METHODS AND TOOLS OF RISK ASSESSMENT AND MODELLING OF SMART ENERGY INFRASTRUCTURE (SEI)

- Application of risk assessment methods for SEI
- Simulation tools for modelling of SEI. GridLabD
- Research of SEI using Energy Storage, Voltage Control and Solar

FUZZY METHODS AND INFORMATION TECHNOLOGIES FOR SAFETY AND SEI RISK ANALYSIS

- Safety analysis of SEI using fuzzy methods
- Application of Fuzzy Logic Toolbox for SEI safety analysis

METHODS AND INFORMATION TECHNOLOGIES OF ASSESSMENT OF CYBER SECURE SEI

- Application of tools for assessment of cyber secure SEI. Netica

University of Ioannina

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

PhD

GREENCO
GREEN COMPUTING & COMMUNICATIONS

ИССЛЕДОВАНИЕ И РАЗРАБОТКА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ИНТЕЛЛЕКТУАЛЬНЫХ ЭНЕРГЕТИЧЕСКИХ ИНФРАСТРУКТУР

Практикум

RESEARCH AND DEVELOPMENT OF INFORMATION TECHNOLOGIES FOR SMART ENERGY INFRASTRUCTURES

2016

European Commission
TEMPUS

Министерство образования и науки Украины
Национальный аэрокосмический университет
им. Н.Е. Жуковского «ХАИ»

Е.В. Брежнев

Исследование и разработка информационных технологий для интеллектуальных энергетических инфраструктур

Практикум

Research and Development of ITs for Smart Energy Infrastructures

Под редакцией В.С. Харченко

Проект
Green Computing and Communication (reference number 530270-TEMPUS-1-2012-1-UK-TEMPUS-JPCR)

2016

УДК 004.9+004.052:621.38
ББК 96.260(0)к
Б63

Викладені матеріали практичної частини начального курсу “Дослідження та розробка інформаційних технологій для інтелектуальних енергетичних інфраструктур” (PhD6, Research and Development of ITs for Smart Energy Infrastructures), підготовленого в рамках проекту Green Computing and Communication (reference number 530270-TEMPUS-1-2012-1- UK-TEMPUS-JPCR).

Курс присвячений методології та практиці оцінювання ризиків та безпеки інтелектуальних енергетичних інфраструктур (смарт грид). Приводиться навчальна програма курсу, опис семінарів, практикумів, методичні рекомендації щодо самостійного вивчення курсу.

Для аспірантів університетів, що навчаються за напрямками комп’ютерних наук, комп’ютерної та програмної інженерії, при вивченні методів та засобів оцінювання ризиків, безпеки смарт грид, а також може бути корисна викладачам, що проводять заняття з відповідних курсів.

Рецензенты: **Мохор Владимир Владимирович**, директор Института проблем моделирования в энергетике им. Г.Е. Пухова Национальной Академии наук Украины, доктор технических наук, профессор;

Сиора Александр Андреевич, генеральный директор ПАО НПП «Радий» (Кировоград, Украина), кандидат технических наук.

Брежнев Е.В.

Исследование и разработка информационных технологий для интеллектуальных энергетических инфраструктур. Практикум / Под ред. Харченко В.С. – Министерство образования и науки Украины, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», 2016. – 130 с.

ISBN 978-966-662-717-5.

Изложены материалы практической части учебного курса «Исследование и разработка информационных технологий для интеллектуальных энергетических инфраструктур» (PhD6, Research and Development of ITs for Smart Energy Infrastructures), подготовленного для аспирантов в рамках проекта Green Computing and Communication (reference number 530270- TEMPUS-1-2012-1-UK-TEMPUS-JPCR). Курс посвящен методологии и практике оценивания рисков и безопасности интеллектуальных энергетических инфраструктур.

Приводится учебная программа курса, дается описание семинаров, практикумов и тренингов, методические рекомендации по самостоятельному изучению материала курса.

Для аспирантов университетов, обучающихся по направлениям компьютерных наук, компьютерной и программной инженерии, при изучении методов и средств оценивания рисков и безопасности смарт грид, а также может быть полезна для преподавателей, ведущих занятия по соответствующим курсам.

Библ. – 51 наименований, рисунков – 50, таблиц – 17.

Утверждено на заседании ученого совета Национального аэрокосмического университета имени Н.Е. Жуковского «ХАИ» (протокол № 1 от 2 сентября 2015 г).

УДК 004.9+004.052:621.38
ББК 96.260(0)к

ISBN 978-966-662-717-5

СПИСОК СОКРАЩЕНИЙ

АСУ – Автоматизированная система управления
ИБ – Информационная безопасность
ИЭИ – Интеллектуальные энергетические инфраструктуры
ИНС – Искусственные нейронные сети
ИТ – Информационные технологии
КЭИ – Критические энергетические инфраструктуры
ЛВС – Локальная вычислительная сеть
ЛПР – Лицо, принимающее решение
ЛЭП – Линии передачи электроэнергии
МИИ – Методы искусственного интеллекта
НСД – Несанкционированный доступ
ПЛК – Программируемый логический контроллер
СБ – Система безопасности
СНЭ – Система нормальной эксплуатации
СШ ГЭС – Саяно-Шушенская гидроэлектростанция
ЦПС – Цифровая подстанция

ALE – Annual Loss Expectancy
COBRA – Consultative Objective and Bi-Functional Risk Analysis
DOE – Department of Energy
LOCA – Loss of Coolant Accident
NPP – Nuclear Power Plan
PNNL – Pacific Northwest National Laboratory
ROI – Return on Investment
SMART – Self-Monitoring Analysis and Reporting Technology
SCADA – Supervisory Control and Data Acquisition Systems
SC – Soft-computing

ВВЕДЕНИЕ

В пособии изложены материалы практической части учебного курса «Исследование и разработка информационных технологий для интеллектуальных энергетических инфраструктур» (Research and Development of ITs for Smart Energy Infrastructures), подготовленного для аспирантов в рамках проекта Green Computing and Communication (reference number 530270-TEMPUS-1-2012-1-UK-TEMPUS-JPCR).

Курс посвящен методологии и практике оценивания, обеспечения безопасности интеллектуальных энергетических инфраструктур как нового поколения энергоэффективных и энергосберегающих систем, направленных на решение существующих экологических проблем.

В пособии приводятся описание семинаров, практикумов, в приложениях изложены учебная программа курса и методические рекомендации по самостоятельному изучению материалов курса.

В первом разделе приведены материалы семинара по обзору и применению методов анализа безопасности и рисков интеллектуальных энергетических инфраструктур (ИЭИ). Теоретический материал содержит краткое описание смарт грид, как пример реализации “зеленой” инфраструктуры, создание которой направлено на решение экологических проблем, снижение “нагрузки” на природную среду. Высокий уровень интеллектуализации инфраструктуры не снижает рисков, связанных с надежностью и безопасностью ее систем и компонентов. В разделе проведен обзор основных методов риск анализа ИЭИ, а также описание семинара по применению методов риск анализа ИЭИ.

Первый раздел содержит также описание практикума, направленного на изучение средств имитационного моделирования параметров ИЭИ с использованием веб утилиты GRID LAB. Знания, полученные после выполнения практикума, используются при выполнении трех лабораторных работ, описание которых приведено в первом разделе.

Во втором разделе представлен практикум по анализу безопасности систем в ИЭИ с использованием нечеткой логики. Практикум основан на применении Fuzzy Logic Toolbox,

позволяющего провести оценку безопасности с использованием экспертных данных. Изложены основные положения анализа безопасности с использованием нечетких подходов, показаны их преимущества и недостатки. Изложена методика применения нечеткой логики при решении задачи оценивания безопасности.

Третий раздел содержит практикум по анализу рисков информационной безопасности ИУС в рамках ИЭИ. Приведен обзор методов анализа ИБ ИУС в ИЭИ. Практикум основан на использовании метода анализа рисков ИБ, основное содержание которого приведено в данном разделе. Метод основан на построении графа, связывающего важные кибер активы ИУС. Метод позволяет оценить связи между состояниями ИБ всех активов ИУС и определить их изменение при возникновении рисков и угроз каждому активу. Практикум предусматривает построение графа для анализа ИБ систем, предложенных для анализа каждому студенту. Рисунки, таблицы и формулы для удобства нумеруются в пределах каждого раздела.

Книга предназначена для магистрантов и аспирантов университетов, обучающихся по компьютерным наукам, компьютерной и программной инженерии при изучении методов оценивания и обеспечения энергоэффективности и безопасности ИЭИ, их кибербезопасности. Может быть полезна также для преподавателей соответствующим курсов.

Пособие подготовлено доцентом кафедры компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ» к.т.н., с.н.с. Брежневым Е.В. Общее редактирование проведено заведующим этой кафедры д.т.н., проф. Харченко В.С. Программа курса разработана совместно Брежневым Е.В. и Харченко В.С.

Автор выражает благодарность рецензентам, студентам кафедры компьютерных сетей и систем, студентам Брошеван Е.В., Карпенко А.С., Криворучко Н.В. за помощь и конструктивные предложения, которые высказывались в процессе обсуждения практической части данного курса.

АНОТАЦІЯ

УДК 004.9+004.052:621.38
Б63

Брежнєв Є.В. **Дослідження та розробка інформаційних технологій для інтелектуальних енергетичних інфраструктур /** За ред. Харченка В.С. – Міністерство освіти і науки України, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», 2016. – 130 с.

ISBN 978-966-662-717-5

Викладені матеріали практичної частини начального курсу “Дослідження та розробка інформаційних технологій щодо інтелектуальних енергетичних інфраструктур” (Research and Development of ITs for Smart Energy Infrastructures), підготовленого в рамках проекту Green Computing and Communication (reference number 530270-TEMPUS-1-2012-1-UK-TEMPUS-JPCR).

Курс присвячений методології та практиці оцінювання ризиків та безпеки інтелектуальних енергетичних інфраструктур (смарт грид). Приводиться навчальна програма курсу, опис семінарів, практикумів, методичні рекомендації щодо самостійного вивчення курсу.

Книга призначена для магістрів, аспірантів університетів, що навчаються за напрямками комп’ютерних наук, комп’ютерної та програмної інженерії, при вивченні методів та засобів оцінювання ризиків, безпеки смарт грид, а також може бути корисна викладачам, що проводять заняття з відповідних курсів.

Бібл. – 51 найменувань, рисунків – 50, таблиць – 17.

ЗМІСТ

ABSTRACT

UDC 004.9+004.052:621.38
Б63

Brezhnev E. V. Research and Development of Information Technologies for Smart Energy Infrastructure. Practicum / Edited by Kharchenko V. S. – Kharkiv: National Aerospace University named after N. E. Zhukovsky "KhAI", 2016. – 130 p.

ISBN 978-966-662-717-5

Practical materials of study course "Research and Development of Information Technologies for Smart Energy Infrastructure" given in this book are developed within project Green Computing and Communication (reference number 530270-TEMPUS-1-2012-1-UK-TEMPUS-JPCR).

The course is devoted to the methodology and practice of risk assessment and safety assurance of critical energy infrastructures (smart grid). In terms of methodology the following were given: syllabus, description of seminars, practical works and recommendations for independent learning of course.

The book is supposed to be used by PhD students of universities that study computer science, computer and program engineering when studying methods and tools for safety, risk assessment and assurance of smart grid. It could be very useful for lecturers and professors who conduct classes on corresponding courses.

Ref. – 51 items, tables-17, figures – 50

CONTENT

ПРИЛОЖЕНИЕ. УЧЕБНАЯ ПРОГРАММА

DESCRIPTION OF THE COURSE

TITLE OF THE COURSE	Code
PhD6. Research and Development of ITs for Smart Energy Infrastructures	

Teacher(s)	Department
Coordinating: Dr. Brezhnev Eugene	Computer Systems and Networks

Study cycle	Level of the module	Type of the module
PhD	A	Full-time tuition

Form of delivery	Duration	Language(s)
Full-time tuition	One semester	English

Prerequisites	
Prerequisites: – Computer Systems and System Analysis; – Probability Theory and Foundations of Mathematical Statistics; – Reliability Theory Foundations; – Mobile application Foundations; – Modelling Foundation knowledge and skills.	**Co-requisites (if necessary):**

Credits of the module	Total student workload	Contact hours	Individual work hours
3	90	46	44

Aim of the module (course unit): competences foreseen by the study programme		
The aim of course is to create a knowledge acquisition about information technologies (IT) of smart energy infrastructures (SEI) safety and security analysis and modelling. Acquisition of knowledge, engineering methodology on SEI analysis and skills for application and development ITs of SEI safety&security by use of modern methods and techniques.		
Learning outcomes of module (course unit)	**Teaching/learning methods**	**Assessment methods**
At the end of course, the successful student will be able to: 1. Analyze and evaluate the main features and underlying IT of SEI. Synthesize information	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Module Evaluation Questionnaire
2. Assimilate, evaluate and analyze information related to risk, safety and security analysis of SEI	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Module Evaluation Questionnaire
3. Use methods for safety and security analysis for solving the practical tasks	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Module Evaluation Questionnaire
4. Use the simulation tools for SEI behavior analysis	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Module Evaluation Questionnaire
5. Use the tools for network and systems security analysis	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Module Evaluation Questionnaire

6. Analyze the modern IT systems and networks in respect to their cyber vulnerabilities	Interactive lectures, Learning in laboratories, Just-in-Time Teaching	Module Evaluation Questionnaire

Themes	**Contact work hours**							**Time and tasks for individual work**	
	Lectures	Consultations	Seminars	Practical work	Laboratory work	Placements	Total contact work	Individual work	**Tasks**
Module 1 Methods of Risk Assessment and Simulation of Smart Energy Infrastructures (SEI)									
1. Introduction in smart energy infrastructure as a new green energy infrastructure 1.1 General characteristics of course and specialty. Basic conceptions and definitions of smart energy infrastructure 1.2 Smart energy infrastructure challenges (Wide-area disruptive events, including natural events, cascading accidents, and co-ordinated cyber and physical attacks).	2						**2**	4	1.4 Key Information and Communication technologies overview (data communications, including Mobile applications, Control automation technologies, etc.) 1.5 Smart grid regulatory domain

1.3 Smart grid vulnerabilities. Interdependencies analysis of the SEI and critical infrastructures.									
2. S**mart energy infrastructure modeling approaches** 2.1 Classification of existing methods for SEI simulation (economic theory based approaches, network based approaches, and others) 2.2 Real-Time SEI Simulation 2.3 Models Shortage, areas of application	2						**2**	4	2.4. Comparison of empirical approaches, agent based approaches
3. **Smart energy infrastructure risk assessment and analysis** 3.1. SEI risk analysis framework 3.2 SEI risk analysis methods and tools. Advantages and shortages 3.3. SEI simulations tools	2		4		12		18		
In total per module	6		4		12		22	8	

Module 2 Fuzzy Methods and Information Technologies for Safety-Oriented Analysis of Smart Energy Infrastructures									
1 Overview of SEI fuzzy safety analysis methods 1.1Foundation of fuzzy sets for engineering 1.2 Analysis and classification of existing fuzzy methods and approaches for safety assessment 1.3 Methods Limitations, peculiarities of application	2							6	1.4 Soft computing for SEI analysis. Computing with words
2. Fuzzy probabilistic safety assessment of SEI 2.1 Introduction to Fuzzy probability. 2.2 Operation with fuzzy probabilities 2.3 Application of fuzzy probabilities for SEI safety assessment: Case –study	2							6	2.4 Application of fuzzy probabilities for SEI decision making
3. **Overview of SEI tools for fuzzy safety analysis.** 3.1 Classification of existing tools for fuzzy safety assessment 3.2 Fuzzy Systems Software: Taxonomy, Current Research Trends and Prospects	2			6				6	3.4 Software for Soft Computing

3.3 Case study: application of fuzzy tools for SEI accident analysis									
In total per module	6			6			**12**	18	
Module 3 Methods and Information Technologies for Security-oriented analysis of Smart Energy Infrastructures									
1. **Security challenges in SEI** 1.1 Potential cyber security threats for SEI 1.2 SEI vulnerabilities classification 1.3 Attack prevention and defense	2							6	1.4 SEI protocol and architecture overview
2. Methods of SEI security analysis 2.1 Methods classification 2.2 Overview of qualitative methods for SEI security analysis 2.3 Overview of quantitative methods for SEI security analysis	2							6	2.4 Comparative analysis of SEI security analysis methods
3. Tools for SEI security analysis 3.1 Existing tools classification 3.2 Tools shortage and limitations 3.3 Tool-based Case study development approach	2			6				6	3.4 SEI safety and security co –analysis: possible methods and approaches
In total	6			6			12	18	
Total/per course	**18**		**4**	**12**	**12**		**46**	**44**	

Assessment strategy	Weight in %	Dead lines	Assessment criteria
Lecture activity, including fulfilling special self-tasks	10	7,14	**85% – 100%** Outstanding work, showing a full grasp of all the questions answered. **70% – 84%** Perfect or near perfect answers to a high proportion of the questions answered. There should be a thorough understanding and appreciation of the material. **60% – 69%** A very good knowledge of much of the important material, possibly excellent in places, but with a limited account of some significant topics. **50% – 59%** There should be a good grasp of several important topics, but with only a limited understanding or ability in places. There may be significant omissions. **45% – 49%** Students will show some relevant knowledge of some of the issues involved, but with a good grasp of only a minority of the material. Some topics may be answered well, but others will be either omitted or incorrect. **40% – 44%** There should be some work of some merit. There may be a few topics answered partly or there may be scattered or perfunctory knowledge across a larger range.

			20% – 39% There should be substantial deficiencies, or no answers, across large parts of the topics set, but with a little relevant and correct material in places. **0% – 19%** Very little or nothing that is correct and relevant.
Learning in laboratories	30	7,14	**85% – 100%** An outstanding piece of work, superbly organized and presented, excellent achievement of the objectives, evidence of original thought. **70% – 84%** Students will show a thorough understanding and appreciation of the material, producing work without significant error or omission. Objectives achieved well. Excellent organization and presentation. **60% – 69%** Students will show a clear understanding of the issues involved and the work should be well written and well organised. Good work towards the objectives. The exercise should show evidence that the student has thought about the topic and has not simply reproduced standard solutions or arguments. **50% – 59%** The work should show evidence that the student has a reasonable understanding of the basic material. There may be some signs of weakness, but overall the grasp of the topic should be sound. The presentation and organization should

			be reasonably clear, and the objectives should at least be partially achieved. **45% – 49%** Students will show some appreciation of the issues involved. The exercise will indicate a basic understanding of the topic, but will not have gone beyond this, and there may well be signs of confusion about more complex material. There should be fair work towards the laboratory work objectives. **40% – 44%** There should be some work towards the laboratory work objectives, but significant issues are likely to be neglected, and there will be little or no appreciation of the complexity of the problem. **20% – 39%** The work may contain some correct and relevant material, but most issues are neglected or are covered incorrectly. There should be some signs of appreciation of the laboratory work requirements. **0% – 19%** Very little or nothing that is correct and relevant and no real appreciation of the laboratory work requirements.
Module Evaluation Quest	60	8,16	The score corresponds to the percentage of correct answers to the test questions

Author	Year of issue	Title	No of periodical or volume	Place of printing. Printing house or internet link
Compulsory literature				
Ed. by V. Kharchenko	2014	Green IT-Engineering. Volume 1. Principles, models, HW&SW		National Aerospace University "KhAI"
E. Brezhnev	2012	An approach for assessing of Common Cause Failures in Critical Infrastructure	Volume 28, number 1	Information&Security. An International Journal. Critical infrastructure safety and security
V. Kharchenko, E. Brezhnev	2012	Formalizing Power Grid Influence to Assess the Safety of Nuclear Power Plants	An International Journal 28, no. 1	Information & Security
V. Kharchenko, E. Brezhnev	2013	Power Grid Safety Assessmen Based on Linguistic Casual Network Under Uncertanties		Proceedings of The Third International Conference on Performance, Safety and Robustness in Complex Systems and Applications
E. Brezhnev	2014	Probabilistic network –based approach to infrastructure safety assessment with human factor consideration	Accession Number: 14502144	Digital Technologies (DT), 10th International conference, INSPEC

V. Kharchenko, E. Brezhnev	2013	Critical infrastructures safety assessment combining fuzzy models and BBN under uncertainties		New results in Dependability & Computing Syst Springer International Publishing, Switzerland,2013, pp.245-254
V. Kharchenko, E. Brezhnev	2012	BBN-based approach for assessment smart grid and NPP interaction		IEEE East west design & test symposium
V. Kharchenko, E. Brezhnev	2012	Grid safety analysis based on linguistic BBN		Dependable systems, services and technologies (Dessert, 2012)
V. Kharchenko, E. Brezhnev	2012	Grid safety analysis based on linguistic Bayesian networks	№ 7(59)	Радіоелектронні і комп'ютерні системи
V. Kharchenko, E. Brezhnev	2012	BBN-based Approach For Assessment of Smart Grid And Nuclear Power Plant Interaction		IEEE EAST-WEST DESIGN & TEST SYMPOSIUM
Brezhnev E	2013	Multi-factor analysis of critical infrastructure safety: BBN-based approach		Proceeding of the 3rd International Workshop "Critical Infrastructure Safety & Security"
V. Kharchenko, E. Brezhnev.	2013	The approach for cyber common cause failures		Proceeding of the 22nd SRA-E Conference (Safe

		risk assessment of smart grid substation with a critical load		societies 2. Coping with complexity and major risk
V. Kharchenko, E. Brezhnev	2015	Smart Grid Substation Availability Assessment: Recovered MSS-Based Approach		ESREL 2015 25th European Safety and Reliability Conference / Proceeding of the 25th European Safety and Reliability Conference
V. Kharchenko, E. Brezhnev	2015	Cyber diversity for digital substations under uncertainties: assurance and assessment/		Proceedings of CSCC / INASE, Zakynthos Island /Recent Advances in Computer Science, ISBN: 978-1-61804-320-7
Additional literature				
Jönsson H.	2007	Risk and Vulnerability Analysis of Complex Systems. A basis for proactive emergency management,		Department of Safety Engineering and System Safety Faculty of Engineering
F. Di Giandomenic	2008	Architecting Dependable Systems	Vol. 5135, 5	Lecture Notes in Computer Science
F. Di Giandomenic	2004	Dependability Modeling & Evaluation of Multiple-Phased Systems using DEEM in	Vol. 53, N. 4	IEEE Transactions on Reliability,
Vidmar P.	2005	Deterministic approach in	№ 23(2)	Risk analysis.

		tunnel safety assessment		
F. Di Giandomenic	2005	A Modeling Methodology for Hierarchical control Systems and its Application	Vol. 10, N. 3	Journal of the Brazilian Computer Society, special Issue on Dependable Computing
L. Nordstrom	2008	Assessment of Information Security Levels in Power Communication Systems Using Evidential Reasoning	Issue 3	IEEE Transactions on Power Delivery
Zadeh L.	1965	Fuzzy sets	Vol. 8.	Inf. Control.
Setola, R., De Porcellinis, S. & Sforna, M.	2009	Critical infrastructure dependency assessment using the input-output inoperability model.	V. 2	International Journal of Critical Infrastructure Protection
Svendsen, N.K. & Wolthusen, S.D.	2007	Connectivity models of interdependency in mixed-type critical infrastructure networks.	# 12	Information Security Technical Report
Bensi, M.T., Der Kiureghian, A. & Straub, D	2009	A Bayesian Network Framework for Post-earthquake Infrastructure System		Proceedings of Winter Simulation Conference

		Performance Assessment.		

СОДЕРЖАНИЕ

Брежнєв Євген Віталійович

ДОСЛІДЖЕННЯ ТА РОЗРОБКА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ІНТЕЛЕКТУАЛЬНИХ ЕНЕРГЕТИЧНИХ ІНФРАСТРУКТУР

Практикум
(російською мовою)

Редактори: Харченко В.С

Комп'ютерна верстка
Харченко Л.Д.

Зв. план, 2012
Підписаний до друку 09.02.2016
Формат 60x84 1/16. Папір офс. №2. Офс. друк.
Умов. друк. арк. 7,6. Уч.-вид. л. 8,2. Наклад 200 прим.
Замовлення 4 . Ціна вільна

Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»
61070, Харків-70, вул. Чкалова, 17 http://www.khai.edu

Видавець: ФОП Голембовська О.О.
03049, Київ, Повітрофлотський пр-кт, б. 3, к. 32.
Свідоцтво про внесення суб'єкта видавничої справи в державний реєстр видавців, виготовлювачів і розповсюджувачів видавничої продукції
ДК №5120 від 08.06.2016.

Віддруковано ТОВ "Юстон ЛТД"
01034, м.Київ, вул. О.Гончара, 36-а Тел. +38 044 360-2266,
www.yuston.com.ua