Igor V Kotenko

List of Publications by Year in Descending Order

244 papers	2,147 citations	15 h-index	40 g-index
295 ext. papers	2,727 ext. citations	1.2 avg, IF	5.77 L-index

#	Paper	IF	Citations
244	Detection of Business Email Compromise Attacks with Writing Style Analysis. *Communications in Computer and Information Science*, **2022**, 248-262	0.3	
243	Classification and Analysis of Vulnerabilities in Mobile Device Infrastructure Interfaces. *Communications in Computer and Information Science*, **2022**, 301-319	0.3	
242	Analytical Modeling for Identification of the Machine Code Architecture of Cyberphysical Devices in Smart Homes.. *Sensors*, **2022**, 22,	3.8	2
241	Construction and Analysis of Integral User-Oriented Trustworthiness Metrics. *Electronics (Switzerland)*, **2022**, 11, 234	2.6	1
240	Ensuring the survivability of embedded computer networks based on early detection of cyber attacks by integrating fractal analysis and statistical methods. *Microprocessors and Microsystems*, **2022**, 90, 104459	2.4	0
239	Security Measuring System for IoT Devices. *Lecture Notes in Computer Science*, **2022**, 256-275	0.9	
238	Static Analysis of Information Systems for IoT Cyber Security: A Survey of Machine Learning Approaches.. *Sensors*, **2022**, 22,	3.8	6
237	Feature Selection for Intelligent Detection of Targeted Influence on Public Opinion in Social Networks. *Lecture Notes in Networks and Systems*, **2022**, 421-430	0.5	
236	An Approach to Modeling of the Security System of Intelligent Transport Systems Based on the Use of Flat Graphs. *Lecture Notes in Networks and Systems*, **2022**, 440-451	0.5	0
235	Construction of Membership Functions for Fuzzy Management of Security Information and Events. *Studies in Systems, Decision and Control*, **2022**, 99-110	0.8	0
234	A Technique for the Design of Abstract Models of Microcontroller-Based Physical Security Systems. *Studies in Computational Intelligence*, **2022**, 397-406	0.8	
233	Security Analysis of Information Systems Based on Attack Sequences Generation and Testing. *Studies in Computational Intelligence*, **2022**, 427-437	0.8	
232	An Approach to the Synthesis of a Neural Network System for Diagnosing Computer Incidents. *Studies in Computational Intelligence*, **2022**, 407-416	0.8	
231	INTERVAL ANALYSIS OF THE SECURITY OF TELECOMMUNICATIONS RESOURCES OF CRITICAL INFRASTRUCTURES. *Matematičeskie Metody V Tehnologiâh I Tehnike*, **2022**, 64-67		
230	Systematic Literature Review of Security Event Correlation Methods. *IEEE Access*, **2022**, 10, 43387-43420	3.5	2
229	Combined Neural Network for Assessing the State of Computer Network Elements. *Studies in Computational Intelligence*, **2021**, 256-261	0.8	
228	Detecting Anomalous Behavior of Users of Data Centers Based on the Application of Artificial Neural Networks. *Lecture Notes in Computer Science*, **2021**, 331-342	0.9	

227	Selection and Justification of Information Security Indicators for Materials Processing Systems. *MATEC Web of Conferences*, **2021**, 346, 01019	0.3	
226	An Approach to Ranking the Sources of Information Dissemination in Social Networks. *Information (Switzerland)*, **2021**, 12, 416	2.6	0
225	An approach for selecting countermeasures against harmful information based on uncertainty management. *Computer Science and Information Systems*, **2021**, 57-57	0.8	
224	An Approach for Stego-Insider Detection Based on a Hybrid NoSQL Database. *Journal of Sensor and Actuator Networks*, **2021**, 10, 25	3.8	1
223	Simulation and assessment of battery depletion attacks on unmanned aerial vehicles for crisis management infrastructures. *Simulation Modelling Practice and Theory*, **2021**, 107, 102244	3.9	1
222	A Variant of the Analytical Specification of Security Information and Event Management Systems. *Studies in Systems, Decision and Control*, **2021**, 321-331	0.8	
221	CONSTRUCTION OF MEMBERSHIP FUNCTIONS IN FUZZY SECURITY INFORMATION AND EVENT MANAGEMENT TASKS. *Matematičeskie Metody V Tehnologiâh I Tehnike*, **2021**, 126-129		
220	Evaluating the Functioning Quality of Data Transmission Networks in the Context of Cyberattacks. *Energies*, **2021**, 14, 4755	3.1	2
219	Evaluation of Information Security of Industrial Automation Systems Using Fuzzy Algorithms and Predicates **2021**,		1
218	Methodology for Management of the Protection System of Smart Power Supply Networks in the Context of Cyberattacks. *Energies*, **2021**, 14, 5963	3.1	2
217	Towards Attacker Attribution for Risk Analysis. *Lecture Notes in Computer Science*, **2021**, 347-353	0.9	1
216	Target functions of the conceptual model for adaptive monitoring of integrated security in material processing systems. *Materials Today: Proceedings*, **2021**, 38, 1454-1458	1.4	
215	Detection and Monitoring of the Destructive Impacts in the Social Networks Using Machine Learning Methods. *Communications in Computer and Information Science*, **2021**, 60-65	0.3	1
214	Modelling attacks in self-organizing wireless sensor networks of smart cities. *IOP Conference Series: Materials Science and Engineering*, **2020**, 971, 032077	0.4	1
213	An Approach to Detecting Cyber Attacks against Smart Power Grids Based on the Analysis of Network Traffic Self-Similarity. *Energies*, **2020**, 13, 5031	3.1	9
212	Increasing the Sensitivity of the Method of Early Detection of Cyber-Attacks in Telecommunication Networks Based on Traffic Analysis by Extreme Filtering. *Energies*, **2020**, 13, 2774	3.1	4
211	Neural Network Based Classification of Attacks on Wireless Sensor Networks **2020**,		2
210	The intelligent system for detection and counteraction of malicious and inappropriate information on the Internet. *AI Communications*, **2020**, 33, 13-25	0.8	0

209	Design and verification of a mobile robot based on the integrated model of cyber-Physical systems. *Simulation Modelling Practice and Theory*, **2020**, 105, 102151	3.9	4
208	Attacker Behaviour Forecasting Using Methods of Intelligent Data Analysis: A Comparative Review and Prospects. *Information (Switzerland)*, **2020**, 11, 168	2.6	12
207	Augmented reality for visualizing security data for cybernetic and cyberphysical systems **2020**,		2
206	Social networks bot detection using Benford law **2020**,		1
205	A Model Checking Based Approach for Verification of Attribute-Based Access Control Policies in Cloud Infrastructures. *Advances in Intelligent Systems and Computing*, **2020**, 165-175	0.4	
204	Data Analytics for Security Management of Complex Heterogeneous Systems: Event Correlation and Security Assessment Tasks. *EAI/Springer Innovations in Communication and Computing*, **2020**, 79-116	0.6	1
203	Anomaly Detection in the HVAC System Operation by a RadViz Based Visualization-Driven Approach. *Lecture Notes in Computer Science*, **2020**, 402-418	0.9	6
202	Towards Intelligent Data Processing for Automated Determination of Information System Assets. *Advances in Information Security, Privacy, and Ethics Book Series*, **2020**, 147-160	0.3	
201	P2Onto: Making Privacy Policies Transparent. *Lecture Notes in Computer Science*, **2020**, 235-252	0.9	1
200	Assessment of components to ensure the security of control and diagnostic information about technological processes. *MATEC Web of Conferences*, **2020**, 329, 03005	0.3	1
199	COMBINED APPROACH TO INSIDER DETECTION ON COMPUTER NETWORKS. *Vestnik Sankt-Peterburgskogo Gosudarstvennogo Universiteta Tehnologii I Dizajna Seri 1, Estestvennye I Tehni skie Nauki*, **2020**, 66-71	0	
198	Problematic Issues of Information Security of Cyber-Physical Systems. *Informatics and Automation*, **2020**, 19, 1050-1088	0.5	2
197	Use of neural networks for forecasting of the exposure of social network users to destructive impacts. *Informatsionno-Upravliaiushchie Sistemy*, **2020**, 24-33	0.7	2
196	Modeling and Evaluation of Battery Depletion Attacks on Unmanned Aerial Vehicles in Crisis Management Systems. *Studies in Computational Intelligence*, **2020**, 323-332	0.8	1
195	ECU-Secure: Characteristic Functions for In-Vehicle Intrusion Detection. *Studies in Computational Intelligence*, **2020**, 495-504	0.8	2
194	The Integrated Model of Secure Cyber-Physical Systems for Their Design and Verification. *Studies in Computational Intelligence*, **2020**, 333-343	0.8	2
193	Adaptive Touch Interface: Application for Mobile Internet Security. *Communications in Computer and Information Science*, **2020**, 53-72	0.3	
192	Analysis of Attack Actions on the Railway Infrastructure Based on the Integrated Model. *Communications in Computer and Information Science*, **2020**, 145-162	0.3	1

191	An Approach to Creating an Intelligent System for Detecting and Countering Inappropriate Information on the Internet. *Studies in Computational Intelligence*, **2020**, 244-254	0.8	3
190	The Common Approach to Determination of the Destructive Information Impacts and Negative Personal Tendencies of Young Generation Using the Neural Network Methods for the Internet Content Processing. *Studies in Computational Intelligence*, **2020**, 302-310	0.8	1
189	Determining the Parameters of the Mathematical Model of the Process of Searching for Harmful Information. *Studies in Systems, Decision and Control*, **2020**, 225-236	0.8	6
188	Machine Learning and Big Data Processing for Cybersecurity Data Analysis. *Intelligent Systems Reference Library*, **2020**, 61-85	0.8	6
187	Hybrid Approach for Bots Detection in Social Networks Based on Topological, Textual and Statistical Features. *Advances in Intelligent Systems and Computing*, **2020**, 412-421	0.4	2
186	Applying Machine Learning and Parallel Data Processing for Attack Detection in IoT. *IEEE Transactions on Emerging Topics in Computing*, **2020**, 1-1	4.1	4
185	The application of the methodology for secure cyber-physical systems design to improve the semi-natural model of the railway infrastructure. *Microprocessors and Microsystems*, **2020**, 87, 103482	2.4	2
184	Stateful RORI-based countermeasure selection using hypergraphs. *Journal of Information Security and Applications*, **2020**, 54, 102562	3.5	0
183	Continuous fields: Enhanced in-vehicle anomaly detection using machine learning models. *Simulation Modelling Practice and Theory*, **2020**, 105, 102143	3.9	4
182	Stateful RORI-based countermeasure selection using hypergraphs. *Journal of Information Security and Applications*, **2020**, 54, 102541	3.5	0
181	The Visual Analytics Approach for Analyzing Trajectories of Critical Infrastructure Employers. *Energies*, **2020**, 13, 3936	3.1	1
180	GRIDHPC: A decentralized environment for high performance computing. *Concurrency Computation Practice and Experience*, **2020**, 32, e5320	1.4	0
179	Ontology of Metrics for Cyber Security Assessment **2019**,		9
178	Formulation of a system of indicators of information protection quality in automatic systems of numerical control machines for advanced material processing. *Materials Today: Proceedings*, **2019**, 19, 1835-1840	1.4	1
177	A role-base approach and a genetic algorithm for VLAN design in large critical infrastructures **2019**,		2
176	Improving the Performance of Manufacturing Technologies for Advanced Material Processing Using a Big Data and Machine Learning Framework. *Materials Today: Proceedings*, **2019**, 11, 380-385	1.4	4
175	Comparative Study of Machine Learning Methods for In-Vehicle Intrusion Detection. *Lecture Notes in Computer Science*, **2019**, 85-101	0.9	10
174	Evaluation of Resource Exhaustion Attacks against Wireless Mobile Devices. *Electronics (Switzerland)*, **2019**, 8, 500	2.6	3

173	Analysis of the Sensitivity of Algorithms for Assessing the Harmful Information Indicators in the Interests of Cyber-Physical Security. *Electronics (Switzerland)*, **2019**, 8, 284	2.6	1
172	Attack Detection in IoT Critical Infrastructures: A Machine Learning and Big Data Processing Approach **2019**,		9
171	Protection Mechanisms against Energy Depletion Attacks in Cyber-Physical Systems **2019**,		5
170	Access Control Visualization Using Triangular Matrices **2019**,		6
169	Modeling the Impact of Cyber Attacks **2019**, 135-169		6
168	Hierarchical fuzzy situational networks for online decision-making: Application to telecommunication systems. *Knowledge-Based Systems*, **2019**, 185, 104935	7.3	7
167	Design and Verification Methodology for Secure and Distributed Cyber-Physical Systems **2019**,		3
166	Monitoring the State of Materials in Cyberphysical Systems: Water Supply Case Study. *Materials Today: Proceedings*, **2019**, 11, 410-416	1.4	1
165	Combining spark and snort technologies for detection of network attacks and anomalies **2019**,		1
164	Applying Fuzzy Computing Methods for On-line Monitoring of New Generation Network Elements. *Advances in Intelligent Systems and Computing*, **2019**, 331-340	0.4	
163	Attack Detection in Mobile Internet and Networks Using the Graph-Based Schemes for Combining the Support Vector Machines. *Communications in Computer and Information Science*, **2019**, 1-16	0.3	0
162	Voronoi Maps for Planar Sensor Networks Visualization. *Communications in Computer and Information Science*, **2019**, 96-109	0.3	1
161	Visualization-Driven Approach to Fraud Detection in the Mobile Money Transfer Services. *Advances in Computer and Electrical Engineering Book Series*, **2019**, 205-236	0.3	1
160	Open challenges in visual analytics for security information and event management. *Informatsionno-Upravliaiushchie Sistemy*, **2019**, 57-67	0.7	
159	Visual Analysis of Information Dissemination Channels in Social Network for Protection Against Inappropriate Content. *Advances in Intelligent Systems and Computing*, **2019**, 95-105	0.4	5
158	Detection of Weaknesses in Information Systems for Automatic Selection of Security Actions. *Automatic Control and Computer Sciences*, **2019**, 53, 1029-1037	0.7	
157	Method of Early Detection of Cyber-Attacks on Telecommunication Networks Based on Traffic Analysis by Extreme Filtering. *Energies*, **2019**, 12, 4768	3.1	8
156	Multi-criteria security assessment of control and diagnostic data on the technological processes. *MATEC Web of Conferences*, **2019**, 298, 00071	0.3	

155	Decomposition and Formulation of System of Features of Harmful Information Based on Fuzzy Relationships **2019**,		2
154	An approach to modeling the decision support process of the security event and incident management based on Markov chains. *IFAC-PapersOnLine*, **2019**, 52, 934-939	0.7	2
153	Approach to organizing of a heterogeneous swarm of cyber-physical devices to detect intruders. *IFAC-PapersOnLine*, **2019**, 52, 945-950	0.7	
152	An Approach to Intelligent Distributed Scanning and Analytical Processing of the Internet Inappropriate Information **2019**,		2
151	Applying Artificial Intelligence Methods to Network Attack Detection. *Intelligent Systems Reference Library*, **2019**, 115-149	0.8	4
150	Attack Graph-Based Countermeasure Selection Using a Stateful Return on Investment Metric. *Lecture Notes in Computer Science*, **2018**, 293-302	0.9	1
149	Genetic Algorithms for Solving Problems of Access Control Design and Reconfiguration in Computer Networks. *ACM Transactions on Internet Technology*, **2018**, 18, 1-21	3.8	2
148	Security event analysis in XBee-based wireless mesh networks **2018**,		3
147	Selection of countermeasures against network attacks based on dynamical calculation of security metrics. *Journal of Defense Modeling and Simulation*, **2018**, 15, 181-204	0.4	5
146	Modeling and Analysis of IoT Energy Resource Exhaustion Attacks. *Studies in Computational Intelligence*, **2018**, 263-270	0.8	2
145	Ontological Hybrid Storage for Security Data. *Studies in Computational Intelligence*, **2018**, 159-171	0.8	
144	The Multi-Layer Graph Based Technique for Proactive Automatic Response Against Cyber Attacks **2018**,		1
143	Hypergraph-driven mitigation of cyberattacks. *Internet Technology Letters*, **2018**, 1, e38	1.3	0
142	Genetic algorithms for role mining in critical infrastructure data spaces **2018**,		1
141	Improvement of Attack Graphs for Cybersecurity Monitoring: Handling of Inaccuracies, Processing of Cycles, Mapping of Incidents and Automatic Countermeasure Selection. *SPIIRAS Proceedings*, **2018**, 2, 211	1.6	4
140	Architecture of the Parallel Big Data Processing System for Security Monitoring of Internet of Things Networks. *SPIIRAS Proceedings*, **2018**, 4, 5	1.6	9
139	An Ontology-based Storage of Security Information. *Information Technology and Control*, **2018**, 47,	1.3	2
138	An Automated Graph Based Approach to Risk Assessment for Computer Networks with Mobile Components. *Communications in Computer and Information Science*, **2018**, 95-106	0.3	0

137	Evolutionary Algorithms for Design of Virtual Private Networks. *Studies in Computational Intelligence*, **2018**, 287-297	0.8	
136	Assessment of Computer Network Resilience Under Impact of Cyber Attacks on the Basis of Stochastic Networks Conversion. *Communications in Computer and Information Science*, **2018**, 107-117	0.3	1
135	Monitoring and Counteraction to Malicious Influences in the Information Space of Social Networks. *Lecture Notes in Computer Science*, **2018**, 159-167	0.9	3
134	Method and Algorithms of Anomaly Detection in Multiservice Network Traffic based on Fuzzy Logical Inference. *Informatsionno-Upravliaiushchie Sistemy*, **2018**, 3, 61-68	0.7	3
133	Fuzzy Adaptive Routing in Multi-service Computer Networks under Cyber Attack Implementation. *Advances in Intelligent Systems and Computing*, **2018**, 215-225	0.4	
132	Intelligent Security Analysis of Railway Transport Infrastructure Components on the Base of Analytical Modeling. *Advances in Intelligent Systems and Computing*, **2018**, 178-188	0.4	1
131	Synthesis of Controlled Parameters of Cyber-Physical-Social Systems for Monitoring of Security Incidents in Conditions of Uncertainty. *Journal of Physics: Conference Series*, **2018**, 1069, 012153	0.3	3
130	Implementation of Intelligent Agents for Network Traffic and Security Risk Analysis in Cyber-Physical Systems **2018**,		2
129	Approach for determination of cyber-attack goals based on the ontology of security metrics. *IOP Conference Series: Materials Science and Engineering*, **2018**, 450, 052006	0.4	3
128	Framework for Mobile Internet of Things Security Monitoring Based on Big Data Processing and Machine Learning. *IEEE Access*, **2018**, 6, 72714-72723	3.5	27
127	Applying Intelligent Agents for Anomaly Detection of Network Traffic in Internet of Things Networks **2018**,		2
126	Ensuring Availability of Wireless Mesh Networks for Crisis Management. *Studies in Computational Intelligence*, **2018**, 344-353	0.8	3
125	Visual Analytics for Improving Efficiency of Network Forensics: Account Theft Investigation. *Journal of Physics: Conference Series*, **2018**, 1069, 012062	0.3	
124	Analytical modeling and assessment of cyber resilience on the base of stochastic networks conversion **2018**,		5
123	AI- and Metrics-Based Vulnerability-Centric Cyber Security Assessment and Countermeasure Selection. *Computer Communications and Networks*, **2018**, 101-130	0.5	3
122	A technique for design of secure data transfer environment: Application for I2C protocol **2018**,		3
121	Visual analysis of CAN bus traffic injection using radial bar charts **2018**,		3
120	Parallelization of Security Event Correlation Based on Accounting of Event Type Links **2018**,		2

119	Parallel Processing of Big Heterogeneous Data for Security Monitoring of IoT Networks **2017**,		7
118	CVSS-based Probabilistic Risk Assessment for Cyber Situational Awareness and Countermeasure Selection **2017**,		16
117	Enhancement of probabilistic attack graphs for accurate cyber security monitoring **2017**,		4
116	Administrating role-based access control by genetic algorithms **2017**,		3
115	Protection Against Information in eSociety: Using Data Mining Methods to Counteract Unwanted and Malicious Data. *Communications in Computer and Information Science*, **2017**, 170-184	0.3	4
114	Modeling and analysis of security incidents for mobile communication mesh Zigbee-based network **2017**,		3
113	The ontological approach application for construction of the hybrid security repository **2017**,		1
112	Reconfiguration of RBAC schemes by genetic algorithms. *Studies in Computational Intelligence*, **2017**, 89-98	0.8	3
111	Hybridization of computational intelligence methods for attack detection in computer networks. *Journal of Computational Science*, **2017**, 23, 145-156	3.4	14
110	Design lifecycle for secure cyber-physical systems based on embedded devices **2017**,		5
109	Correlation of security events based on the analysis of structures of event types **2017**,		3
108	Analytical attack modeling and security assessment based on the common vulnerability scoring system **2017**,		3
107	Generation of Source Data for Experiments with Network Attack Detection Software. *Journal of Physics: Conference Series*, **2017**, 820, 012033	0.3	3
106	Categorisation of web pages for protection against inappropriate content in the internet. *International Journal of Internet Protocol Technology*, **2017**, 10, 61	0.3	13
105	Aggregation of elastic stack instruments for collecting, storing and processing of security information and events **2017**,		4
104	A System for Collecting, Storing and Processing Security Information and Events based on Elastic Stack Tools. *SPIIRAS Proceedings*, **2017**, 5, 5	1.6	3
103	Assessment of Cyber-Resilience of Computer Networks based on Simulation of Cyber Attacks by the Stochastic Networks Conversion Method. *SPIIRAS Proceedings*, **2017**, 6, 160	1.6	9
102	Network Anomaly Detection Based on an Ensemble of Adaptive Binary Classifiers. *Lecture Notes in Computer Science*, **2017**, 143-157	0.9	3

101	Choosing Models for Security Metrics Visualization. *Lecture Notes in Computer Science*, **2017**, 75-87	0.9	12
100	Detection of traffic anomalies in multi-service networks based on a fuzzy logical inference. *Studies in Computational Intelligence*, **2017**, 79-88	0.8	4
99	Visualization Model for Monitoring of Computer Networks Security Based on the Analogue of Voronoi Diagrams. *Lecture Notes in Computer Science*, **2016**, 141-157	0.9	3
98	Countermeasure Selection Based on the Attack and Service Dependency Graphs for Security Incident Management. *Lecture Notes in Computer Science*, **2016**, 107-124	0.9	10
97	Reconfiguration of Access Schemes in Virtual Networks of the Internet of Things by Genetic Algorithms. *Studies in Computational Intelligence*, **2016**, 155-165	0.8	1
96	Using Genetic Algorithms for Design and Reconfiguration of RBAC Schemes **2016**,		7
95	Analysis and Classification of Methods for Network Attack Detection. *SPIIRAS Proceedings*, **2016**, 2, 207	1.6	19
94	An Analysis of Security Event Correlation Techniques in Siem-Systems. Part 1. *SPIIRAS Proceedings*, **2016**, 4, 5	1.6	6
93	Combined Design Technique for Secure Embedded Devices Exemplified by a Perimeter Protection System. *SPIIRAS Proceedings*, **2016**, 5, 5	1.6	11
92	Improving the Categorization of Web Sites by Analysis of Html-Tags Statistics to Block Inappropriate Content. *Studies in Computational Intelligence*, **2016**, 257-263	0.8	7
91	Application of Hybrid Neural Networks for Monitoring and Forecasting Computer Networks States. *Lecture Notes in Computer Science*, **2016**, 521-530	0.9	2
90	Mathematical Models of Visualization in SIEM Systems. *SPIIRAS Proceedings*, **2016**, 3, 90	1.6	2
89	An Analysis of Security Event Correlation Techniques in SIEM-Systems. Part 2. *SPIIRAS Proceedings*, **2016**, 6, 208	1.6	3
88	An Approach to Aggregation of Security Events in Internet-of-Things Networks Based on Genetic Optimization **2016**,		4
87	Application of a Technique for Secure Embedded Device Design Based on Combining Security Components for Creation of a Perimeter Protection System **2016**,		3
86	Dynamical Calculation of Security Metrics for Countermeasure Selection in Computer Networks **2016**,		12
85	Automated design, verification and testing of secure systems with embedded devices based on elicitation of expert knowledge. *Journal of Ambient Intelligence and Humanized Computing*, **2016**, 7, 705-719	3.7	5
84	Event correlation in the integrated cyber-physical security system **2016**,		9

83	Detection of anomalies in data for monitoring of security components in the Internet of Things **2015**,		16
82	Investigation of DDoS Attacks by Hybrid Simulation. *Lecture Notes in Computer Science*, **2015**, 179-189	0.9	5
81	Countermeasure Selection in SIEM Systems Based on the Integrated Complex of Security Metrics **2015**,		9
80	Neural network approach to forecast the state of the Internet of Things elements **2015**,		22
79	Attack tree-based approach for real-time security event processing. *Automatic Control and Computer Sciences*, **2015**, 49, 701-704	0.7	5
78	Design and verification of protected systems with integrated devices based on expert knowledge. *Automatic Control and Computer Sciences*, **2015**, 49, 648-652	0.7	
77	Simulation of Bio-inspired Security Mechanisms against Network Infrastructure Attacks. *Studies in Computational Intelligence*, **2015**, 127-133	0.8	1
76	A Genetic Approach for Virtual Computer Network Design. *Studies in Computational Intelligence*, **2015**, 95-105	0.8	6
75	Design of Integrated Vulnerabilities Database for Computer Networks Security Analysis **2015**,		4
74	Abnormal traffic detection in networks of the Internet of things based on fuzzy logical inference **2015**,		5
73	Evaluation of text classification techniques for inappropriate web content blocking **2015**,		6
72	The CAPEC based generator of attack scenarios for network security evaluation **2015**,		11
71	Countermeasure Security Risks Management in the Internet of Things Based on Fuzzy Logic Inference **2015**,		10
70	Network Attack Detection Based on Combination of Neural, Immune and Neuro-Fuzzy Classifiers **2015**,		16
69	The Genetic Approach for Design of Virtual Private Networks **2015**,		2
68	Improved genetic algorithms for solving the optimisation tasks for design of access control schemes in computer networks. *International Journal of Bio-Inspired Computation*, **2015**, 7, 98	2.9	15
67	Creation of a Fuzzy Knowledge Base for Adaptive Security Systems **2014**,		3
66	Analysis and Evaluation of Web Pages Classification Techniques for Inappropriate Content Blocking. *Lecture Notes in Computer Science*, **2014**, 39-54	0.9	9

65	Security Metrics Based on Attack Graphs for the Olympic Games Scenario **2014**,		6
64	The framework for simulation of bioinspired security mechanisms against network infrastructure attacks. *Scientific World Journal, The*, **2014**, 2014, 172583	2.2	0
63	Fast Network Attack Modeling and Security Evaluation based on Attack Graphs. *Journal of Cyber Security and Mobility*, **2014**, 3, 27-46	1	6
62	Interactive Multi-View Visualization for Fraud Detection in Mobile Money Transfer Services. *International Journal of Mobile Computing and Multimedia Communications*, **2014**, 6, 73-97	0.7	4
61	Creating new-generation cybersecurity monitoring and management systems. *Herald of the Russian Academy of Sciences*, **2014**, 84, 424-431	0.7	4
60	Security Evaluation for Cyber Situational Awareness **2014**,		3
59	Visualization of Security Metrics for Cyber Situation Awareness **2014**,		6
58	Dynamical Attack Simulation for Security Information and Event Management. *Lecture Notes in Geoinformation and Cartography*, **2014**, 219-234	0.3	1
57	Expert Knowledge Based Design and Verification of Secure Systems with Embedded Devices. *Lecture Notes in Computer Science*, **2014**, 194-210	0.9	6
56	Visual Analytics for Detecting Anomalous Activity in Mobile Money Transfer Services. *Lecture Notes in Computer Science*, **2014**, 63-78	0.9	2
55	Security Assessment of Computer Networks Based on Attack Graphs and Security Events. *Lecture Notes in Computer Science*, **2014**, 462-471	0.9	19
54	Logical Inference Framework for Security Management in Geographical Information Systems. *Lecture Notes in Geoinformation and Cartography*, **2014**, 203-218	0.3	
53	Simulation of Protection Mechanisms Based on "Nervous Network System" against Infrastructure Attacks **2013**,		2
52	The Ontology of Metrics for Security Evaluation and Decision Support in SIEM Systems **2013**,		16
51	Computer attack modeling and security evaluation based on attack graphs **2013**,		13
50	Simulation-based study of botnets and defense mechanisms against them. *Journal of Computer and Systems Sciences International*, **2013**, 52, 43-65	1	6
49	Analytical Visualization Techniques for Security Information and Event Management **2013**,		18
48	Design and Implementation of a Hybrid Ontological-Relational Data Repository for SIEM Systems. *Future Internet*, **2013**, 5, 355-375	3.3	7

47	VisSecAnalyzer: A Visual Analytics Tool for Network Security Assessment. *Lecture Notes in Computer Science*, **2013**, 345-360	0.9	5
46	Agent-based simulation of cooperative defence against botnets. *Concurrency Computation Practice and Experience*, **2012**, 24, 573-588	1.4	8
45	Using Low-Level Dynamic Attributes for Malware Detection Based on Data Mining Methods. *Lecture Notes in Computer Science*, **2012**, 254-269	0.9	0
44	The Ontological Approach for SIEM Data Repository Implementation **2012**,		13
43	Common Framework for Attack Modeling and Security Evaluation in SIEM Systems **2012**,		18
42	A Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded Components **2012**,		14
41	Design and Performance Evaluation of Improved Genetic Algorithm for Role Mining Problem **2012**,		10
40	Configuration-Based Approach to Embedded Device Security. *Lecture Notes in Computer Science*, **2012**, 270-285	0.9	9
39	An Approach for Network Information Flow Analysis for Systems of Embedded Components. *Lecture Notes in Computer Science*, **2012**, 146-155	0.9	5
38	Security Analysis of Information Systems Taking into Account Social Engineering Attacks **2011**,		15
37	Verification of security policy filtering rules by Model Checking **2011**,		9
36	Genetic Algorithms for Role Mining Problem **2011**,		16
35	Combining of Scanning Protection Mechanisms in GIS and Corporate Information Systems. *Lecture Notes in Geoinformation and Cartography*, **2011**, 45-58	0.3	1
34	Malware Detection by Data Mining Techniques Based on Positionally Dependent Features **2010**,		16
33	Genetic Optimization of Access Control Schemes in Virtual Local Area Networks. *Lecture Notes in Computer Science*, **2010**, 209-216	0.9	3
32	Security and Scalability of Remote Entrusting Protection. *Lecture Notes in Computer Science*, **2010**, 298-306	0.9	1
31	Simulation of Botnets: Agent-Based Approach. *Studies in Computational Intelligence*, **2010**, 247-252	0.8	
30	Framework for Integrated Proactive Network Worm Detection and Response **2009**,		2

29	Integrated Usage of Data Mining Methodsfor Malware Detection. *Lecture Notes in Geoinformation and Cartography*, **2009**, 343-357	0.3	2
28	Proactive monitoring of security policy accomplishment in computer networks **2009**,		1
27	Design of Entrusting Protocols for Software Protection. *Lecture Notes in Geoinformation and Cartography*, **2009**, 301-316	0.3	0
26	Multi-agent Framework for Simulation of Adaptive Cooperative Defense Against Internet Attacks **2007**, 212-228		2
25	Multiagent simulation of protection of information resources in internet. *Journal of Computer and Systems Sciences International*, **2007**, 46, 741-755	1	
24	Multi-agent Modelling and Simulation of Cyber-Attacks and Cyber-Defense for Homeland Security **2007**,		13
23	Software Environment for Simulation and Evaluation of a Security Operation Center **2007**, 111-127		1
22	Security Policy Verification Tool for Geographical Information Systems **2007**, 128-146		1
21	Policy-Based Proactive Monitoring of Security Policy Performance **2007**, 197-212		
20	Event Calcululus Based Checking of Filtering Policies **2007**, 248-253		
19	Attack Graph Based Evaluation of Network Security. *Lecture Notes in Computer Science*, **2006**, 216-227	0.9	42
18	Agent Teams in Cyberspace: Security Guards in the Global Internet **2006**,		7
17	Simulation of Internet DDoS Attacks and Defense. *Lecture Notes in Computer Science*, **2006**, 327-342	0.9	12
16	Agent-Based Simulation Of Distributed Defense Against Computer Network Attacks **2006**,		2
15	Security Checker Architecture for Policy-Based Security Management. *Lecture Notes in Computer Science*, **2005**, 460-465	0.9	2
14	Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages of Computer Network Life Cycle. *Lecture Notes in Computer Science*, **2005**, 311-324	0.9	6
13	Experiments with Simulation of Attacks against Computer Networks. *Lecture Notes in Computer Science*, **2003**, 183-194	0.9	4
12	Teamwork of Hackers-Agents: Modeling and Simulation of Coordinated Distributed Attacks on Computer Networks **2003**, 464-474		2

11	Dynamic panel data models: a guide to micro data methods and practice. *Portuguese Economic Journal*, **2002**, 1, 141-162	0.9	1039
10	Software Development Kit for Multi-agent Systems Design and Implementation. *Lecture Notes in Computer Science*, **2002**, 121-130	0.9	12
9	Attacks against Computer Network: Formal Grammar-Based Framework and Simulation Tool. *Lecture Notes in Computer Science*, **2002**, 219-238	0.9	19
8	Agent-Based Model of Computer Network Security System: A Case Study. *Lecture Notes in Computer Science*, **2001**, 39-50	0.9	14
7	Ontology-Based Multi-agent Model of an Information Security System. *Lecture Notes in Computer Science*, **1999**, 528-532	0.9	4
6	Bleomycin mimics. Design and synthesis of an acridine derivative whichcleaves DNA in a sequence-neutral manner. *Journal of the Chemical Society Perkin Transactions II*, **1997**, 523-532		4
5	Active vulnerability assessment of computer networks by simulation of complex remote attacks		9
4	Formal framework for modeling and simulation of DDoS attacks based on teamwork of hackers-agents		1
3	The Software Environment for Multi-agent Simulation of Defense Mechanisms against DDoS Attacks		3
2			2
1	The multi-agent systems for computer network security assurance: frameworks and case studies		8