Andrey Chechulin

List of Publications by Year
in descending order

68 papers	429 citations	1162367 8 h-index	1125271 13 g-index
77 all docs	77 docs citations	77 times ranked	180 citing authors

#	Article	IF	Citations
1	Common Framework for Attack Modeling and Security Evaluation in SIEM Systems. , 2012, , .		29
2	A Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded Components. , 2012, , .		23
3	Comparative Study of Machine Learning Methods for In-Vehicle Intrusion Detection. Lecture Notes in Computer Science, 2019, , 85-101.	1.0	19
4	Computer attack modeling and security evaluation based on attack graphs. , 2013, , .		18
5	Categorisation of web pages for protection against inappropriate content in the internet. International Journal of Internet Protocol Technology, 2017, 10, 61.	0.2	18
6	Fast Network Attack Modeling and Security Evaluation based on Attack Graphs. Journal of Cyber Security and Mobility, 2014, 3, 27-46.	0.7	16
7	Combined Design Technique for Secure Embedded Devices Exemplified by a Perimeter Protection System. SPIIRAS Proceedings, 2016, 5, 5.	0.8	14
8	SEPAD â€" Security Evaluation Platform for Autonomous Driving. , 2020, , .		13
9	Event correlation in the integrated cyber-physical security system. , 2016, , .		12
10	Analysis and Evaluation of Web Pages Classification Techniques for Inappropriate Content Blocking. Lecture Notes in Computer Science, 2014, , 39-54.	1.0	11
11	Security Metrics Based on Attack Graphs for the Olympic Games Scenario. , 2014, , .		9
12	Evaluation of text classification techniques for inappropriate web content blocking. , 2015, , .		9
13	Design lifecycle for secure cyber-physical systems based on embedded devices. , 2017, , .		9
14	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
15	Analytical attack modeling and security assessment based on the common vulnerability scoring system. , 2017, , .		8
16	A technique for design of secure data transfer environment: Application for I2C protocol. , 2018, , .		8
17	Design and Implementation of a Hybrid Ontological-Relational Data Repository for SIEM Systems. Future Internet, 2013, 5, 355-375.	2.4	7
18	AI- and Metrics-Based Vulnerability-Centric Cyber Security Assessment and Countermeasure Selection. Computer Communications and Networks, 2018, , 101-130.	0.8	7

#	Article	IF	Citations
19	Design and Verification Methodology for Secure and Distributed Cyber-Physical Systems. , 2019, , .		7
20	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
21	An Analysis of Security Event Correlation Techniques in Siem-Systems. Part 1. SPIIRAS Proceedings, 2016, 4, 5.	0.8	7
22	Access Control Visualization Using Triangular Matrices. , 2019, , .		6
23	In-Vehicle Situation Monitoring for Potential Threats Detection Based on Smartphone Sensors. Sensors, 2020, 20, 5049.	2.1	6
24	Camouflaged bot detection using the friend list. , 2021, , .		6
25	Problematic Issues of Information Security of Cyber-Physical Systems. Informatics and Automation, 2020, 19, 1050-1088.	0.6	6
26	Attack tree-based approach for real-time security event processing. Automatic Control and Computer Sciences, 2015, 49, 701-704.	0.4	5
27	Design of Integrated Vulnerabilities Database for Computer Networks Security Analysis. , 2015, , .		5
28	Generation of Source Data for Experiments with Network Attack Detection Software. Journal of Physics: Conference Series, 2017, 820, 012033.	0.3	5
29	An Approach for Network Information Flow Analysis for Systems of Embedded Components. Lecture Notes in Computer Science, 2012, , 146-155.	1.0	5
30	Threats Classification Method for the Transport Infrastructure of a Smart City. , 2020, , .		5
31	Application of a Technique for Secure Embedded Device Design Based on Combining Security Components for Creation of a Perimeter Protection System. , 2016, , .		4
32	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
33	Visual analysis of CAN bus traffic injection using radial bar charts. , 2018, , .		4
34	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.	1.8	4
35	Augmented reality for visualizing security data for cybernetic and cyberphysical systems. , 2020, , .		4
36	An Analysis of Security Event Correlation Techniques in SIEM-Systems. Part 2. SPIIRAS Proceedings, 2016, 6, 208.	0.8	4

#	Article	IF	Citations
37	Integrated Approach to Provide Security of Cyber-Physical Systems Based on Microcontrollers. Voprosy Kiberbezopasnosti, 2018, , 29-38.	0.1	4
38	Monitoring and Counteraction to Malicious Influences in the Information Space of Social Networks. Lecture Notes in Computer Science, 2018, , 159-167.	1.0	4
39	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
40	An Ontology-based Storage of Security Information. Information Technology and Control, 2018, 47, .	1.1	3
41	Mathematical Models of Visualization in SIEM Systems. SPIIRAS Proceedings, 2016, 3, 90.	0.8	3
42	ECU-Secure: Characteristic Functions for In-Vehicle Intrusion Detection. Studies in Computational Intelligence, 2020, , 495-504.	0.7	3
43	The Integrated Model of Secure Cyber-Physical Systems for Their Design and Verification. Studies in Computational Intelligence, 2020, , 333-343.	0.7	3
44	Classification andÂAnalysis ofÂVulnerabilities inÂMobile Device Infrastructure Interfaces. Communications in Computer and Information Science, 2022, , 301-319.	0.4	3
45	Threats Detection during Human-Computer Interaction in Driver Monitoring Systems. Sensors, 2022, 22, 2380.	2.1	3
46	Dynamical Attack Simulation for Security Information and Event Management. Lecture Notes in Geoinformation and Cartography, 2014, , 219-234.	0.5	2
47	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
48	Categorisation of web pages for protection against inappropriate content in the internet. International Journal of Internet Protocol Technology, 2017, 10, 61.	0.2	2
49	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
50	Multi-Aspect Based Approach to Attack Detection in IoT Clouds. Sensors, 2022, 22, 1831.	2.1	2
51	Design of Secure Microcontroller-Based Systems: Application to Mobile Robots for Perimeter Monitoring. Sensors, 2021, 21, 8451.	2.1	2
52	The ontological approach application for construction of the hybrid security repository. , 2017, , .		1
53	Application of Image Classification Methods for Protection against Inappropriate Information in the Internet. , 2018, , .		1
54	Cyberattack detection in vehicles using characteristic functions, artificial neural networks, and visual analysis. Informatics and Automation, 2021, 20, 845-868.	0.6	1

#	Article	IF	Citations
55	Overview of Vulnerabilities of Decision Support Interfaces Based on Virtual and Augmented Reality Technologies. Lecture Notes in Networks and Systems, 2022, , 400-409.	0.5	1
56	Combining of Scanning Protection Mechanisms in GIS and Corporate Information Systems. Lecture Notes in Geoinformation and Cartography, 2011, , 45-58.	0.5	1
57	Social networks bot detection using Benfordâ€™s law. , 2020, , .		1
58	Use of Adaptive Touch Interface in Information Security Applications. Voprosy Kiberbezopasnosti, 2020, , 18-28.	0.1	1
59	An Approach to Ranking the Sources of Information Dissemination in Social Networks. Information (Switzerland), 2021, 12, 416.	1.7	1
60	Methodology for disseminating information channels analysis in social networks. Vestnik Sankt-Peterburgskogo Universiteta, Prikladnaya Matematika, Informatika, Protsessy Upravleniya, 2018, 14, .	0.1	1
61	Voronoi Maps for Planar Sensor Networks Visualization. Communications in Computer and Information Science, 2019, , 96-109.	0.4	1
62	Unmanned Transport Environment Threats. Smart Innovation, Systems and Technologies, 2021, , 395-408.	0.5	1
63	Active learning approach for inappropriate information classification in social networks. , 2022, , .		1
64	Security and Privacy Analysis of Smartphone-Based Driver Monitoring Systems from the Developerâ€™s Point of View. Sensors, 2022, 22, 5063.	2.1	1
65	Ontological Hybrid Storage for Security Data. Studies in Computational Intelligence, 2018, , 159-171.	0.7	0
66	Visual Analytics for Improving Efficiency of Network Forensics: Account Theft Investigation. Journal of Physics: Conference Series, 2018, 1069, 012062.	0.3	0
67	Approach to organizing of a heterogeneous swarm of cyber-physical devices to detect intruders. IFAC-PapersOnLine, 2019, 52, 945-950.	0.5	0
68	Adaptive Touch Interface: Application for Mobile Internet Security. Communications in Computer and Information Science, 2020, , 53-72.	0.4	0