Igor V Kotenko

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/889911/publications.pdf

Version: 2024-02-01

277 papers	3,396 citations	516215 16 h-index	233125 45 g-index
296 all docs	296 docs citations	296 times ranked	1916 citing authors

#	Article	IF	Citations
1	Dynamic panel data models: a guide to micro data methods and practice. Portuguese Economic Journal, 2002, 1, 141-162.	0.6	1,504
2	Attack Graph Based Evaluation of Network Security. Lecture Notes in Computer Science, 2006, , 216-227.	1.0	59
3	Framework for Mobile Internet of Things Security Monitoring Based on Big Data Processing and Machine Learning. IEEE Access, 2018, 6, 72714-72723.	2.6	52
4	Attacks against Computer Network: Formal Grammar-Based Framework and Simulation Tool. Lecture Notes in Computer Science, 2002, , 219-238.	1.0	38
5	Hybridization of computational intelligence methods for attack detection in computer networks. Journal of Computational Science, 2017, 23, 145-156.	1.5	32
6	Analysis and Classification of Methods for Network Attack Detection. SPIIRAS Proceedings, 2016, 2, 207.	0.8	31
7	Common Framework for Attack Modeling and Security Evaluation in SIEM Systems. , 2012, , .		29
8	Security Assessment of Computer Networks Based on Attack Graphs and Security Events. Lecture Notes in Computer Science, 2014, , 462-471.	1.0	28
9	Security Analysis of Information Systems Taking into Account Social Engineering Attacks. , 2011, , .		27
10	Malware Detection by Data Mining Techniques Based on Positionally Dependent Features. , 2010, , .		26
11	Neural network approach to forecast the state of the Internet of Things elements. , 2015, , .		26
12	Analytical Visualization Techniques for Security Information and Event Management. , 2013, , .		25
13	CVSS-based Probabilistic Risk Assessment for Cyber Situational Awareness and Countermeasure Selection. , 2017, , .		25
14	Simulation of Internet DDoS Attacks and Defense. Lecture Notes in Computer Science, 2006, , 327-342.	1.0	24
15	Multi-agent Modelling and Simulation of Cyber-Attacks and Cyber-Defense for Homeland Security. , 2007, , .		24
16	Detection of anomalies in data for monitoring of security components in the Internet of Things. , 2015, , .		24
17	A Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded Components. , 2012, , .		23
18	Agentâ€based simulation of cooperative defence against botnets. Concurrency Computation Practice and Experience, 2012, 24, 573-588.	1.4	23

#	Article	IF	Citations
19	Static Analysis of Information Systems for IoT Cyber Security: A Survey of Machine Learning Approaches. Sensors, 2022, 22, 1335.	2.1	23
20	The Ontology of Metrics for Security Evaluation and Decision Support in SIEM Systems. , 2013, , .		21
21	Network Attack Detection Based on Combination of Neural, Immune and Neuro-Fuzzy Classifiers. , 2015, , .		21
22	The CAPEC based generator of attack scenarios for network security evaluation. , 2015, , .		20
23	An Approach to Detecting Cyber Attacks against Smart Power Grids Based on the Analysis of Network Traffic Self-Similarity. Energies, 2020, 13, 5031.	1.6	20
24	Genetic Algorithms for Role Mining Problem. , 2011, , .		19
25	Hierarchical fuzzy situational networks for online decision-making: Application to telecommunication systems. Knowledge-Based Systems, 2019, 185, 104935.	4.0	19
26	Comparative Study of Machine Learning Methods for In-Vehicle Intrusion Detection. Lecture Notes in Computer Science, 2019, , 85-101.	1.0	19
27	Computer attack modeling and security evaluation based on attack graphs. , 2013, , .		18
28	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.	0.6	18
29	Dynamical Calculation of Security Metrics for Countermeasure Selection in Computer Networks. , 2016, , .		18
30	Categorisation of web pages for protection against inappropriate content in the internet. International Journal of Internet Protocol Technology, 2017, 10, 61.	0.2	18
31	Attacker Behaviour Forecasting Using Methods of Intelligent Data Analysis: A Comparative Review and Prospects. Information (Switzerland), 2020, 11, 168.	1.7	18
32	Agent-Based Model of Computer Network Security System: A Case Study. Lecture Notes in Computer Science, 2001, , 39-50.	1.0	18
33	Verification of security policy filtering rules by Model Checking. , 2011, , .		17
34	Attack Detection in IoT Critical Infrastructures: A Machine Learning and Big Data Processing Approach. , 2019, , .		17
35	The multi-agent systems for computer network security assurance: frameworks and case studies. , 0, , .		16
36	Active vulnerability assessment of computer networks by simulation of complex remote attacks. , 0, , .		16

#	Article	IF	Citations
37	Fast Network Attack Modeling and Security Evaluation based on Attack Graphs. Journal of Cyber Security and Mobility, 2014, 3, 27-46.	0.7	16
38	Systematic Literature Review of Security Event Correlation Methods. IEEE Access, 2022, 10, 43387-43420.	2.6	16
39	The Ontological Approach for SIEM Data Repository Implementation. , 2012, , .		15
40	Design and Performance Evaluation of Improved Genetic Algorithm for Role Mining Problem. , 2012, , .		14
41	Abnormal traffic detection in networks of the Internet of things based on fuzzy logical inference. , 2015, , .		14
42	Countermeasure Security Risks Management in the Internet of Things Based on Fuzzy Logic Inference. , 2015, , .		14
43	Combined Design Technique for Secure Embedded Devices Exemplified by a Perimeter Protection System. SPIIRAS Proceedings, 2016, 5, 5.	0.8	14
44	Visualization of Security Metrics for Cyber Situation Awareness. , 2014, , .		13
45	Ontology of Metrics for Cyber Security Assessment. , 2019, , .		13
46	Architecture of the Parallel Big Data Processing System for Security Monitoring of Internet of Things Networks. SPIIRAS Proceedings, 2018, 4, 5.	0.8	13
47	Event correlation in the integrated cyber-physical security system. , 2016, , .		12
48	Countermeasure Selection Based on the Attack and Service Dependency Graphs for Security Incident Management. Lecture Notes in Computer Science, 2016, , 107-124.	1.0	12
49	Method of Early Detection of Cyber-Attacks on Telecommunication Networks Based on Traffic Analysis by Extreme Filtering. Energies, 2019, 12, 4768.	1.6	12
50	Machine Learning and Big Data Processing for Cybersecurity Data Analysis. Intelligent Systems Reference Library, 2020, , 61-85.	1.0	12
51	Analysis and Evaluation of Web Pages Classification Techniques for Inappropriate Content Blocking. Lecture Notes in Computer Science, 2014, , 39-54.	1.0	11
52	Parallel Processing of Big Heterogeneous Data for Security Monitoring of IoT Networks. , 2017, , .		11
53	Assessment of Cyber-Resilience of Computer Networks based on Simulation of Cyber Attacks by the Stochastic Networks Conversion Method. SPIIRAS Proceedings, 2017, 6, 160.	0.8	11
54	Anomaly Detection in the HVAC System Operation by a RadViz Based Visualization-Driven Approach. Lecture Notes in Computer Science, 2020, , 402-418.	1.0	11

#	Article	IF	Citations
55	Agent Teams in Cyberspace: Security Guards in the Global Internet. , 2006, , .		10
56	Multi-agent Framework for Simulation of Adaptive Cooperative Defense Against Internet Attacks. , 2007, , 212-228.		10
57	Countermeasure Selection in SIEM Systems Based on the Integrated Complex of Security Metrics. , 2015, , .		10
58	Selection of countermeasures against network attacks based on dynamical calculation of security metrics. Journal of Defense Modeling and Simulation, 2018, 15, 181-204.	1.2	10
59	Analytical modeling and assessment of cyber resilience on the base of stochastic networks conversion. , 2018, , .		10
60	Modeling the Impact of Cyber Attacks. , 2019, , 135-169.		10
61	Continuous fields: Enhanced in-vehicle anomaly detection using machine learning models. Simulation Modelling Practice and Theory, 2020, 105, 102143.	2.2	10
62	Simulation and assessment of battery depletion attacks on unmanned aerial vehicles for crisis management infrastructures. Simulation Modelling Practice and Theory, 2021, 107, 102244.	2.2	10
63	Using Genetic Algorithms for Design and Reconfiguration of RBAC Schemes. , 2016, , .		10
64	Simulation-based study of botnets and defense mechanisms against them. Journal of Computer and Systems Sciences International, 2013, 52, 43-65.	0.2	9
65	Security Metrics Based on Attack Graphs for the Olympic Games Scenario. , 2014, , .		9
66	Evaluation of text classification techniques for inappropriate web content blocking. , 2015, , .		9
67	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.	3.3	9
68	Design lifecycle for secure cyber-physical systems based on embedded devices. , 2017, , .		9
69	Applying machine learning and parallel data processing for attack detection in IoT. IEEE Transactions on Emerging Topics in Computing, 2021, 9, 1642-1653.	3.2	9
70	Design and verification of a mobile robot based on the integrated model of cyber-Physical systems. Simulation Modelling Practice and Theory, 2020, 105, 102151.	2.2	9
71	Methodology for Management of the Protection System of Smart Power Supply Networks in the Context of Cyberattacks. Energies, 2021, 14, 5963.	1.6	9
72	VisSecAnalyzer: A Visual Analytics Tool for Network Security Assessment. Lecture Notes in Computer Science, 2013, , 345-360.	1.0	9

#	Article	IF	Citations
73	Ontology-Based Multi-agent Model of an Information Security System. Lecture Notes in Computer Science, 1999, , 528-532.	1.0	8
74	Experiments with Simulation of Attacks against Computer Networks. Lecture Notes in Computer Science, 2003, , 183-194.	1.0	8
75	Analytical attack modeling and security assessment based on the common vulnerability scoring system. , 2017, , .		8
76	Aggregation of elastic stack instruments for collecting, storing and processing of security information and events. , 2017, , .		8
77	Enhancement of probabilistic attack graphs for accurate cyber security monitoring. , 2017, , .		8
78	A technique for design of secure data transfer environment: Application for I2C protocol. , 2018, , .		8
79	Design and Implementation of a Hybrid Ontological-Relational Data Repository for SIEM Systems. Future Internet, 2013, 5, 355-375.	2.4	7
80	An Approach to Aggregation of Security Events in Internet-of-Things Networks Based on Genetic Optimization. , 2016, , .		7
81	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	7
82	AI- and Metrics-Based Vulnerability-Centric Cyber Security Assessment and Countermeasure Selection. Computer Communications and Networks, 2018, , 101-130.	0.8	7
83	Parallelization of Security Event Correlation Based on Accounting of Event Type Links. , 2018, , .		7
84	Design and Verification Methodology for Secure and Distributed Cyber-Physical Systems. , 2019, , .		7
85	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.	1.6	7
86	Neural Network Based Classification of Attacks on Wireless Sensor Networks. , 2020, , .		7
87	Selection of Deep Neural Network Models for IoT Anomaly Detection Experiments. , 2021, , .		7
88	Visual Analysis of Information Dissemination Channels in Social Network for Protection Against Inappropriate Content. Advances in Intelligent Systems and Computing, 2019, , 95-105.	0.5	7
89	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	7
90	Expert Knowledge Based Design and Verification of Secure Systems with Embedded Devices. Lecture Notes in Computer Science, 2014, , 194-210.	1.0	7

#	Article	IF	Citations
91	Visual Analytics for Detecting Anomalous Activity in Mobile Money Transfer Services. Lecture Notes in Computer Science, 2014, , 63-78.	1.0	7
92	An Analysis of Security Event Correlation Techniques in Siem-Systems. Part 1. SPIIRAS Proceedings, 2016, 4, 5.	0.8	7
93	Detection of traffic anomalies in multi-service networks based on a fuzzy logical inference. Studies in Computational Intelligence, 2017, , 79-88.	0.7	7
94	The Software Environment for Multi-agent Simulation of Defense Mechanisms against DDoS Attacks. , 0, , .		6
95	Creating new-generation cybersecurity monitoring and management systems. Herald of the Russian Academy of Sciences, 2014, 84, 424-431.	0.2	6
96	Security event analysis in XBee-based wireless mesh networks. , 2018, , .		6
97	Access Control Visualization Using Triangular Matrices. , 2019, , .		6
98	Stateful RORI-based countermeasure selection using hypergraphs. Journal of Information Security and Applications, 2020, 54, 102562.	1.8	6
99	An Approach for Stego-Insider Detection Based on a Hybrid NoSQL Database. Journal of Sensor and Actuator Networks, 2021, 10, 25.	2.3	6
100	Agent-Based Modeling and Simulation of Network Infrastructure Cyber-Attacks and Cooperative Defense Mechanisms. , 0, , .		6
101	Problematic Issues of Information Security of Cyber-Physical Systems. Informatics and Automation, 2020, 19, 1050-1088.	0.6	6
102	The control of teams of autonomous objects in the time-constrained environments. , 0, , .		5
103	Interactive Multi-View Visualization for Fraud Detection in Mobile Money Transfer Services. International Journal of Mobile Computing and Multimedia Communications, 2014, 6, 73-97.	0.4	5
104	Attack tree-based approach for real-time security event processing. Automatic Control and Computer Sciences, 2015, 49, 701-704.	0.4	5
105	Design of Integrated Vulnerabilities Database for Computer Networks Security Analysis. , 2015, , .		5
106	Investigation of DDoS Attacks by Hybrid Simulation. Lecture Notes in Computer Science, 2015, , 179-189.	1.0	5
107	Administrating role-based access control by genetic algorithms. , 2017, , .		5
108	Generation of Source Data for Experiments with Network Attack Detection Software. Journal of Physics: Conference Series, 2017, 820, 012033.	0.3	5

#	Article	IF	Citations
109	A role-base approach and a genetic algorithm for VLAN design in large critical infrastructures. , 2019, , .		5
110	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.	0.9	5
111	Protection Mechanisms against Energy Depletion Attacks in Cyber-Physical Systems. , 2019, , .		5
112	Evaluation of Information Security of Industrial Automation Systems Using Fuzzy Algorithms and Predicates. , 2021, , .		5
113	A System for Collecting, Storing and Processing Security Information and Events based on Elastic Stack Tools. SPIIRAS Proceedings, 2017, 5, 5.	0.8	5
114	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.	0.8	5
115	An Approach for Network Information Flow Analysis for Systems of Embedded Components. Lecture Notes in Computer Science, 2012, , 146-155.	1.0	5
116	Assessment of components to ensure the security of control and diagnostic information about technological processes. MATEC Web of Conferences, 2020, 329, 03005.	0.1	5
117	Bleomycin mimics. Design and synthesis of an acridine derivative which cleaves DNA in a sequence-neutral manner. Journal of the Chemical Society Perkin Transactions II, 1997, , 523-532.	0.9	4
118	Genetic Optimization of Access Control Schemes in Virtual Local Area Networks. Lecture Notes in Computer Science, 2010, , 209-216.	1.0	4
119	Creation of a Fuzzy Knowledge Base for Adaptive Security Systems. , 2014, , .		4
120	The Genetic Approach for Design of Virtual Private Networks. , 2015, , .		4
121	Application of a Technique for Secure Embedded Device Design Based on Combining Security Components for Creation of a Perimeter Protection System. , 2016, , .		4
122	Protection Against Information in eSociety: Using Data Mining Methods to Counteract Unwanted and Malicious Data. Communications in Computer and Information Science, 2017, , 170-184.	0.4	4
123	Correlation of security events based on the analysis of structures of event types. , 2017, , .		4
124	Modeling and Analysis of IoT Energy Resource Exhaustion Attacks. Studies in Computational Intelligence, 2018, , 263-270.	0.7	4
125	Approach for determination of cyber-attack goals based on the ontology of security metrics. IOP Conference Series: Materials Science and Engineering, 2018, 450, 052006.	0.3	4
126	Visual analysis of CAN bus traffic injection using radial bar charts. , 2018, , .		4

#	Article	IF	Citations
127	Evaluation of Resource Exhaustion Attacks against Wireless Mobile Devices. Electronics (Switzerland), 2019, 8, 500.	1.8	4
128	Applying Artificial Intelligence Methods to Network Attack Detection. Intelligent Systems Reference Library, 2019, , 115-149.	1.0	4
129	The application of the methodology for secure cyberâ€“physical systems design to improve the semi-natural model of the railway infrastructure. Microprocessors and Microsystems, 2020, 87, 103482.	1.8	4
130	A technique for early detection of cyberattacks using the traffic self-similarity property and a statistical approach. , 2021, , .		4
131	Evaluating the Functioning Quality of Data Transmission Networks in the Context of Cyberattacks. Energies, 2021, 14, 4755.	1.6	4
132	Augmented reality for visualizing security data for cybernetic and cyberphysical systems. , 2020, , .		4
133	Agent-Based Simulation Of Distributed Defense Against Computer Network Attacks. , 2006, , .		4
134	An Analysis of Security Event Correlation Techniques in SIEM-Systems. Part 2. SPIIRAS Proceedings, 2016, 6, 208.	0.8	4
135	Monitoring and Counteraction to Malicious Influences in the Information Space of Social Networks. Lecture Notes in Computer Science, 2018, , 159-167.	1.0	4
136	Method and Algorithms of Anomaly Detection in Multiservice Network Traffic based on Fuzzy Logical Inference. Informatsionno-Upravliaiushchie Sistemy, 2018, 3, 61-68.	0.3	4
137	Modeling and Evaluation of Battery Depletion Attacks on Unmanned Aerial Vehicles in Crisis Management Systems. Studies in Computational Intelligence, 2020, , 323-332.	0.7	4
138	Analysis of Attack Actions on the Railway Infrastructure Based on the Integrated Model. Communications in Computer and Information Science, 2020, , 145-162.	0.4	4
139	P2Onto: Making Privacy Policies Transparent. Lecture Notes in Computer Science, 2020, , 235-252.	1.0	4
140	Analytical Modeling for Identification of the Machine Code Architecture of Cyberphysical Devices in Smart Homes. Sensors, 2022, 22, 1017.	2.1	4
141	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.	1.8	4
142	Formal framework for modeling and simulation of DDoS attacks based on teamwork of hackers-agents. , 0, , .		3
143	Framework for Integrated Proactive Network Worm Detection and Response. , 2009, , .		3
144	Integrated Usage of Data Mining Methodsfor Malware Detection. Lecture Notes in Geoinformation and Cartography, 2009, , 343-357.	0.5	3

#	Article	IF	Citations
145	Proactive monitoring of security policy accomplishment in computer networks. , 2009, , .		3
146	Security metrics for risk assessment of distributed information systems. , 2013, , .		3
147	Security Evaluation for Cyber Situational Awareness. , 2014, , .		3
148	Modeling and analysis of security incidents for mobile communication mesh Zigbee-based network. , 2017, , .		3
149	Reconfiguration of RBAC schemes by genetic algorithms. Studies in Computational Intelligence, 2017, , 89-98.	0.7	3
150	Genetic Algorithms for Solving Problems of Access Control Design and Reconfiguration in Computer Networks. ACM Transactions on Internet Technology, 2018, 18, 1-21.	3.0	3
151	Implementation of Intelligent Agents for Network Traffic and Security Risk Analysis in Cyber-Physical Systems. , 2018, , .		3
152	Applying Intelligent Agents for Anomaly Detection of Network Traffic in Internet of Things Networks. , 2018, , .		3
153	Ensuring Availability of Wireless Mesh Networks for Crisis Management. Studies in Computational Intelligence, 2018, , 344-353.	0.7	3
154	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.	0.9	3
155	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.	0.5	3
156	The intelligent system for detection and counteraction of malicious and inappropriate information on the Internet. AI Communications, 2020, 33, 13-25.	0.8	3
157	Teamwork of Hackers-Agents: Modeling and Simulation of Coordinated Distributed Attacks on Computer Networks. , 2003, , 464-474.		3
158	An Approach to Creating an Intelligent System for Detecting and Countering Inappropriate Information on the Internet. Studies in Computational Intelligence, 2020, , 244-254.	0.7	3
159	Network Anomaly Detection Based on an Ensemble of Adaptive Binary Classifiers. Lecture Notes in Computer Science, 2017, , 143-157.	1.0	3
160	An Ontology-based Storage of Security Information. Information Technology and Control, 2018, 47, .	1.1	3
161	Mathematical Models of Visualization in SIEM Systems. SPIIRAS Proceedings, 2016, 3, 90.	0.8	3
162	ECU-Secure: Characteristic Functions for In-Vehicle Intrusion Detection. Studies in Computational Intelligence, 2020, , 495-504.	0.7	3

#	Article	IF	Citations
163	The Integrated Model of Secure Cyber-Physical Systems for Their Design and Verification. Studies in Computational Intelligence, 2020, , 333-343.	0.7	3
164	Application of Deep Learning Methods in Cybersecurity Tasks. Voprosy Kiberbezopasnosti, 2020, , 76-86.	0.1	3
165	Classification andÂAnalysis ofÂVulnerabilities inÂMobile Device Infrastructure Interfaces. Communications in Computer and Information Science, 2022, , 301-319.	0.4	3
166	Security Measuring System forÂIoT Devices. Lecture Notes in Computer Science, 2022, , 256-275.	1.0	3
167	Using Low-Level Dynamic Attributes for Malware Detection Based on Data Mining Methods. Lecture Notes in Computer Science, 2012, , 254-269.	1.0	2
168	Simulation of Protection Mechanisms Based on "Nervous Network System" against Infrastructure Attacks. , 2013, , .		2
169	Dynamical Attack Simulation for Security Information and Event Management. Lecture Notes in Geoinformation and Cartography, 2014, , 219-234.	0.5	2
170	Event analysis for security incident management on a perimeter access control system. , 2016, , .		2
171	Attack Graph-Based Countermeasure Selection Using a Stateful Return onÂInvestment Metric. Lecture Notes in Computer Science, 2018, , 293-302.	1.0	2
172	The Multi-Layer Graph Based Technique for Proactive Automatic Response Against Cyber Attacks. , 2018, , .		2
173	Genetic algorithms for role mining in critical infrastructure data spaces. , 2018, , .		2
174	Monitoring the State of Materials in Cyberphysical Systems: Water Supply Case Study. Materials Today: Proceedings, 2019, 11, 410-416.	0.9	2
175	Decomposition and Formulation of System of Features of Harmful Information Based on Fuzzy Relationships. , 2019, , .		2
176	An Approach to Intelligent Distributed Scanning and Analytical Processing of the Internet Inappropriate Information. , 2019, , .		2
177	The Visual Analytics Approach for Analyzing Trajectories of Critical Infrastructure Employers. Energies, 2020, 13, 3936.	1.6	2
178	Latest advances in parallel, distributed, and networkâ€based processing. Concurrency Computation Practice and Experience, 2020, 32, e5683.	1.4	2
179	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	2
180	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.	0.7	2

#	Article	IF	Citations
181	Hybrid Approach for Bots Detection in Social Networks Based on Topological, Textual and Statistical Features. Advances in Intelligent Systems and Computing, 2020, , 412-421.	0.5	2
182	A Semantic Model for Security Evaluation of Information Systems. Journal of Cyber Security and Mobility, 0, , .	0.7	2
183	Categorisation of web pages for protection against inappropriate content in the internet. International Journal of Internet Protocol Technology, 2017, 10, 61.	0.2	2
184	Use of neural networks for forecasting of the exposure of social network users to destructive impacts. Informatsionno-Upravliaiushchie Sistemy, 2020, , 24-33.	0.3	2
185	Simulation of Botnets: Agent-Based Approach. Studies in Computational Intelligence, 2010, , 247-252.	0.7	2
186	Application of Hybrid Neural Networks for Monitoring and Forecasting Computer Networks States. Lecture Notes in Computer Science, 2016, , 521-530.	1.0	2
187	Intelligent Security Analysis of Railway Transport Infrastructure Components on the Base of Analytical Modeling. Advances in Intelligent Systems and Computing, 2018, , 178-188.	0.5	2
188	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.	0.4	2
189	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.	0.4	2
190	Visualization-Driven Approach to Fraud Detection in the Mobile Money Transfer Services. Advances in Computer and Electrical Engineering Book Series, 2019, , 205-236.	0.2	2
191	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.	0.9	2
192	Intelligent support for network administrator decisions based on combined neural networks. , 2020, , .		2
193	Detection of Business Email Compromise Attacks with Writing Style Analysis. Communications in Computer and Information Science, 2022, , 248-262.	0.4	2
194	Multi-Aspect Based Approach to Attack Detection in IoT Clouds. Sensors, 2022, 22, 1831.	2.1	2
195	Towards Security Decision Support for large-scale Heterogeneous Distributed Information Systems. , 2021, , .		2
196	Design of Secure Microcontroller-Based Systems: Application to Mobile Robots for Perimeter Monitoring. Sensors, 2021, 21, 8451.	2.1	2
197	The Framework for Simulation of Bioinspired Security Mechanisms against Network Infrastructure Attacks. Scientific World Journal, The, 2014, 2014, 1-11.	0.8	1
198	Simulation of Bio-inspired Security Mechanisms against Network Infrastructure Attacks. Studies in Computational Intelligence, 2015, , 127-133.	0.7	1

#	Article	IF	Citations
199	The ontological approach application for construction of the hybrid security repository. , 2017, , .		1
200	Application of Image Classification Methods for Protection against Inappropriate Information in the Internet. , 2018, , .		1
201	Determination of Security Threat Classes on the basis of Vulnerability Analysis for Automated Countermeasure Selection. , 2018, , .		1
202	Hypergraph-driven mitigation of cyberattacks. Internet Technology Letters, 2018, 1, e38.	1.4	1
203	Automated Revealing of Organizational Assets Based on Event Correlation. , 2019, , .		1
204	Analysis of the Sensitivity of Algorithms for Assessing the Harmful Information Indicators in the Interests of Cyber-Physical Security. Electronics (Switzerland), 2019, 8, 284.	1.8	1
205	Network Protocols Determination Based on Raw Data Analysis for Security Assesment under Uncertainty. , 2019, , .		1
206	GRIDHPC: A decentralized environment for high performance computing. Concurrency Computation Practice and Experience, 2020, 32, e5320.	1.4	1
207	Stateful RORI-based countermeasure selection using hypergraphs. Journal of Information Security and Applications, 2020, 54, 102541.	1.8	1
208	Modelling attacks in self-organizing wireless sensor networks of smart cities. IOP Conference Series: Materials Science and Engineering, 2020, 971, 032077.	0.3	1
209	Combined Approach to Anomaly Detection in Wireless Sensor Networks on Example of Water Management System. , 2021, , .		1
210	Increasing the Reliability of Computer Network Protection System by Analyzing its Controllability Models. , 2021, , .		1
211	Towards Attacker Attribution for Risk Analysis. Lecture Notes in Computer Science, 2021, , 347-353.	1.0	1
212	Combining of Scanning Protection Mechanisms in GIS and Corporate Information Systems. Lecture Notes in Geoinformation and Cartography, 2011, , 45-58.	0.5	1
213	Combining spark and snort technologies for detection of network attacks and anomalies. , 2019, , .		1
214	Social networks bot detection using Benfordâ€™s law. , 2020, , .		1
215	Selection and Justification of Information Security Indicators for Materials Processing Systems. MATEC Web of Conferences, 2021, 346, 01019.	0.1	1
216	An Approach to Ranking the Sources of Information Dissemination in Social Networks. Information (Switzerland), 2021, 12, 416.	1.7	1

#	Article	IF	Citations
217	Agent-Based Simulation Environment And Experiments For Investigation Of Internet Attacks And Defense. , 2007, , .		1
218	Design of Entrusting Protocols for Software Protection. Lecture Notes in Geoinformation and Cartography, 2009, , 301-316.	0.5	1
219	Experiments With Simulation Of Botnets And Defense Agent Teams. , 2013, , .		1
220	Detection of Anomalous Activity in Mobile Money Transfer Services Using RadViz-Visualization. SPIIRAS Proceedings, 2016, 5, 32.	0.8	1
221	Fuzzy Adaptive Routing in Multi-service Computer Networks under Cyber Attack Implementation. Advances in Intelligent Systems and Computing, 2018, , 215-225.	0.5	1
222	An Automated Graph Based Approach to Risk Assessment for Computer Networks with Mobile Components. Communications in Computer and Information Science, 2018, , 95-106.	0.4	1
223	Methodology for disseminating information channels analysis in social networks. Vestnik Sankt-Peterburgskogo Universiteta, Prikladnaya Matematika, Informatika, Protsessy Upravleniya, 2018, 14, .	0.1	1
224	Correlation of Information in SIEM Systems based on Event Type Relation Graph. Informatsionno-Upravliaiushchie Sistemy, 2018, 1, 58-67.	0.3	1
225	Image Clustering Method based on Particle Swarm Optimization. , 0, , .		1
226	Voronoi Maps for Planar Sensor Networks Visualization. Communications in Computer and Information Science, 2019, , 96-109.	0.4	1
227	An approach for selecting countermeasures against harmful information based on uncertainty management. Computer Science and Information Systems, 2022, 19, 415-433.	0.7	1
228	Application of Deep Learning Methods in Cybersecurity Tasks. Part 2. Voprosy Kiberbezopasnosti, 2020, , 11-21.	0.1	1
229	COMBINED APPROACH TO INSIDER DETECTION ON COMPUTER NETWORKS. Vestnik Sankt-Peterburgskogo Gosudarstvennogo Universiteta Tehnologii I Dizajna SeriÄ¢ 1, Estestvennye I TehniÄeskie Nauki, 2020, , 66-71.	0.0	1
230	Software Environment for Simulation and Evaluation of a Security Operation Center. , 2007, , 111-127.		1
231	Security Policy Verification Tool for Geographical Information Systems. , 2007, , 128-146.		1
232	Detection of Stego-Insiders in Corporate Networks Based on a Hybrid NoSQL Database Model. , 2020, , .		1
233	Identification of the Traffic Model Parameters for Network and Cloud Platform Security Management. , 2020, , .		1
234	Construction and Analysis of Integral User-Oriented Trustworthiness Metrics. Electronics (Switzerland), 2022, 11, 234.	1.8	1

#	Article	IF	Citations
235	Detection andÂMonitoring ofÂtheÂDestructive Impacts inÂtheÂSocial Networks Using Machine Learning Methods. Communications in Computer and Information Science, 2021, , 60-65.	0.4	1
236	Privacy Policies of IoT Devices: Collection and Analysis. Sensors, 2022, 22, 1838.	2.1	1
237	An approach to formal desription of the user notification scenarios in privacy policies. , 2022, , .		1
238	Towards Resilient and Efficient Big Data Storage: Evaluating a SIEM Repository Based on HDFS. , 2022, , .		1
239	Vector-based Dynamic Assessment of Cyber-Security of Critical Infrastructures. , 2022, , .		1
240	Security and Privacy Analysis of Smartphone-Based Driver Monitoring Systems from the Developerâ€™s Point of View. Sensors, 2022, 22, 5063.	2.1	1
241	Antagonistic Agents in the Internet: Computer Network Warfare Simulation. , 2006, , .		0
242	Hybrid Multi-module Security Policy Verification. , 2007, , .		0
243	Multiagent simulation of protection of information resources in internet. Journal of Computer and Systems Sciences International, 2007, 46, 741-755.	0.2	0
244	Packet Level Simulation of Cooperative Distributed Defense against Internet Attacks. , 2008, , .		0
245	Message from iThings 2012 Program Co-chairs. , 2012, , .		0
246	Design and verification of protected systems with integrated devices based on expert knowledge. Automatic Control and Computer Sciences, 2015, 49, 648-652.	0.4	0
247	Message from Organizing Committee Chairs. , 2017, , .		0
248	Ontological Hybrid Storage for Security Data. Studies in Computational Intelligence, 2018, , 159-171.	0.7	0
249	Software Tool for Testing the Packet Analyzer of Network Attack Detection Systems. , 2018, , .		0
250	Formation of Indicators for Assessing Technical Reliability of Information Security Systems. , 2018, , .		0
251	Visual Analytics for Improving Efficiency of Network Forensics: Account Theft Investigation. Journal of Physics: Conference Series, 2018, 1069, 012062.	0.3	0
252	Message from Organizing Chairs. , 2018, , .		0

#	Article	IF	Citations
253	Detection of Weaknesses in Information Systems for Automatic Selection of Security Actions. Automatic Control and Computer Sciences, 2019, 53, 1029-1037.	0.4	0
254	Multi-criteria security assessment of control and diagnostic data on the technological processes. MATEC Web of Conferences, 2019, 298, 00071.	0.1	0
255	Approach to organizing of a heterogeneous swarm of cyber-physical devices to detect intruders. IFAC-PapersOnLine, 2019, 52, 945-950.	0.5	0
256	Methods of Assessing the Effectiveness of Network Content Processing Systems for Detecting Malicious Information9 Taking into Account the Elimination of Uncertainty in the Semantic Content of Information Objects. , 2019, , .		0
257	Optimizing Secure Information Interaction in Distributed Computing Systems by the Sequential Concessions Method. , 2020, , .		0
258	A Variant of the Analytical Specification of Security Information and Event Management Systems. Studies in Systems, Decision and Control, 2021, , 321-331.	0.8	0
259	Fuzzy Sets in Problems of Identification of Attacks on Wireless Sensor Networks. , 2021, , .		0
260	CONSTRUCTION OF MEMBERSHIP FUNCTIONS IN FUZZY SECURITY INFORMATION AND EVENT MANAGEMENT TASKS. MatematiÄeskie Metody V TehnologiÃ¢h I Tehnike, 2021, , 126-129.	0.0	0
261	Target functions of the conceptual model for adaptive monitoring of integrated security in material processing systems. Materials Today: Proceedings, 2021, 38, 1454-1458.	0.9	0
262	Detecting Anomalous Behavior of Users of Data Centers Based on the Application of Artificial Neural Networks. Lecture Notes in Computer Science, 2021, , 331-342.	1.0	0
263	INVESTIGATION OF COOPERATIVE DEFENSE AGAINST DDOS. , 2007, , .		0
264	Logical Inference Framework for Security Management in Geographical Information Systems. Lecture Notes in Geoinformation and Cartography, 2014, , 203-218.	0.5	0
265	Evolutionary Algorithms for Design of Virtual Private Networks. Studies in Computational Intelligence, 2018, , 287-297.	0.7	0
266	Applying Fuzzy Computing Methods for On-line Monitoring of New Generation Network Elements. Advances in Intelligent Systems and Computing, 2019, , 331-340.	0.5	0
267	Optimization of the cyber security system structure based on accounting of the prevented damage cost. , 2019, , .		0
268	Open challenges in visual analytics for security information and event management. Informatsionno-Upravliaiushchie Sistemy, 2019, , 57-67.	0.3	0
269	Adaptive Touch Interface: Application for Mobile Internet Security. Communications in Computer and Information Science, 2020, , 53-72.	0.4	0
270	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.	0.5	0

#	Article	IF	Citations
271	Towards Intelligent Data Processing for Automated Determination of Information System Assets. Advances in Information Security, Privacy, and Ethics Book Series, 2020, , 147-160.	0.4	0
272	Policy-Based Proactive Monitoring of Security Policy Performance. , 2007, , 197-212.		0
273	Event Calcululus Based Checking of Filtering Policies. , 2007, , 248-253.		0
274	Combined Neural Network for Assessing the State of Computer Network Elements. Studies in Computational Intelligence, 2021, , 256-261.	0.7	0
275	Situational Control of a Computer Network Security System in Conditions of Cyber Attacks. , 2021, , .		0
276	INTERVAL ANALYSIS OF THE SECURITY OF TELECOMMUNICATIONS RESOURCES OF CRITICAL INFRASTRUCTURES. MatematiÄeskie Metody V TehnologiÃ¢h I Tehnike, 2022, , 64-67.	0.0	0
277	Simulation-based and Graph oriented Approach to Detection of Network Attacks. , 2022, , .		0