

Edited by Serhii Yevseiev, Volodymir Ponomarenko,
Oleksandr Laptiev, Oleksandr Milov

SYNERGY

OF BUILDING CYBERSECURITY SYSTEMS



UDC 004.056
S98

Published in 2021
by PC TECHNOLOGY CENTER
Shatylova dacha str., 4, Kharkiv, Ukraine, 61165

Approved by the Academic Council of Simon Kuznets Kharkiv National University of Economics,
Protocol No. 3 of 15.03.2021

Reviewers:

Nataliia Lukova-Chuiko, Doctor of Technical Science, Head of the Department of Cybersecurity and Information Protection of Taras Shevchenko National University of Kyiv;

Korchenko Alexandr, Doctor of Technical Sciences, Professor, Head of the Department of Information Technology Security of National Aviation University.

S98

Authors:

Edited by **Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov**

Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.

ISBN 978-617-7319-31-2 (on-line)

ISBN 978-617-7319-32-9 (print)

The monograph discusses the main types of models used in modeling the behavior of intelligent agents. The originality of the approach associated with the introduction into consideration of the concept of the contour of business processes as an integral object to be protected. The idea of the spatio-temporal structure of the model basis was proposed by the authors, that reflects not only the distribution of the set of models over the corresponding levels of the proposed methodology, but also sets the sequence of their interaction. The application of the developed models to ensure the protection of information and user data in social networks will allow a new look at existing social networks and create new social networks that will provide more reliable security of user data while maintaining usage parameters. The monograph is intended for teachers, researchers and engineers involved in information security research.

Figures 65, Tables 26, References 155 items.

All rights reserved. No part of this book may be reprinted or reproduced or utilised in any form or by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying and recording, or in any information storage or retrieval system, without permission in writing from the authors.

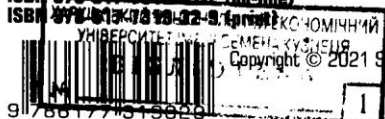
This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

DDI: 10.15587/978-617-7319-31-2

ISBN 978-617-7319-31-2 (on-line)



9 786177 731932

This is an open access article under the
Creative Commons CC BY license

784855



CONTENTS

List of Tables	viii
List of Figures	ix
Circle of Readers and Scope of Application	xii
1 Introduction	1
2 Methodology for Cooperative Conflict Interaction Modeling of Security System Agents	2
2.1 The traditional approach to modeling the behavior of agents in security systems	3
2.2 Agent-based models of the parties to the cyber conflict. The main directions of the classification of methods of agent-based modeling	7
2.3 Game-theoretic models of conflict situations	13
2.4 System-dynamic models of conflict-cooperative interaction of agents	24
2.5 Methodological foundations for the development of a cyber threat classifier	33
2.6 Development of the spatio-temporal structure of the model basis for the conflict-cooperative interaction of security agents	49
3 Mathematical models of information protection in social networks, taking into account the specifics of their parameters	64
3.1 Specific parameters of social networks and their impact on the security of user information	65
3.2 Model for determining the security of information under the trust between users and the amount of information in the network	75
3.3 Model of information defense in correspondence with the path of information transfer	79
3.4 Method of calculating the security of information for the network elements clustering	85
3.5 Impact of the noise and the interference in the protection of information on social networks	92
3.6 Assessing the level of economic costs for the protection of information in the social network	98
4 Methodological aspects of postquantum asymmetric McEliece and Niederreiter systems on algebra-geometric codes design	102
4.1 Research of requirements for post-quantum cryptography algorithms	103
4.2 Properties of asymmetric crypto-code systems McEliece and Niederreiter based on elliptical codes	105

CONTENTS

4.3 Sidelnikov's attack on the crypto-code constructions of McEliece and Niederreiter ..	111
4.4 Asymmetric crypto-code constructions of McEliece and Niederreiter based on modified elliptical codes.....	112
4.5 Hybrid asymmetric crypto-code constructions of McEliece and Niederreiter based on defective codes.....	130
4.6 Construction of methods of strict authentication on the basis of crypto-code constructions of McEliece and Niederreiter	141
4.7 The use of asymmetric crypto-code structures in the Security Concept of an innovative active university.....	147
Conclusions	164
References	165