systems.....	35
1.2.1 Analysis of multi-version systems classification.....	35
1.2.2 Analysis of multi-version systems models.....	38
1.3 Analysis of existing methods and techniques for diversity assessment.....	40
1.3.1 Basic principles of assessment multi-version systems.....	40
1.3.2 Assessment methods of multi-version systems.....	40
1.3.3 Metric-probabilistic assessment methods of multi-version systems.....	43
1.3.4 Assessment techniques of multi-version systems.....	44
1.4 Problem statement and rationale of research technique.....	45
1.4.1 Total and partial research problems.....	46
1.4.2 Research technique.....	47
1.5 Conclusions.....	49
<b>PART 2 MODEL OF ARCHITECTURE AND TECHNOLOGY DIVERSITY OF INFORMATION AND CONTROL SYSTEMS.....</b>	<b>51</b>

2.1 Set-theoretic description of the diversity attributes.....	51
2.1.1 Set-theoretic model of multi-version systems.....	51
2.1.2 Classification and rearranging the diversity attributes.....	56
2.1.3 Architecture and technology diversity of multi-version system model.....	60
2.1.4 Rearranging layers of the model of the architecture and technology diversity .....	68
2.2 Multilevel directed graph describing versions.....	73
2.2.1 Diversity model as a multilevel graph.....	73
2.2.2 Rearranging of the diversity sub-attributes of multilevel graph.....	75
2.2.3 Description version of multi-version system based on multilevel graph.....	78
2.2.4 Representation of multi-level graph.....	80
2.3 Procedure for developing set-theoretical models of the multi-version systems with architecture and technology diversity.....	82
2.4 Building a multilevel graph of describing versions.....	85
2.5 Conclusions.....	92
<b>PART 3 METHOD OF INFORMATION AND CONTROL SYSTEMS</b>	
<b>DIVERSITY ASSESSMENT.....</b>	<b>94</b>
3.1 Diversity metric assessment.....	94
3.2 Diversity assessment method by using normed indirect metrics of the diversity.....	100
3.2.1 Typical structures of multilevel directed graph.....	100
3.2.2 Assessment of normed indirect metrics for the technology diversity.....	103
3.2.3 Assessment of normed indirect metrics for the architecture diversity.....	109
3.3 Diversity assessment by using normed indirect metrics.....	111
3.4 Reliability assessment of multi-version systems with architecture and technology diversity.....	115
3.5 Generation the set of versions.....	119
3.5.1 Development of the algorithm generating a set of versions.....	119
3.5.2 Development of the algorithm generating a set of multi-version systems.....	124
3.5.3 Procedure for generating a set of multi-version systems.....	128

3.6 Assessment diversity method of information and control systems.....	129
3.7 Conclusions.....	133
PART 4 DEVELOPMENT AND PRACTICAL APPLICATION OF INFORMATION TECHNOLOGY OF INFORMATION AND CONTROL SYSTEMS FUNCTIONAL SAFETY ASSURANCE USING THE ARCHITECTURE AND TECHNOLOGY DIVERSITY.....	
135	135
4.1 Development of information technology to ensure functional safety of information and control systems.....	135
4.1.1 Development principles of multi-version IC&S with architecture and technology diversity.....	135
4.1.2 Tasks that solve when designing of multi-version systems.....	136
4.1.3 Choice of model and method for solving typical tasks.....	138
4.1.4 Development of the information technology.....	141
4.1.5 The usage procedure of the proposed procedures for solving typical tasks of ensuring functional safety IC&S.....	147
4.2 Development of selection procedure.....	152
4.3 Practical usage of information technology to ensure functional safety IC&S.....	154
4.4 Conclusions.....	157
RESEARCH CONCLUSIONS.....	159
REFERENCES.....	162
RELATED PUBLICATIONS.....	180
CHRONOLOGY OF DISSERTATIONS DEFENSE AT THE DEPARTMENT OF COMPUTER SYSTEMS AND NETWORKS.....	
205	205

## ЗМІСТ

АНОТАЦІЯ.....	11
SUMMARY.....	14
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	16
ВСТУП.....	17
РОЗДІЛ 1 АНАЛІЗ МОДЕЛЕЙ І МЕТОДІВ ОЦІНЮВАННЯ БАГАТОВЕРСІЙНИХ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧИХ СИСТЕМ.....	24
1.1 Аналіз вимог щодо використання принципу диверсності в ІУС.....	24
1.1.1 Аналіз вимог до систем, важливих для безпеки.....	24
1.1.2 Аналіз системи стандартів з функціональної безпеки ІУС.....	26
1.1.3 Аналіз вимог до функціональної безпеки ІУС.....	28
1.1.4 Нормативний профіль функціональної безпеки.....	30
1.1.5 Аналіз використання принципу диверсності.....	32
1.1.6 Аналіз проблем використання принципу диверсності в ІУС.....	33
1.1.7 Аналіз нормативних документів щодо використання диверсності.....	33
1.2 Аналіз класифікаційних схем і моделей подання багатOVERСІЙНИХ систем.....	35
1.2.1 Аналіз класифікаційних схем багатOVERСІЙНИХ систем.....	35
1.2.2 Аналіз моделей багатOVERСІЙНИХ систем.....	38
1.3 Аналіз існуючих методів і методик оцінювання диверсності.....	40
1.3.1 Базові принципи оцінювання багатOVERСІЙНИХ систем.....	40
1.3.2 Методи оцінювання багатOVERСІЙНИХ систем.....	40
1.3.3 Метрично-імовірнісні методи оцінювання багатOVERСІЙНИХ систем... ..	43
1.3.4 Методики оцінювання багатOVERСІЙНИХ систем.....	44
1.4 Постановка задачі й обґрунтування методики дослідження.....	45
1.4.1 Загальна та часткові задачі дослідження.....	46
1.4.2 Методика досліджень.....	47
1.5 Висновки до розділу.....	49
РОЗДІЛ 2 МОДЕЛЬ АРХІТЕКТУРНО-ТЕХНОЛОГІЧНОЇ ДИВЕРСНОСТІ БАГАТОВЕРСІЙНИХ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧИХ СИСТЕМ.....	51

2.1 Теоретико-множинний опис видів диверсності.....	51
2.1.1 Теоретико-множинна модель багатоверсійних систем.....	51
2.1.2 Класифікація та впорядкування видів диверсності.....	56
2.1.3 Архітектурно-технологічна диверсність моделі багатоверсійних систем.....	60
2.1.4 Впорядкування шарів моделі архітектурно-технологічної диверсності.....	68
2.2 Багаторівневий орієнтований граф опису версій.....	73
2.2.1 Модель диверсності у вигляді багаторівневого графа.....	73
2.2.2 Впорядкування підвидів диверсності багаторівневого графа.....	75
2.2.3 Опис версій багатоверсійної системи на основі багаторівневого графа, ..	78
2.2.4 Форми подання багаторівневого графа.....	80
2.3 Процедура розроблення теоретико-множинної моделі багатоверсійних систем із архітектурно-технологічною диверсністю.....	82
2.4 Формування багаторівневого графа опису версій.....	85
2.5 Висновки до розділу.....	92
РОЗДІЛ 3 МЕТОД ОЦІНЮВАННЯ ДИВЕРСНОСТІ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧИХ СИСТЕМ.....	94
3.1 Метричне оцінювання диверсності.....	94
3.2 Оцінювання диверсності шляхом використання нормованих метрик диверсності за непрямыми ознаками.....	100
3.2.1 Типові структури орієнтованого багаторівневого графа.....	100
3.2.2 Обчислення нормованих метрик технологічної диверсності за непрямыми ознаками.....	103
3.2.3 Обчислення нормованих метрик архітектурної диверсності за непрямыми ознаками.....	109
3.3 Оцінювання диверсності шляхом використання нормованих метрик диверсності за прямими ознаками.....	111
3.4 Оцінювання надійності багатоверсійних систем з архітектурно-технологічною диверсністю.....	115



3.5 Генерація множини версій.....	119
3.5.1 Розроблення алгоритму генерації множини версій.....	119
3.5.2 Розроблення алгоритму генерації множини багатoversійних систем ..	124
3.5.3 Процедура генерації множини багатoversійних систем.....	128
3.6 Метод оцінювання диверсності інформаційно-управляючих систем.....	129
3.7 Висновки до розділу.....	133
<b>РОЗДІЛ 4 РОЗРОБЛЕННЯ ТА ПРАКТИЧНЕ ЗАСТОСУВАННЯ</b>	
<b>ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ</b>	
<b>БЕЗПЕКИ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧИХ СИСТЕМ ІЗ</b>	
<b>ВИКОРИСТАННЯМ АРХІТЕКТУРНО-ТЕХНІЧНОЇ ДИВЕРСНОСТІ.....</b>	
	135
4.1 Розроблення інформаційної технології забезпечення функціональної безпеки інформаційно-управляючих систем.....	135
4.1.1 Принципи розроблення багатoversійних ІУС з архітектурно- технологічною диверсністю.....	135
4.1.2 Задачі, які вирішують при розробленні багатoversійних систем.....	136
4.1.3 Вибір моделі та методу вирішення типових задач.....	138
4.1.4 Розроблення інформаційної технології.....	141
4.1.5 Порядок використання запропонованих процедур для вирішення типових задач забезпечення функціональної безпеки ІУС.....	147
4.2 Розроблення процедури вибору.....	152
4.3 Практичне використання інформаційної технології забезпечення функціональної безпеки ІУС.....	154
4.4 Висновки до розділу.....	157
<b>ВИСНОВКИ.....</b>	159
<b>СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....</b>	162
<b>ОСНОВНІ ПУБЛІКАЦІЇ.....</b>	180
<b>ХРОНОЛОГІЯ ЗАХИСТУ ДИСЕРТАЦІЙНИХ РОБОТ НА КАФЕДРІ</b>	
<b>КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ.....</b>	208