Ruslan HRYSHCHUK, Serhii YEVSEIEV, Alexander SHMATKO

CONSTRUCTION METHODOLOGY OF INFORMATION SECURITY SYSTEM OF BANKING INFORMATION IN AUTOMATED BANKING SYSTEMS

PREMIER
Publishing

Ruslan HRYSHCHUK, LtC, SRes, Dsc.

Date and place of birth: 1981, Pischantsya, Ovruch district, Zhytomyr region, Ukraine.
Education: S.P. Korolov Zhytomyr Military Institute, 2003.
Ivan Chernyakhovsky National Defense University of Ukraine, at the present time.
Affiliation and functions: Head of the Research Department of the Information & Cyber Security of Zhytomyr Military institute Research Centre since 2015.
Research interests: Information & Cyber Security of the state. Publications: over 254 scientific publications including monographs, textbooks, papers & patents.
ORCID: https://orcid.org/0000-0001-9985-8477
Scopus ID: 57192962495
Researcher ID: H-5679-2018
Google Scholar: https://scholar.google.com.ua/citations?user=A9xz0uP0SJ0C&hl=uk
E-mail: Dr.Hry@i.ua

Sergii YEVSEIEV , LtC, SRes, Dsc.

Date and place of birth: 1969, Hartsizk, Donetsk region, Ukraine.
Education: Kharkov Military University, 2002.
Affiliation and functions: Associate Processor of Information Systems since 2007.
Research Interests: Information & Cybersecurity of the banking systems. Publications: over 190 scientific publications including monographs, textbooks, papers & patents.
ORCID: https://orcid.org/0000-0003-1647-6444
AJ&view_op=list_works&sortby=pubdateScopus ID: 57190440690
Researcher ID: H-4734-2018
Google Scholar:
https://scholar.google.com./citations?hl=ru&user=Y4kNr38AAA
E-mail: saerhii.yevsiev@hneu.net

Alexander SHMATKO , Ass. Prof., PhD.

Date and place of birth: 1973, Odessa, Odessa region, Ukraine.
Education: Kharkov Aviation University, 1997.
Affiliation and functions: Associate Professor of Software Engineering, and Management Information Technologies Department, since 2007.
Research Interests: Information & Cybersecurity, critical computing, project management.
Publications: over 90 scientific publications including monoqraphs, textbooks, papers & patents.
ORCID: https://orcid.org/0000-0002-2426-900X
Researcher ID: M-7566-2017
Scopus Author ID: 6602623478
Google Scholar:
https://scholar.google.com.ua/citations?user=Wyv6ESUAAAAJ&hl=Ru
E-mail: asu.spios@gmail.com

ISBN 978-3-903197-50-3

Ruslan HRYSHCHUK, Serhii YEVSEIEV, Alexander SHMATKO

CONSTRUCTION METHODOLOGY OF INFORMATION SECURITY SYSTEM OF BANKING INFORMATION IN AUTOMATED BANKING SYSTEMS

Monograph

PREMIER Publishing

Premier Publishing s.r.o.

Vienna 2018

Hryshchuk R., Yevsciev, S. Shmatko A.

Construction methodology of information security system of banking information in automated banking systems : monograph – Vienna.: Premier Publishing s.r.o., 2018. – 284 p.

ISBN 978-3-903197-50-3

The monograph presents modern methodology of building information security systems of banking information systems. The methodology is based on a new concept of building a threat model, constructed on synergistic principles. As a result, for the first time a three-tier security model of strategic management of banking information technologies has being built for the automated banking system. This system takes into account threats of cybersecurity, information security and threats for the security of banking information at the same time.

Special attention should be given to the methods proposed in the monograph to ensure the confidentiality, integrity and authenticity of information in banking information systems. In contrast to the known ones, the proposed methods are built on hybrid cryptographic structures with redundant codes. Principles of the methods are mathematical models of hybrid cryptocodic constructions with using asymmetric crypto-modified McEliece and Niederreiter codes and modified geometric codes.

The book is full of applied examples that confirm the validity of the developed methods and the adequacy of the proposed models.

In this way a comprehensive solution has been proposed from a systemic position on the base of a synergistic approach, to ensure the information security of banking information systems. The proposed methodology opens up the new methods to building security systems for the critical information infrastructures of the state and business which is new in terms of security and a rational in terms of money spent

The results are proposed to be used at planning measures to ensure the information security of automated banking systems for minimization of risks from new threats to the security of banking information.

The monograph will be useful for researchers and applicants for scientific degrees, and can also be used by students during training to raise awareness of information and cybersecurity issues of modern information technologies.

Subscribe to print 28/11/2018. Format 60x90 1/16.
Offset Paper. Garinitura Amo. Conv. Pec. liter. 11. Edition of 500 copies.
Typeset in Berling by Ziegler Buchdruckerei, Linz, Austria.

Printed by Premier Publishing s.r.o. Vienna,
Vienna, Austria on acid-free paper.
Am Gestade 1,1010 Vienna, Austria
pub@ppublishing.org, ppublishing.org

ISBN 978-3-903197-50-3

Contents

List of Conditions..... **7**

INTRODUCTION..... **9**

CHAPTER 1. State of the art analysis..... **11**

1.1 Review of the literature on problem..... 11

1.1.1 Analysis of the nature and content of information security problems in the current development of science and technology..... *11*

1.1.2 Investigation of the role and place of information security system of banking information in automated banking systems..... *23*

1.1.3 Research infrastructure facilities threats automated banking systems..... *28*

1.1.4 Analysis of current state services and mechanisms for cryptographic protection of banking information..... *39*

1.2 Substantiation of the dissertation..... 46

1.3 Formulation of the problem..... 49

1.4 Conclusions of the first chapter..... 50

References in Chapter 1..... 51

CHAPTER 2. Development conceptual foundations of information security of banking information in the automated banking system..... **57**

2.1 Developing the concept of building a synergetic model of banking information security threats in automated banking systems..... 57

2.2 The formalization of the principles of construction components threats branch banking information security, information security, cyber security, information security..... 65

2.3 The formalization of the problem of evaluation generalized index of banking information security in automated banking systems..... 70

2.3.1 Improving the infrastructure of automated banking system..... *70*

2.3.2 Development of a conceptual model of synergistic threats to information security of banking information in automated banking systems....78
2.3.3 Improving the offending model based on a synergistic approach to the assessment of threats to information security, cyber security, and information security....81
2.3.4 Improving evaluation model of banking security in automated banking systems....87
2.4 Conclusions of the second section....90
References in Chapter 2....91

CHAPTER 3. Development approaches to security banking services in automated banking system on hybrid crypto-code designs from unprofitable codes.... 98

3.1 Setting properties crypto-code systems geometrical codes....98
3.1.1 Setting properties asymmetric crypto code of McEliece and Niederreiter Elliptic codes....105
3.1.2 Development of a method of masking elliptical codes.... 110
3.1.3 Develop methods modified elliptical codes....112
3.1.4 Research on properties of modified elliptical cryptographic codes....129
3.2 Develop methods to ensure the integrity and confidentiality of banking information in automated banking systems on hybrid designs crypto code of unprofitable codes.... 136
3.2.1 Research on the cryptographic properties of building codes unprofitable....136
3.2.2 The development of mathematical models of hybrid crypto-code constructions based on asymmetric crypto-modified code of McEliece and Niederreiter on modified geometrical codes.... 147
3.2.3 Studying the properties of hybrid crypto-code designs on unprofitable codes....160
3.3 Develop methods to ensure the authenticity of the bank in automated banking systems based on two-factor authentication hybrid crypto code structures with unprofitable codes....168
3.3.1 Research protocols two-factor authentication.... 168
3.3.2 Analysis of the threats that are relevant for todays two factor authentication protocols....172

3.3.3 Use two-factor authentication based on PassWindow and analysis of safety....176
3.3.4 Research methods for constructing OTP-password.... 180
3.3.5 Development of two factor authentication protocol on hybrid designs crypto code of unprofitable codes....184
3.3.6 Studying the properties of the proposed method of two-factor authentication....188
3.4 Conclusions of the third section.... 189
References in Chapter 3.... 190

CHAPTER 4. Development effectiveness evaluation approach to investment banking in information security in automated banking system 196

4.1 Development of evaluation method investment information security of banking information in terms of simultaneous action of threats to information security, cyber security and banking information.... 196
4.1.1 Development of composite indicator of investment in the system of banking information security in automated banking systems.... *196*
4.1.2 The development of methods of cryptosystems stability evaluation based on entropy method for assessing the randomness of the original sequence.... *206*
4.2 Develop comprehensive measure of service quality evaluation objects automated banking system to ensure the safety of bank information.... 212
4.3 The findings of the fourth section.... 224
References in Chapter 4.... 225

CHAPTER 5. Verification and investigation of developed models and methods. Construction methodology of information security system of banking information in the automated banking system....231

5.1 Comparative analysis of the transfer banking information efficiency in automated banking systems developed through comprehensive measure of evaluating the quality of service objects automated banking system to ensure the safety of bank information....231

5.2 Generalization of the results: the methodology of synthesis and analysis of the proposed models and methods of information security of banking information..... 235
5.3 Experiment..... 252
5.4 Conclusions of the fifth section..... 275
References in Chapter 5..... 277
CONCLUSIONS..... 282