NIMA DORZHIEV

York, PA
nxd5381@psu.edu
linkedin.com/in/nima-dorzhiev

OBJECTIVE

Research assistant or internship position in AI Security and Cybersecurity, applying published research in adversarial LLM security, agentic systems, and industrial control system security toward trustworthy AI, while pursuing a PhD in AI Security and Governance.

EDUCATION

Pennsylvania State University — World Campus Expected 2029
Bachelor of Science in Cybersecurity Analytics & Operations

Starting Summer 2026

~50–60 transfer credits accepted from prior degrees.

Harrisburg Area Community College (HACC) *York, PA* Graduated 2025
Associate in science, Computer Information Security

GPA: 3.82 / 4.00 | Phi Theta Kappa International Honor Society, Dean's List

East-Siberian State University of Technology & Management *Russia* Graduated 2016
B.S. in Computer Science & Computer Engineering | GPA: 3.5

M.S. in Biotechnology (same institution, 2020)

Irkutsk National Research Technical University (IRNTU) *Russia*
Postgraduate Studies, Computer Science (incomplete, ~2.5 years)

Dissertation: Automated System for the Optimal Control of the Autoclave Gold Desorption Process from Activated Carbons based on the Use of Neural Networks

PUBLICATIONS

Dorzhiev, N., Liu, P. *"Strengthening Polymorphic Prompt Assembling: Dynamic Separator Generation Against Emerging Prompt Injection Attacks."* arXiv preprint, 2026.

Dorzhiev, N. *"RIPA: Sensory-Vector Prompt Injection Attacks on LLM-Controlled ROS 2 Robots."* arXiv preprint, 2026.

N. Dorzhiev, V. Elshin "*Requirements for a Neural Network in the Gold Desorption Process from Active Carbons."* Proc. Conf. on Prospects for the Development of Hydrocarbon and Mineral Processing Technology, pp. 244–247, 2022

N. Dorzhiev, V. Elshin *"Review and Application of Artificial Intelligence Methods in Optimal Control Systems for Metallurgical Processes".* Proc. Conf. on Prospects for the Development of Hydrocarbon and Mineral Processing Technology, pp. 194–198, 2021

RESEARCH EXPERIENCE

Independent Researcher *AI Agent & ICS Security* 2025—Present

- Designed MCPDrift, a benchmark measuring multi-turn behavioral drift in MCP agents under tool-poisoning attacks; evaluating across multiple LLM backends toward publication.
- Co-authored a published extension to Polymorphic Prompt Assembling with Prof. Peng Liu (Penn State IST/LIONS Center), introducing per-request dynamic separator generation to eliminate separator-leakage blast radius.
- Authored RIPA, a sole-authored, large-sample (n≥100) study of sensory-vector prompt injection on LLM-controlled ROS 2 robots across visual, audio, and LiDAR channels; released code and data publicly.

Postgraduate Researcher *IRNTU, Automated Systems Dept. — Irkutsk, Russia* 09/2020—02/2023

- Developed neural network architecture to optimize chemical autoclave desorption of gold in real time.
- Modeled system dynamics in Python; conducted experiments with feed-forward and recurrent NN topologies.
- Built a simulation environment for training and evaluating control algorithms under varying process parameters.
- Applied principles of optimal control theory in conjunction with data-driven machine learning approaches.

Security Researcher *HACC Capstone — York, PA* 2024—2025

- Conducted applied information security research; integrated NIST frameworks into project design.
- Produced security assessment documentation aligned with NIST SP 800-53 controls.

OTHER WORK EXPERIENCE

Incident & Response Manager *OTR IT Solutions — Irkutsk, Russia* 12/2020—02/2023

- Led root-cause analysis for complex incidents; coordinated across all support tiers.
- Designed escalation procedures; communicated resolution timelines to executive stakeholders.

Software Developer *ST8 — Ulan-Ude, Russia* 07/2018—10/2020

Software Engineer *RBSOFT — Ulan-Ude, Russia* 06/2016—07/2018

LEADERSHIP & AFFILIATIONS

Phi Theta Kappa International Honor Society, Member 2025—Present

ISC² — International Information Systems Security Consortium, Member 2024—Present

Penn State World Campus Student Community Starting Summer 2026

TECHNICAL SKILLS

Languages: Python, C#, SQL, Bash

AI/LLM Security: Prompt Injection Analysis, Adversarial Robustness Evaluation, Multi-Turn Attack Benchmarking (ASR, Wilson CI), MCP Protocol Security

Security: NIST AI RMF, EU AI Act, ISC² CC, Vulnerability Analysis, Incident Management, Bug Bounty Research

ML / AI: Neural Networks, Supervised Learning, NLP Pipelines, Optimization Algorithms

Systems: ROS 2, Gazebo, ICS/SCADA Architectures

Tools: Git, Linux, Docker, REST APIs, Burp Suite, MATLAB, Simulink, NumPy, SciPy, Jupyter

Languages (spoken): Russian (Native), Buryat (Native), English (Professional)