Contents

Preface xi
Alexei A. GAIVORONSKI, Pavel S. KNOPOV,
Vladimir I. NORKIN and Volodymyr A. ZASLAVSKYI

Part 1. Mathematical Models and Methods for Risk Mitigation and Defending Critical Infrastructure 1

Introduction to Part 1 3
Pavel S. KNOPOV and Vladimir I. NORKIN

Chapter 1. Three Approaches to Decision-making Under Risk and Uncertainty for the Critical Infrastructure Protection 5
Vladimir S. KIRILYUK

1.1. Introduction 5
1.2. Decision-making in stochastic conditions of risk and uncertainty 7
1.2.1. Definition, classification of risks and assessment procedure 7
1.2.2. Elements of polyhedral coherent measures of risk 9
1.2.3. Reduction of SP and RO problems to PCMR problems 13
1.3. Some traditional risk assessments and worst-case analysis 19
1.3.1. Risk-matrix and RAMCAP formula 19
1.3.2. Worst-case analysis and some models of CI protection 21
1.4. Adversarial risk analysis in conditions of terrorist threat 26
1.5. Conclusion 28
1.6. Acknowledgments 29

1.7. List of abbreviations 29
1.8. References 29

Chapter 2. Models of Anti-Terrorist Protection 33
Vladimir I. NORKIN

2.1. Area control tasks 33
2.2. Simulation of attack and passive defense 37
2.3. Modeling attack on a market: a linear programming model 39
2.4. A probabilistic version of the problem of attacking the objective function 41
2.5. Modeling an attack on resources of optimal systems 42
2.6. Modeling an attack on the transport system 42
2.7. Models of protection of transport and information networks 44
2.8. Stochastic models of passive protection of transport and information networks 47
2.9. Acknowledgments 49
2.10. References 49

Chapter 3. Allocation of Resources for the Critical Infrastructure Protection 53
Vladimir I. NORKIN, Alexei A. GAIVORONSKI, Pavel S. KNOPOV and Volodymyr A. ZASLAVSKYI

3.1. The hierarchical dynamic programming 53
3.2. Examples of resource allocation problems 60
3.3. Conclusion 64
3.4. Acknowledgments 64
3.5. References 64

Chapter 4. Simulation of the Defender–Attacker Game for Critical Objects Protection 67
Vladimir I. NORKIN

4.1. Introduction 67
4.2. A simple strategic attacker–defender game 70
4.3. Generalizations 76
4.4. Further generalization 77
4.5. Conclusion 77
4.6. Acknowledgments 78
4.7. References 78

Chapter 5. Making Decisions and Motion Control in Conditions of Conflict 81
Arkadii CHIKRII

5.1. Introduction. 81
5.2. Problem statement 82
5.3. Pontryagin's first direct method. 84
5.4. Schemes of the method of resolving functions 86
5.5. Scheme with fixed points of the terminal set solid part 96
5.6. Connection of the first direct method with the method of resolving functions 98
5.7. Conclusion 103
5.8. Acknowledgments. 103
5.9. References 104

Chapter 6. Contemporary Stochastic Quasi-gradient Algorithms 107
Vladimir I. NORKIN, Alexei A. GAIVORONSKI, Pavel S. KNOPOV and Anton KOZYRIEV

6.1. Introduction. 107
6.2. A stochastic optimization problem 109
6.3. Stochastic approximation. 109
6.4. Application of stochastic quasi-gradient algorithms in machine learning. 110
6.5. Stochastic gradient methods 111
6.5.1. Stochastic gradient decent. 112
6.5.2. Accelerated methods 113
6.5.3. Adaptive methods. 116
6.5.4. Extension to non-smooth functions 118
6.5.5. Numerical illustration 121
6.6. Conclusion 123
6.7. Acknowledgments. 123
6.8. References 123

Chapter 7. Two Classes of Optimization Problems for Arcs Capacities Modernization for Fault-tolerant Networks. 127
Petro STETSYUK, Viktor STOVBA and Volodymyr ZHYDKOV

7.1. Basic concepts for a fault-tolerant network 127
7.2. Basic LP-problems A and P 131
7.3. Boolean problems A and P. 134

7.4. Convex problems A and P: decomposition algorithms 138
7.5. Software: programs SolverA and SolverP 142
7.6. Acknowledgements 145
7.7. References 145

Part 2. Cyber Security of Critical Infrastructure Facilities 147

Introduction to Part 2 149
Alexei A. GAIVORONSKI and Volodymyr A. ZASLAVSKYI

Chapter 8. Digital Authentication of the Type "friend-or-foe" by Means of One-time Signatures 151
Anatoly ANISIMOV

8.1. Introduction 151
8.2. Coalition group 153
8.3. Authentication in public-key cryptography 155
8.4. Authentication through digital signatures and sigma protocols 156
8.5. A general description of a "friend-or-foe" authentication protocol using OTSs 162
8.6. References 171

Chapter 9. Main Directions and Basic Mathematical Ideas of Cryptographic Information Security 175
Lyudmila KOVALCHUK and Mikhail SAVCHUK

9.1. Introduction 175
9.2. Problems and aspects of information security, basic concepts of cryptographic information security 175
9.2.1. Fields of application, goals, and methods of information security 176
9.2.2. Basic notions of cryptographic information security and cryptology 177
9.3. Classification of cryptosystems 179
9.4. Symmetric cryptography 180
9.4.1. General scheme of secret communication in symmetric cryptography 180
9.4.2. General classification of classical ciphers 181
9.4.3. Development of "technological" tools of cryptography 182

9.4.4. The main types of cryptographic attacks depending on the type of information, known to adversary . . . 184
9.4.5. Shannon's theory of secret systems . . . 186
9.4.6. Modern symmetric cryptosystems . . . 192
9.5. Asymmetric cryptography: public key cryptosystems . . . 195
9.5.1. One-way functions . . . 196
9.5.2. The first cryptographic algorithms of asymmetric cryptography . . . 200
9.5.3. Authentication and digital signature . . . 205
9.6. Conclusion . . . 208
9.7. References . . . 209

Chapter 10. Cybersecurity Investments in Networks . . . 211
Vasyl GORBACHUK, Maksym DUNAIEVSKYI and Seit-Bekir SULEIMANOV

10.1. Introduction . . . 211
10.2. Cybersecurity in SCNs . . . 212
10.3. Numerical experiments for networks . . . 219
10.4. Critical and risky SCNs . . . 226
10.5. Acknowledgements . . . 231
10.6. References . . . 231

List of Authors . . . 235

Index . . . 239

Summary of Volume 1 . . . 243