SERGEI CHUPROV

https://faculty.utrgv.edu/sergei.chuprov/

Google Scholar **LinkedIn**

Email: sergei.chuprov@utrgv.edu

PhD in Computing and Information Sciences

University of Texas Rio Grande Valley (UTRGV), Edinburg, TX

RESEARCH AREA

Artificial Intelligence and Machine Learning Systems, Robustness of Intelligent Systems and their Practical Applications, Cybersecurity, Data Quality and Security Evaluation and Analytics

HIGHLIGHTS

- 48 peer-reviewed publications, 2 pending patent applications, Google Scholar $\boldsymbol{h}$-index: 8.
- My publication list includes renowned peer-reviewed conferences and journals, such as IEEE ICC, IEEE Systems journal, IEEE CEC, IEEE WCCI, IEEE INFOCOM (CNERT Workshop), and others.
- I have a valuable experience participating in R&D projects supported by NSF, DoD (USMA), CRDF Global, and other funding agencies.
- I received multiple grants and scholarships awarded for the excellence demonstrated in research and education.
- I have 6+ years of Graduate Research and Teaching Assistant experience, mentoring and advising students in various institutions and countries.

EDUCATION

PhD in Computing and Information Sciences
Rochester Institute of Technology (RIT), NY, USA *August 2021 - May 2024*
Department of Computer Science and Department of Cybersecurity **GPA:** 3.83/4.0
Thesis: Robust Machine Learning Under Vulnerable Cyberinfrastructure and Varying Data Quality

Master's in Information Security
Saint-Petersburg National Research University of *September 2017 - June 2019*
Information Technologies, Mechanics and Optics (ITMO), Russia **GPA:** 4.0/4.0 (with honors)
Faculty of Secure Information Technologies
Thesis: Assurance of Information in a Mobile Robotic System with Decentralized Control

Bachelor's in Information Security
ITMO University, Saint Petersburg, Russia *September 2013 - June 2017*
Faculty of Secure Information Technologies **GPA:** 3.5/4.0
Thesis: Vulnerability Analysis and Classification in Local Networks Based on Microsoft OS Family

ACADEMIC WORK & TEACHING EXPERIENCE

Department of Computer Science, UTRGV
Edinburg, TX, USA *September 2024 - present*
Assistant Professor (tenure-track)
Scope & Responsibilities: teach undergraduate and graduate courses, conduct research in AI/ML security and robustness, and contribute to departmental and university service activities.

B. Thomas Golisano College of Computer Science, RIT
Rochester, NY, USA *August 2021 - July 2024*
Graduate Research Assistant (part-time)
Scope & Responsibilities: research and development in the area of Artificial Intelligence- and Machine Learning-based systems security, Data Quality and Security Assurance, Robustness of Machine Learning-end Systems. **Results:** 2 pending patent applications; more than 15 published papers in refereed journals and conference proceedings (see Publication List below).

B. Thomas Golisano College of Computer Science, RIT
Rochester, NY, USA *August 2022 - July 2024*
Graduate Teaching Assistant (part-time)
Scope & Responsibilities: assisting the course instructor in teaching Computer Science-related courses. **Results:** gained teaching activities experience and knowledge related to building effective communication with the students; holding office hours and grading assignments for the classes of 20 undergraduate and graduate students; providing constructive feedback and communicating students' questions and concerns related to the course content and assignments; supervised student capstone projects and mentored them. **Courses:**

- CSCI-735 Foundations of Intelligent Security Systems (instructor: Dr. Leon Reznik)
- CSCI-536 Information Retrieval, undergraduate section (instructor: Dr. Richard Zanibbi)
- CSCI-636 Information Retrieval, graduate section (instructor: Dr. Richard Zanibbi)

Mobile Intelligent Systems Laboratory, ETU "LETI" University
Saint Petersburg, Russia *May 2021 - August 2021*
Researcher (part-time)
Scope & Responsibilities: research and development in the area of Cyber-Physical Systems security and safety, Intelligent Systems security. Lead a group of 4 developers and engineers; developed models and software tools for Reputation and Trust-based simulation environment to model communication in decentralized IoT networks; applied the developed models and tools on a real-world IoT hardware devices; developed projects' reports and technical documentation. **Results:** 7 published papers in refereed journals and conference proceedings (see Publication List below).

Department of Secure Information Technologies, ITMO University
Saint Petersburg, Russia *September 2019 - May 2021*
Teaching Assistant (part-time)
Scope & Responsibilities: assisting the course instructor in teaching undergraduate and graduate courses in the areas of Information Security and Computer Science. **Results:** gained experience in teaching laboratory and practical sessions for the classes of 10-20 undergraduate and graduate students; holding office hours and communicating students' questions and concerns; developed and graded assignments for the selected courses; assisted in developing the coursework content for the "Functional Security and Safety Assurance in Autonomous Vehicles" Master's degree program, established at ITMO in 2019. **Courses:**

- Foundations of Information Technology (instructor: Dr. Ilia Viksnin)
- Introduction to Imitation Modeling (instructor: Dr. Igor Komarov)
- Information Security Technology and Methodology (instructor: Dr. Victoria Korzhuk)
- Foundations of Autonomous Vehicles Safety (instructor: Dr. Ilia Viksnin)
- Autonomous Vehicles Imitation Modeling (instructor: Dr. Cyril Pshenichny)

Department of Secure Information Technologies, ITMO University
Saint Petersburg, Russia *May 2018 - May 2021*
Researcher (part-time)
Scope & Responsibilities: research and development in the area of Information Security, Multi-Agent Mobile Robotic Systems Security, Knowledge Representation in Intelligent Systems. **Results:** developed security and safety models and methods for decentralized and multi-agent mobile robotic systems (see Projects below); developed security-inspired smart factory models in AnyLogic simulation environment; 14 publications in refereed journals and conference proceedings (see Publication List below).

PROJECTS

Collaborative research: IDEAS lab: ETAUS: Smarter Microbial Observatories for Realtime ExperimentS (SMORES) (participant)

August 2023 - Present

- **Objective:** this recently started project involves the collaboration between RIT, Harvard University, Florida International University, and the University of Georgia to study marine sediments and their role in natural carbon sequestration, using AI and ML to optimize data collection and predictions during field experiments. The project is supported by NSF award #2321652.

Enhancing Security and Privacy of the Conventional Federated Learning (participant)
September 2022 - Present

- **Objective:** to develop methods and software tools aimed at detecting compromised and failed local units in the Federated Learning and excluding them from the aggregation. **Results:** 4 published papers [C1,C2,C9,C10]; 1 pending patent application [P1]; and 6 poster and other presentations [NP2,NP3,NP5-NP8]. The project is supported by the United States Military Academy (USMA) and is accomplished under Grant Number W911NF-20-1-0337.

Developing Methods and Tools for Machine Learning Robustness Assurance under Vulnerable Cyber-infrastructure and Varying Data Quality (participant) *May 2022 - April 2024*

- **Objective:** to develop system integration methods and tools for providing feedback to the Machine Learning system cyberinfrastructure components in order to enhance Machine Learning robustness to input Data Quality variations. **Results:** 1 pending patent application [P2]; 8 published papers [C5,C6,C11-C16]. The project was supported by the grant from the U.S. Civilian Research & Development Foundation (CRDF Global) with funding from the United States Department of State.

Partisan Telegram Application and Operational Security Assessment (participant)
February 2022 - July 2022

- **Objective:** to conduct comprehensive security evaluation of the Partisan Telegram Android application. **Results:** developed an open-source report on comprehensive security assessment of the Partisan Telegram Android OS application; conducted functional analysis of the application's source code; investigated and verified vulnerabilities that jeopardized user's privacy. The project was supported by the Open Technology Fund.

Enhancing Sensor Network Security with Reputation and Trust-Based Technique (group leader)
May 2021 - August 2021

- **Objective:** to develop methods and software tools aimed at detecting malicious nodes in sensor networks using Reputation and Trust indicators. **Results:** developed software and hardware tools that allows: modeling the communication between real sensor devices; modeling malicious attacks against the quality of the communicated data; verifying the effectiveness of the developed security solutions. 2 published papers [C18,O1]. The project was supported by the Ministry of Science and Higher Education of the Russian Federation, #075-01024-21-02 dated 29.09.2021 (project FSEE-2021-0014)

Development of Hardware and Software Modules for Critical Objects Monitoring over the Conditions of Uncertainty and Data Incompleteness for Malicious Attacks Prevention and Mitigation, *Industrial partnership project* (participant) *September 2019 - October 2020*

- **Objective:** to develop software methods and tools implemented on sensor-equipped hardware modules aimed at monitoring and detecting hazardous environmental events in the conditions of malicious attacks. **Results:** developed intelligent security evaluation models, risk evaluation models and methods, and software and hardware prototypes, implemented by Murmansk Commercial Seaport OAO, Russia. The work was supported by the Ministry of Science and Higher Education of the Russian Federation under the agreement No. 05.605.21.0189.

Development of a Quantum Secure Hybrid Platform for Distributed Cyber-Physical Systems Control (participant) *May 2018 - August 2019*

- **Objective:** to develop methods and tools aimed at assuring data security and confidentiality in a group of autonomous mobile robotic devices equipped with quantum key generation facilities. **Results:** developed Multi-Agent based security models and methods for mobile robotic system equipped with quantum key generation facilities, and mobile robotic devices prototypes, implemented at ITMO University for further research and educational purposes. The work was financially supported by the Government of Russian Federation, Grant 074-U01.

Development of Experimental Testbed for Smart City Control and Security Algorithms Research and Verification (participant) *May 2018 - March 2019*

- **Objective:** to develop physical testbed for conducting real-world empirical verification of the developed IoT security solutions deployed in decentralized systems, such as Intelligent Transportation Systems. **Results:** developed physical testbed equipped with IoT communication facilities and 10 autonomous vehicle models for

security and optimization algorithms verification. Published 8 papers [J7,J8,C23,C25-C29]. The video of the developed testbed can be found in a public access: URL.

GRANT PROPOSAL WRITING EXPERIENCE

Amazon AWS Cloud Credit for Research, "Empirical Study of Industrial Machine Learning End Systems Robustness to Data Quality Degradation", PI *2022*
Supported, $4,000 in AWS credits awarded.
Summary of contributions: developed research motivation and problem description, formulated research questions, developed research agenda, developed specification and empirical study design.

Ministry of Science and Higher Education of the Russian Federation (#05.605.21.0189), "Development of Hardware and Software Modules for Critical Objects Monitoring over the Conditions of Uncertainty and Data Incompleteness for Malicious Attacks Prevention and Mitigation", neither PI or Co-PI (Research Assistant) *2019*
Supported, $500,000 awarded.
Summary of contributions: developed sections related to risk management models, created figures, performed editing.

GRANTS AND AWARDS

IEEE CAI 2023 Student Conference Grant *June 2023*
Santa Clara, CA, USA.

Gold Medal (1st prize) for the poster presented at the UPSTAT 2023 conference *April 2023*
Rochester, NY, USA.

NSF grant for participation in POWDER Mobile and Wireless Week 2023 *January 2023*
Salt Lake City, UT, USA

Amazon AWS Cloud Credit for Research, awarded for one year *August 2022*
Rochester, NY, USA

Saint-Petersburg's Academic and Industrial Institutions Students' Grant *(2): 2019, 2022*
Saint-Petersburg, Russia

IEEE INFOCOM 2022 Student Conference Grant *May 2022*
London, UK

Rochester Institute of Technology PhD Research and Tuition Scholarship *(3): 2021-2023*
Rochester, NY, USA

Scholarship of the Russian Federation President for Students of Higher Education Universities Studying Abroad in 2021/2022 Academic Year *May 2021*
Saint-Petersburg, Russia

Scholarship of the Russian Federation President and Government for the Students of Priority Education Directions *(2): 2021, 2022*
Saint-Petersburg, Russia

ITMO University's Best Student's Research MS Thesis Award *August 2019*
Saint-Petersburg, Russia

Scholarship of the Russian Federation Government *September 2019*
Saint-Petersburg, Russia

INVITED TALKS & SESSIONS

Invited Talk (remote) at From Theory to Practice (T2P) Worshop, Kigali, Rwanda *16 April 2024*
Title: *Security and Robustness of Machine Learning under Vulnerable Cyberinfrastructure and Varying Data Quality*

Invited Session at UPSTAT 2024 Conference, NY, USA *13 April 2024*
Title: *Improving Federated Learning Robustness towards Security Violations and Data Quality Degradations OR How to Learn Better via Extracting Knowledge and Accumulating History?*
Organized together with Dr. Leon Reznik and Raman Zatsarenko (PhD student, RIT)

SERVICE, VOLUNTEERING & MENTORING EXPERIENCE

◇ ACADEMIC SERVICE:

Journal of Data and Information Quality
Reviewed 1 manuscript

IEEE World Congress on Computational Intelligence (WCCI) 2024: The International Joint Conference on Neural Networks (IJCNN)
Reviewed 4 manuscripts

The 30th International Conference on Neural Information Processing (ICONIP 2023)
Reviewed 2 manuscripts

◇ VOLUNTEERING:

GENIUS Olympiad
Rochester Institute of Technology, NY, USA *(2): 2023, 2024*
Volunteer Judge
Evaluated and graded 12 science projects (each year) presented at 2023 and 2024 GENIUS Olympiad. Provided constructive feedback on the projects and presentations to the participants.

◇ STUDENT MENTORING:

Harshil Pravinbhai Patel, MS
Rochester Institute of Technology, NY, USA *2024*
MS capstone project: "Improving Federated Learning Security with Trust Evaluation to Detect Adversarial Attacks"

Shweta Sandip Sharma, MS
Rochester Institute of Technology, NY, USA *2024*
MS capstone project: "Analyzing Effects of Adversarial Attacks on Classifier Performance"

Gaurav Thakur, MS
Rochester Institute of Technology, NY, USA *2024*
MS capstone project: "Resilience of Federated Learning Models in Image Classification Under Data Degradation"

Vedika Vishwanath Painjane, MS
Rochester Institute of Technology, NY, USA *2024*
MS capstone project: "Analyzing the Effect of Data Poisoning on Semantic Segmentation Using Federated Learning"

Anirudh Narayanan, MS
Rochester Institute of Technology, NY, USA *2024*
MS capstone project: "Soccer Games Automatic Video Highlights Generator", [GitHub]

Moinuddin Memon, MS
Rochester Institute of Technology, NY, USA *2023*
MS capstone project: "Knowledge-Based Client Filtering Algorithm for Federated Learning" (see [C10])

Ilya Sakhno, BS
ITMO University, Saint Petersburg, Russia *2021*
BS qualification project: "Unified Security Profile for Contactless Payment Technology"

Egor Marinenkov, BS
ITMO University, Saint Petersburg, Russia *2020*
BS qualification project: "Detecting Data Integrity Violations in Cyber-Physical Systems using Game Theory Approach" (see [J5] and [C31])

ADDITIONAL RESEARCH EXPERIENCE

Summer research program in Cybersecurity under the supervision of Dr. Leon Reznik
RIT, NY, USA *June 2019 - August 2019*
Results: 3 published papers [J6,C19,C20] related to security and safety assurance in a group of autonomous vehicles

with Reputation, Trust, and Data Quality indicators.

ADDITIONAL TRAINING COURSES

"Graduate Teaching Assistant Foundations" training
RIT, Rochester, NY *December 2022*
Online training included 3 modules that covered: strategies and resources for supporting academic integrity; ways to ensure equitable opportunities for students; digital tools for classroom learning goals; instructions on identifying and responding to microaggressions in the classroom, and other topics.

Online intensive course: "Blended Learning: Digital Teaching Competencies"
ITMO University, Saint Petersburg, Russia *24 - 29 August 2020*
72 hours of online intensive lectures, practice, and master-classes with a final project defense. Confirmed by a state-recognized certificate.

In-person intensive course: "Foundations of Public Speaking in the 21st Century"
ITMO University, Saint Petersburg, Russia *13 March - 24 April 2019*
72 hours of intensive lectures, practice, and master-classes with final public-speaking project defense. Confirmed by a state-recognized certificate.

SKILLS & TOOLS

Modeling & Analysis	Python Libraries (NumPy, pandas, scikit-learn, etc), Matlab, AnyLogic, IBM SPSS, Network Simulator (2,3), Simulator of Urban Mobility (SUMO), CARLA
Deep Learning & Computer Vision	Python Frameworks (TensorFlow, PyTorch, Keras, Flower)
Software Development	Python, C/C++, Git

MEDIA

Related publications in social media:

◇ ITMO's R&D Project Results and Their Applications: URL

REFEREES

Dr. Leon Reznik, advisor, Professor of Computer Science (primary affiliation) and Computing Security (secondary affiliation) at RIT, NY. **Email:** leon.reznik@rit.edu

Dr. Richard Zanibbi, Professor of Computer Science and Director of the Document and Pattern Recognition Lab at RIT, NY. **Email:** rxzvcs@rit.edu

Dr. Roman Yampolskiy, Associate Professor of Computer Science and Engineering and Director of Cyber Security Laboratory in Speed School of Engineering, University of Louisville, KY. **Email:** roman.yampolskiy@louisville.edu

Dr. Ivan De Oliveira Nunes, Assistant Professor of Cybersecurity at RIT, NY. **Email:** ivanoliv@mail.rit.edu

PUBLICATION LIST

PATENTS

[P1] Chuprov, S., & Reznik, L. "Federated Learning with A Compromised Unit Exclusion from Receiving Global Model Updates".

Provisional application filed on January 13, 2023. Converted to non-provisional

[P2] Chuprov, S., & Reznik, L. "Network Adjustment based on Machine Learning End System Performance Monitoring Feedback".

Provisional application filed on September 14, 2022. Converted to non-provisional

REPRINTS

[R1] **Chuprov, S.**, Belyaev, P., Gataullin, R., Reznik, L., Neverov, E., & Viksnin, I. (2024) "Robust Autonomous Vehicle Computer-Vision-Based Localization in Challenging Environmental Conditions" in Applied Sciences. 2024, pp. 34-48., doi: doi.org/10.3390/books978-3-7258-2184-6. *Reprint of the Special Issue "Challenges in the Guidance, Navigation and Control of Autonomous and Transport Vehicles" that was published in Applied Sciences in 2023.* URL

REFEREED JOURNAL PUBLICATIONS

[J1] **Chuprov, S.**, Zatsarenko, R., Reznik, L., & Khokhlov, I. (2024). "Data Quality Based Intelligent Instrument Selection with Security Integration" in ACM Journal of Data and Information Quality. 2024, vol. 16, no. 3, pp. 1-24. doi: 10.1145/3695770. URL. **Q2**.

[J2] **Chuprov, S.**, Belyaev, P., Gataullin, R., Reznik, L., Neverov, E., & Viksnin, I. (2023). "Robust Autonomous Vehicle Computer-Vision-Based Localization in Challenging Environmental Conditions" in Applied Sciences. 2023, no. 13(9):5735. doi: 10.3390/app13095735. URL. **Q1**. *Published in Special Issue*

[J3] Berezovskaya, O., **Chuprov, S.**, Neverov, E., & Sadreev, E. (2023). "Review and Comparison of Lightweight Modifications of the AES Cipher for a Network of Low-Power Devices" in Automatic Control and Computer Sciences. 2022, no. 56, pp. 994-1006. doi: 10.3103/S0146411622080028. URL

[J4] Melnikov, T., **Chuprov, S.**, Lazarev, E., Gataullin, R., & Viksnin, I. (2022). "Improving Reputation and Trust-Based Approach with Reliability Indicators for Autonomous Vehicles Intergroup Communication" in Tomsk State University Journal of Control and Computer Science. 2022, no. 61, pp. 108-117. URL

[J5] Marinenkov, E., **Chuprov, S.**, Tursukov, N., Kim, I., & Viksnin, I. (2022). "Study on Destructive Informational Impact in Unmanned Aerial Vehicles Intergroup Communication" in Symmetry. 2022. Vol. 14, no. 8, pp. 1-18. URL. **Q2**. *Published in Special Issue*

[J6] Viksnin, I., Marinenkov, E., & **Chuprov, S.** (2022). "A Game Theory approach for communication security and safety assurance in cyber-physical systems with Reputation and Trust-based mechanisms" in Scientific and Technical Journal of Information Technologies, Mechanics and Optics, vol. 22, no. 1, pp. 47–59. doi: 10.17586/2226-1494-2022-22-1-47-59. URL

[J7] Khokhlov, I., Reznik, L., & **Chuprov, S.** (2020). "Framework for Integral Data Quality and Security Evaluation in Smartphones" in IEEE Systems Journal, vol. 15, no. 2, pp. 2058-2065, doi: 10.1109/JSYST.2020.2985343. URL. **Q1**

[J8] **Chuprov, S.**, Viksnin, I., Kim, I., Tursukov, N., & Nedosekin, G. (2020). Empirical Study on Discrete Modeling of Urban Intersection Management System. International Journal of Embedded and Real-Time Communication Systems (IJERTCS), vol. 11(2), pp. 16-38, doi: 10.4018/IJERTCS.2020040102. URL

[J9] **Chuprov, S.**, Viksnin, I., Kim, I., Marinenkov, E., Usova, M., Lazarev, E., Melnikov, T., & Zakoldaev, D. (2019). Reputation and Trust Approach for Security and Safety Assurance in Intersection Management System. Energies, 12(23), 4527, doi: 10.3390/en12234527. URL. **Q1**

REFEREED CONFERENCES' PROCEEDINGS AND PRESENTATIONS

[C1] Narayanan, A., **Chuprov, S.**, Reznik, L., Zatsarenko, R., & Korobeinikov, D. "Intelligent Soccer Event Detection and Highlights Generation with Broadcast Cues Integration" in 23rd International Conference on Machine Learning and Applications (ICMLA'24). *Accepted for presentation and publication. Will be published after December 2024*

[C2] Patel, H., **Chuprov, S.**, Korobeinikov, D., Zatsarenko, R., & Reznik, L. (2024). "Improving Federated Learning Security with Trust Evaluation to Detect Adversarial Attacks" in 19th Annual Symposium on Information Assurance (ASIA' 24), 2024, pp. 37-43. URL

[C3] Korobeinikov, D., **Chuprov, S.**, Zatsarenko, R., & Reznik, L., (2024). "Federated Learning Robustness on Real World Data in Intelligent Transportation Systems" in 19th Annual Symposium on Information Assurance (ASIA' 24), 2024, pp. 30-36. URL

[C4] **Chuprov, S.**, Zatsarenko, R., Korobeinikov, D., & Reznik, L. (2024). "Robust Training on the Edge: Federated vs. Transfer Learning for Computer Vision in Intelligent Transportation Systems" in 2024 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, 2024, pp. 172-178, doi: 10.1109/AIIoT61789.2024.10578970. URL

[C5] Zatsarenko, R., **Chuprov, S.**, Korobeinikov, D., & Reznik, L. (2024). "Trust-Based Anomaly Detection in Federated Edge Learning" in 2024 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, 2024, pp. 273-279, doi: 10.1109/AIIoT61789.2024.10578967. URL

[C6] Kovtun R., **Chuprov, S.**, Gataullin, R., Ruchkan, A., Alhasan, A., & Viksnin, I. (2024). "A Modern Approach to High Dynamic Range Image Processing with Machine Learning Architectures" in 2024 XXVII International Conference on Soft Computing and Measurements (SCM), 2024, pp. 207-212, doi: 10.1109/SCM62608.2024.10554097. URL

[C7] Garifullin M., Turushev, T., Tursukov, N., & **Chuprov, S.** (2024). "Extended Formulation of the Problem of Terrain Exploration using a Multi-agent System" in 2024 XXVII International Conference on Soft Computing and Measurements (SCM), 2024, pp. 207-212, doi: 10.1109/SCM62608.2024.105
54236. URL

[C8] **Chuprov, S.**, Mahajan, S., Zatsarenko, R., Reznik, L. & Ruchkan, A. (2023). "Are Industrial ML Image Classifiers Robust to Withstand Adversarial Attacks on Videos?" in 2023 IEEE Western New York Image and Signal Processing Workshop (WNYISPW), 2023, pp. 1-4, doi: 10.1109/WNYISPW60588.2023.10349595. URL

[C9] Zatsarenko, R., **Chuprov, S.**, Marathe, C.A., Hyland, M., & Reznik, L. (2023). "Are Industrial ML Image Classifiers Robust to Data Affected by Network QoS Degradation?" in 2023 IEEE Western New York Image and Signal Processing Workshop (WNYISPW), 2023, pp. 1-4, doi: 10.1109/WNYISPW60588.2023.10349560. URL

[C10] Neverov, E., Viksnin, I., & **Chuprov, S.** (2023) "The Research of AutoML Methods in the Task of Wave Data Classification" in 2023 XXVI International Conference on Soft Computing and Measurements (SCM), 2023, pp. 156-158, doi: 10.1109/SCM58628.2023.10159058. URL

[C11] Tursukov N., Viksnin I., Neverov E., Sheinman E., & **Chuprov S.** (2023) "Evaluation of the Effectiveness of Neural Networks Based on the Criteria for Completing the Object Classification Task" in 2023 XXVI International Conference on Soft Computing and Measurements (SCM), 2023, pp. 120-122, doi: 10.1109/SCM58628.2023.10159070. URL

[C12] **Chuprov, S.**, Bhatt, K.M., & Reznik, L. (2023). "Federated Learning for Robust Computer Vision in Intelligent Transportation Systems" in 2023 IEEE Conference on Artificial Intelligence (CAI), Santa Clara, CA, USA, 2023, pp. 26-27, doi: 10.1109/CAI54212.2023.00019. URL

[C13] **Chuprov, S.**, Memon, M., & Reznik, L. (2023). "Federated Learning with Trust Evaluation for Industrial Applications" in 2023 IEEE Conference on Artificial Intelligence (CAI), Santa Clara, CA, USA, 2023, pp. 347-348, doi: 10.1109/CAI54212.2023.00153. URL

[C14] **Chuprov, S.**, Reznik, L., & Grigoryan, G. (2022). "Study on Network Importance for ML End Application Robustness" ICC 2023 - IEEE International Conference on Communications, Rome, Italy, 2023, pp. 6627-6632, doi: 10.1109/ICC45041.2023.10279698. URL

[C15] **Chuprov, S.**, Satam, A. N., & Reznik, L. (2022). "Are ML Image Classifiers Robust to Medical Image Quality Degradation?" in 2022 IEEE Western New York Image and Signal Processing Workshop (WNYISPW), 2022, pp. 1-4, doi: 10.1109/WNYISPW57858.2022.9983488. URL

[C16] **Chuprov, S.**, Khokhlov, I., Reznik, L., & Manghi, K. (2022). "Multi-Modal Sensor Selection with Genetic Algorithms" in 2022 IEEE Sensors, 2022, pp. 1-4, doi: 10.1109/SENSORS52175.2022.9967296. URL

[C17] Khokhlov, I., **Chuprov, S.**, & Reznik, L. (2022). "Integrating Security with Accuracy Evaluation in Sensors Fusion" in 2022 IEEE Sensors, 2022, pp. 1-4, doi: 10.1109/SENSORS52175.2022.9967235. URL

[C18] **Chuprov, S.**, Khokhlov, I., Reznik, L., & Shetty, S. (2022). "Influence of Transfer Learning on Machine Learning Systems Robustness to Data Quality Degradation" in 2022 International Joint Conference on Neural Networks (IJCNN 2022), 2022, pp. 1-8, doi: 10.1109/IJCNN55064.2022.9892247. URL

[C19] **Chuprov, S.**, Reznik, L., Obeid, A., & Shetty, S. (2022). "How Degrading Network Conditions Influence Machine Learning End Systems Performance?" in IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2022, pp. 1-6, doi: 10.1109/INFOCOMWKSHPS54753.2022.9798388. URL

[C20] **Chuprov, S.**, Gataullin, R., Neverov, E., Belyaev, P., Kim, I., & Viksnin, I. (2022). "Police Office Model Performance and Security Evaluation in a Simulated Group of Mobile Robots" in The 5th International Conference on Future Networks & Distributed Systems (ICFNDS 2021). Association for Computing Machinery, New York, NY, USA, pp. 606–615, doi: 10.1145/3508072.3508195. URL

[C21] **Chuprov, S.**, Viksnin, I., Kim, I., Melnikov, T., Reznik, L., & Khokhlov, I. (2021). "Improving Knowledge Based Detection of Soft Attacks Against Autonomous Vehicles with Reputation, Trust and Data Quality Service Models" in 2021 IEEE International Conference on Smart Data Services (SMDS), pp. 115-120. URL

[C22] Domnitsky, E., Mikhailov, V., Zoloedov, E., Alyukov, D., **Chuprov, S.**, Marinenkov, E., & Viksnin, I. (2021). "Software Module for Unmanned Autonomous Vehicle's On-board Camera Faults Detection and Correction" in CEUR Workshop Proceedings, Vol. 2893, pp. 1-10. URL

[C23] Lyakhovenko, Y., Viksnin, I., & **Chuprov, S.** (2021). "Integrating Smart Contracts into Smart Factory Elements' Informational Interaction Model" in CEUR Workshop Proceedings, Vol. 2893, pp. 1-6. URL

[C24] Usova, M., Viksnin, I., & **Chuprov, S.** (2021). "Informational Messages and Space Models Application in Smart Factory Concept" in CEUR Workshop Proceedings, Vol. 2893, pp. 1-8. URL

[C25] Khanh, T.D., Komarov, I., Don, L.D., Iureva, R., & **Chuprov, S.** (2020). "TRA: Effective Authentication Mechanism For Swarms Of Unmanned Aerial Vehicles" in 2020 IEEE Symposium Series on Computational Intelligence, pp. 1852-1858, doi: 10.1109/SSCI47803.2020.
9308140. URL

[C26] Melnikov, T., Lazarev, E., Berezovskaya, O., **Chuprov, S.**, & Viksnin, I. (2020). "Empirical Study on Premises Monitoring Algorithm Implementation in Mobile Robotic System" in The International Conference "Nonlinearity, Information and Robotics", pp. 1-6, doi: 10.1109/NIR50484.2020.9290188. URL

[C27] Usova, M., **Chuprov, S.**, & Viksnin, I. (2020). "Informational Space and Messages Interaction Models for Smart Factory Concept" in 2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT, pp. 617-621, doi: 10.1109/MetroInd4.0IoT48571.2020.9138292. URL

[C28] **Chuprov, S.**, Marinenkov, E., Viksnin, I., Reznik, L., & Khokhlov, I (2020). "Image Processing in Autonomous Vehicle Model Positioning and Movement Control" in IEEE 6th World Forum on Internet of Things (WF-IoT) Proceedings, pp. 1-6, doi: 10.1109/WF-IoT48130.2020.9221258. URL

[C29] **Chuprov, S.**, Viksnin, I., Kim, I., Reznik, L., & Khokhlov, I. (2020). "Reputation and Trust Models with Data Quality Metrics for Improving Autonomous Vehicles Traffic Security and Safety" in Proc. IEEE/NDIA/INCOSE Syst. Secur. Symp, pp. 1-8, doi: 10.1109/SSS47320.2020.9174269. URL

[C30] **Chuprov, S.**, Viksnin, I., & Kim, I. (2019) "Urban Intersection Management with Connected Infrastructure Objects and Autonomous Vehicles" in 2019 IEEE International Conference on Connected Vehicles and Expo (ICCVE), pp. 1-4, doi: 10.1109/ICCVE45908.201
9.8964917. URL

[C31] **Chuprov, S.**, Viksnin, I., Kim, I., & Nedosekin, G. (2019). "Optimization of Autonomous Vehicles Movement in Urban Intersection Management System" in 2019 24th Conference of Open Innovations Association (FRUCT), pp. 60-66, doi: 10.23919/FRUCT.2019.8711967. URL

[C32] **Chuprov, S.**, Viksnin, I., Kim, I., & Usova, M. (2019). "Intersection Management Tasks in Mobile Robotic System with Decentralized Control" in CEUR Workshop Proceedings, vol. 2344, pp. 1-12. URL

[C33] Usova, M., **Chuprov, S.**, Viksnin, I., Gataullin, R., Komarova, A., & Iuganson, A. (2019). "Model of Smart Manufacturing System" in International Symposium on Intelligent and Distributed Computing, pp. 356-362, doi: 10.1007/978-3-030-32258-8_42. URL

[C34] Marinenkov, E., **Chuprov, S.**, Viksnin, I., & Kim, I. (2019). "Empirical Study on Trust, Reputation, and Game Theory Approach to Secure Communication in a Group of Unmanned Vehicles" in CEUR Workshop Proceedings, vol. 2590, pp. 1-12. URL

[C35] Usova, M., **Chuprov, S.**, Viksnin, I., & Baranova, O. (2019). "Model of Secure Informational Messages for Ensuring Informational Interaction in Smart Factory" in CEUR Workshop Proceedings, vol. 2590, pp. 1-8. URL

[C36] Viksnin, I., Lyakhovenko, J., Tursukov, N., **Chuprov, S.**, & Sozinova, E. (2019). "Empirical Study on Modeling of People Behavior in Emergency" in CEUR Workshop Proceedings, vol. 2590, pp. 1-8. URL

[C37] Kim, I., Matos-Carvalho, J. P., Viksnin, I., Campos, L. M., Fonseca, J. M., Mora, A., & **Chuprov, S.** (2019). "Use of Particle Swarm Optimization in Terrain Classification based on UAV Downwash" in 2019 IEEE Congress on Evolutionary Computation (CEC), pp. 604-610, doi: 10.1109/CEC.2019.8790031. URL

[C38] Viksnin, I., **Chuprov, S.**, Usova, M., & Zakoldaev, D. (2019). "Police Office Model for Multi-agent Robotic Systems" in IOP Conference Series: Materials Science and Engineering, vol. 497, no. 1, p. 012036, doi: 10.1088/1757-899X/497/1/012036. URL

DISSERTATIONS

[D1] **Chuprov, S.** (2024) "Robust Machine Learning Under Vulnerable Cyberinfrastructure and Varying Data Quality", Ph.D. dissertation, B. Thomas Golisano College of Computing and Information Sciences, Rochester Institute of Technology, Rochester, NY, USA, 2024. URL

[D2] **Chuprov, S.** (2019) "Assurance of Information in a Mobile Robotic System with Decentralized Control", Master's dissertation, Department of Secure Information Technologies, ITMO University, Saint Petersburg, Russia, 2019.

OTHER PUBLICATIONS AND PRESENTATIONS

[O1] Belov, A., Belyaev, P., Viksnin, I., Kim, I., Radabolsky, V., Turushev, T., & **Chuprov, S.** (2023). "Software and Hardware Bundle for Controlling a Group of Unmanned Vehicles Based on Robust Computer Vision Algorithms" in LETI Transactions on Electrical Engineering & Computer Science. 2023, vol. 16, no. 6. pp. 52–69. – *in Russian.* URL

[O2] Berezovskaya, O., **Chuprov, S.**, Neverov, E., & Sadreev., E. (2022). "Review and Comparison of AES Lightweight Modifications for a Low-Power Devices Network" in Problems of Information Security. Computer Systems. no. 2, pp. 35-50. doi: 10.48612/jisp/gp9v-96dh-32
v1. – *in Russian.* URL

[O3] Buzina, E., **Chuprov, S.**, Tursukov, N., Belyaev, P., & Viksnin, I. (2022). "Algorithm for Uniform Coverage of the Monitoring Territory by Unmanned Aerial Vehicles" in LETI Transactions on Electrical Engineering & Computer Science. 2022. Vol. 15, no. 5/6. P. 41–50. doi: 10.32603/2071-8985-2022-15-5/6-41-50. – *in Russian.* URL

[O4] **Chuprov, S.**, Gataullin, R., & Viksnin, I. (2021). "Vulnerabilities Assesment in Mobile Robotic Control System" in Proceedings of the St. Petersburg State Electrotechnical University LETI, vol. 10, pp. 70-75. – *in Russian.* URL

[O5] **Chuprov, S.** (2020). "Intersection Management Tasks Application in Mobile Robotic System with Autonomous Vehicle Models" in Saint-Petersburg's Government Grant Award Winners, pp. 68-74. URL

[O6] **Chuprov, S.** (2020). "Reputation, Trust, and Data Quality Concept for Security and Safety Assurance in a Group of Autonomous Vehicles" in IX Young Scientists Congress Proceedings, Electronic Edition. URL

[O7] **Chuprov, S.** (2019). "Security Assurance of Mobile Robotic Systems with Decentralized Control" in 2019 ITMO University Annotated Master's Research Thesis Proceedings, pp. 66-72. URL

[O8] **Chuprov, S.**, Viksnin, I., & Kim, I. (2019). "Organization of Safe Intersections Passage by Unmanned Vehicles in a Mobile Robotic System" in VIII Young Scientists Congress Proceedings, Electronic Edition. URL

[O9] **Chuprov, S.**, Viksnin, I., Kim, I., & Usova, M. (2019). "Secure Intersection Management Passage with a Group of Autonomous Vehicles in Mobile Robotic System with Decentralized Control" in ITMO University Young Scientists Almanac, vol. 2, pp. 43-48. URL

[O10] **Chuprov, S.**, Viksnin, I., & Usova, M. (2018). "Police Office Model with Partial Decentralized Control in Mobile Robotic System" in Regional Informatics and Information Secutity SPOISU Proceedings, vol. 6, pp. 245-249. URL

Presentations, posters, forums, workshops, and seminars w/o publications:

[NP1] **Chuprov, S.** (2024). "Security and Robustness of Machine Learning under Vulnerable Cyberinfrastructure and Varying Data Quality" at From Theory to Practice (T2P) Workshop, 15-19 April 2024, Kigali, Rwanda – *Remote presentation.*

[NP2] **Chuprov, S.**, Zatsarenko, R., & Reznik, L. (2024). "Improving Federated Learning Robustness towards Security Violations and Data Quality Degradations OR How to Learn Better via Extracting Knowledge and Accumulating History?" at UPSTAT 2024, 12-13 April 2024, Rochester, NY, USA.

[NP3] **Chuprov, S.**, & Reznik, L. (2023). "FLAME: Federated Learning against Malicious Engineering. Employing Trust and Reputation to Enhance Learning Security and Privacy" at Rochester Security Summit (RSS:2023), 25-26 October 2023, Rochester, NY, USA.

[NP4] **Chuprov, S.**, Reznik, L., & Zatsarenko, R. (2023). "MLIN or How to Make Networks and ML Applications Work Together in Real Conditions?" at First IEEE Upstate New York Workshop on Secure and Sustainable Communications Networks (SSCN), 10 October 2023, Rochester Institute of Technology, Rochester, NY, USA.

[NP5] **Chuprov, S.**, Reznik, L., & Zatsarenko, R. (2023). "FLAME: Federated Learning against Malicious Engineering. Employing Trust and Reputation to Enhance Learning Security and Privacy" at Eastern Great Lakes (EaGL) Theory Computation Workshop 2023, 30 September – 1 October 2023, University of Rochester, Rochester, NY, USA.

[NP6] **Chuprov, S.**, Reznik, L., & Memon, M. (2023). "Enhancing Federated Learning Security with Reputation and Trust-Based Indicators" at UPSTAT 2023, 21–22 April 2023, Rochester Institute of Technology, Rochester, NY, USA.

[NP7] **Chuprov, S.**, Reznik, L., Bhatt, K.M., & Memon, M. (2023). "Discovering and Addressing Privacy and Robustness Flaws in Federated Learning" at the Great Lakes Security Day (GLSD) 2023, 21 April 2023, Rochester Institute of Technology, Rochester, NY, USA.

[NP8] **Chuprov, S.** (2022). "Discovering and Addressing Privacy and Robustness Flaws in Federated Learning" at the Research Idea Ring (RIR) in Computer Science, 17 November 2022, Rochester Institute of Technology, Rochester, NY, USA.

[NP9] **Chuprov, S.**, & Reznik, L. (2021). "Reputation and Trust Models with Data Quality Metrics for Improving Autonomous Vehicles Traffic Security and Safety" at Great Lakes Security Day (GLSD) 2021 Online, 12 November 2021, Rochester, NY, USA. – *Poster session.*

[NP10] **Chuprov, S.** (2020). "Security and Safety Approaches to "Soft" Attacks Detection in Intelligent Systems and IoT" at Technology Development Trend of Intelligent Internet online workshop, 4 December 2020, Saint-Petersburg, Russia.

[NP11] **Chuprov, S.** (2020). "Reputation and Trust Approach for Cyber-physical Systems Security and Safety Assurance" at ITMO University's XLIX Research, Educational and Methodical Conference, 29 January 2020 - 1 Febeuary 2020. Saint-Petersburg, Russia.

[NP12] **Chuprov, S.** (2019). "Secure and Optimal Intersections' Traversal by a Group of Autonomous Vehicles in Mobile Robotic System" at Saint-Petersburg's Academic and Industrial Institutions Students' Grant Award Winners Round Table Discussion "Natural and Exact Sciences", 6th December 2019. Saint-Petersburg, Russia.

[NP13] **Chuprov, S.** (2019). "Reputation and Trust-based Approach for Security and Safety Assurance in a Group of Autonomous Vehicles" at Huawei Trust Worthy Software Technology Forum, 28 - 29 November 2019. Saint-Petersburg, Russia.

[NP14] **Chuprov, S.** (2019). "Multi-Agent Physical Testbed for Smart City's Control and Security Algorithms Verification" at Geek Picnic, 11 - 12 July 2019. Saint-Petersburg, Russia.

[NP15] **Chuprov, S.** (2018). "Multi-agent Systems Laboratory Current Research Projects" at Saint-Petersburg's International Youth Forum 6.0, 1 December 2018. Saint-Petersburg, Russia.