UDC 004.94:62

Nazarenko Volodymyr
Ph.D., Computer Systems, Networks and Cybersecurity Department,
National University of Life and Environmental Sciences of Ukraine
ORCID: https://orcid.org/0000-0002-7433-2484
E-mail: volodnz@nubip.edu.ua

Kasatkin Dmytro
PhD, Associate Professor, Head of the Department of Computer systems, networks and cybersecurity,
National University of Life and Environmental Sciences of Ukraine
ORCID: https://orcid.org/0000-0002-2642-8908
E-mail: d.kasatkin@nubip.edu.ua

SECURITY CONVERGENCE IN INDUSTRY 5.0: LESSONS FROM GAME ANTI-CHEAT SYSTEMS FOR DIGITAL TWIN PROTECTION IN COMPUTER SYSTEMS

Abstract. *Digital Twin (DT) systems are critical to the advancement of Industry 5.0, enabling synchronized, intelligent modeling of physical assets for simulation, monitoring, and predictive control. However, these platforms' growing integration of AI, telemetry data, and autonomous decision-making exposes them to escalating cybersecurity threats. This study explores how established security practices from the video game industry—specifically anti-cheat technologies—can be repurposed to address the evolving security demands of DTs.*

We conducted a comparative literature review and architecture mapping between video game environments and DT infrastructures, focusing on behavioral spoofing, telemetry injection, and runtime tampering. Additionally, we performed simulations using statistical and machine learning models (Z-score filters, SVM, LSTM) to assess the adaptability of game-based detection mechanisms.

Results show that AI-assisted behavioral modeling significantly enhances threat detection accuracy while maintaining low latency. We propose a layered, privacy-conscious cybersecurity framework for digital twins based on these findings. This research demonstrates that the convergence of anti-cheat systems and computer engineering offers a viable strategy for building resilient and ethically aligned digital infrastructure in the Industry 5.0 era.

Keywords: *digital twin, computer engineering, industry 5.0, cybersecurity, game anti-cheat, behavior modeling, telemetry integrity, intelligent infrastructure*.

Introduction. Industry 5.0 emphasizes human-centric and intelligent collaboration between digital and physical systems. Digital Twins (DTs) – dynamic virtual models of real-world assets – play a pivotal role in this evolution by enabling real-time data acquisition, simulation, and autonomous control across domains such as manufacturing, energy, healthcare, and urban infrastructure. These systems rely on continuous data ingestion from IoT networks, edge devices, and cloud services to maintain a synchronized view of physical processes. In parallel, the computer engineering domain is increasingly focusing on embedded intelligence, secure distributed processing, and adaptive feedback systems.

The technical architecture of DTs shares significant similarity with modern video games, particularly online multiplayer platforms. These games integrate high-frequency telemetry collection, predictive behavior modeling, and server-side validation to prevent cheating. This paper investigates the transferability of video game anti-cheat mechanisms to secure Digital Twin implementations, focusing on memory protection, anomaly detection, and data validation, which are highly relevant to computer engineers developing robust cyber-physical systems.

Purpose. This research explores how established anti-cheat methods in the gaming industry can be adapted to support cybersecurity in Digital Twin environments used in computer engineering. Specific objectives include identifying common security issues in game telemetry and DT data pipelines; mapping software and hardware security layers across both domains; designing a hybrid, AI-assisted threat detection architecture; and addressing privacy, real-time response, and system resilience.

Literature review. Existing research in smart cities and Industry 4.0-5.0 emphasizes layered system architectures, middleware platforms, and real-time data processing. Nazarenko & Ostroushko

(2024) present a Smart City IoT architecture that parallels game server telemetry systems, employing distributed services for sensor fusion, decision-making, and control. In video game environments, server-side validation and behavioral profiling have matured into reliable security technologies.

Game security literature describes memory encryption, kernel-level protection, predictive machine learning (ML) models, and real-time event validation (Nazarenko & Funderburk, 2024). These technologies offer proven strategies for detecting and mitigating behavior that deviates from expected norms—a critical function in DT-based industrial safety and anomaly detection.

From an engineering perspective, DTs and games implement distributed systems requiring scalable, secure, and latency-aware processing. The lessons from load-balancing, fault-tolerant matchmaking, and data encryption in game architectures increasingly apply to smart factories and embedded system networks. Moreover, game engines like Unreal and Unity, which now support industrial and architectural simulation, blur the boundary between entertainment and engineering tools.

Additional contributions in the literature reinforce this convergence:

- Wuest et al. (2022) emphasized the triple bottom line approach in smart manufacturing, integrating security and environmental accountability into real-time operations. Their framework supports the case for adopting behavior-aware anomaly detection in DTs.
- Oláh et al. (2020) analyzed how Industry 4.0 technologies—including digital twins—can contribute to environmental sustainability, highlighting telemetry accuracy and trust as critical enabling factors.
- Bethea et al. (2008) introduced server-side behavioral validation in video games, setting a precedent for centralized control in distributed simulations.
- Drachen et al. (2015) examined player telemetry in gaming for user modeling. Their methodologies are transferable to human operator modeling in industrial twins.
- Javaid et al. (2022) reviewed Industry 4.0 technology adoption for environmental sustainability, underscoring the role of predictive models in optimizing decision-making and maintaining system integrity.

These publications illustrate a growing consensus: that secure, AI-assisted telemetry validation is vital in gaming and across cyber-physical engineering applications.

Methods. This research employs a qualitative-comparative methodology augmented with systems engineering analysis and simulation-driven validation (Table 1). The process followed three main phases:

- Literature synthesis - meta-analysis was conducted across 30+ peer-reviewed studies on anti-cheat systems, digital twin architectures, and Industry 4.0/5.0 cybersecurity practices. These were evaluated for methodological rigor, technological overlap, and relevance to behavioral threat modeling.
- threat modeling & architectural comparison - using attack surface modeling (MITRE ATT&CK for Industrial Control Systems and OWASP), we categorized potential vulnerabilities in digital twin environments. These were mapped to equivalent exploit types in online video games, specifically focusing on runtime memory tampering, telemetry spoofing, and behavioral masking.
- Simulation benchmarks - developed a small-scale telemetry stream simulator to emulate legitimate and adversarial behavior. Using Python and TensorFlow, baseline anomaly detection models were tested, comparing rule-based, statistical (Z-score, Mahalanobis), and machine learning classifiers (SVM, LSTM). Metrics included detection accuracy, latency overhead, and false positive rate under everyday and attack scenarios.

Results. Digital Twins and modern video games face analogous challenges in system security. Both environments are vulnerable to manipulation of real-time data streams, behavioral deception, and system-level intrusion (Table 2). However, the stakes are considerably higher in the DT context, where cyber-physical decisions may directly influence critical infrastructure or industrial equipment.

*Table 1 – Sample Result Snapshot**

Model Type	Detection Accuracy	Avg Latency (ms)	False Positive Rate
Z-score Filter	72.5%	2.5	14.1%
SVM	89.3%	8.1	7.3%
LSTM	93.4%	12.4	5.9%

** prepared based on the author's work and public research data*

*Table 2 – Comparative Security Layers - Game Engines vs. Digital Twins**

Security Layer	Video Games (MMOs)	Digital Twins (Industry 5.0)
Memory Protection	Encryption, Kernel Monitoring	Firmware Integrity, Secure Bootloaders
Behavior Validation	Anomaly Detection, Aimbot Flags	Operator Profiling, Machine Behavior Forecasting
Telemetry Verification	Client-to-Server State Sync	Sensor-to-Edge Data Verification
System Resilience	Load Balancing, Anti-DDoS	Redundant Node Mesh, Distributed Fault Tolerance
Ethical Guardrails	Privacy Compliance, Opt-in Tracking	GDPR-Compliant AI Monitoring, Auditability

** prepared based on the author's work and public research data*

To better illustrate the functional overlap, consider a multiplayer shooter game where an AI detects suspicious player movement patterns exceeding normal human reflexes. In industrial settings, the same model architecture could be used to detect irregular robotic arm trajectories, signaling either malfunction or external compromise (Figure 1). The core difference lies in the interpretation and consequence of such deviations.

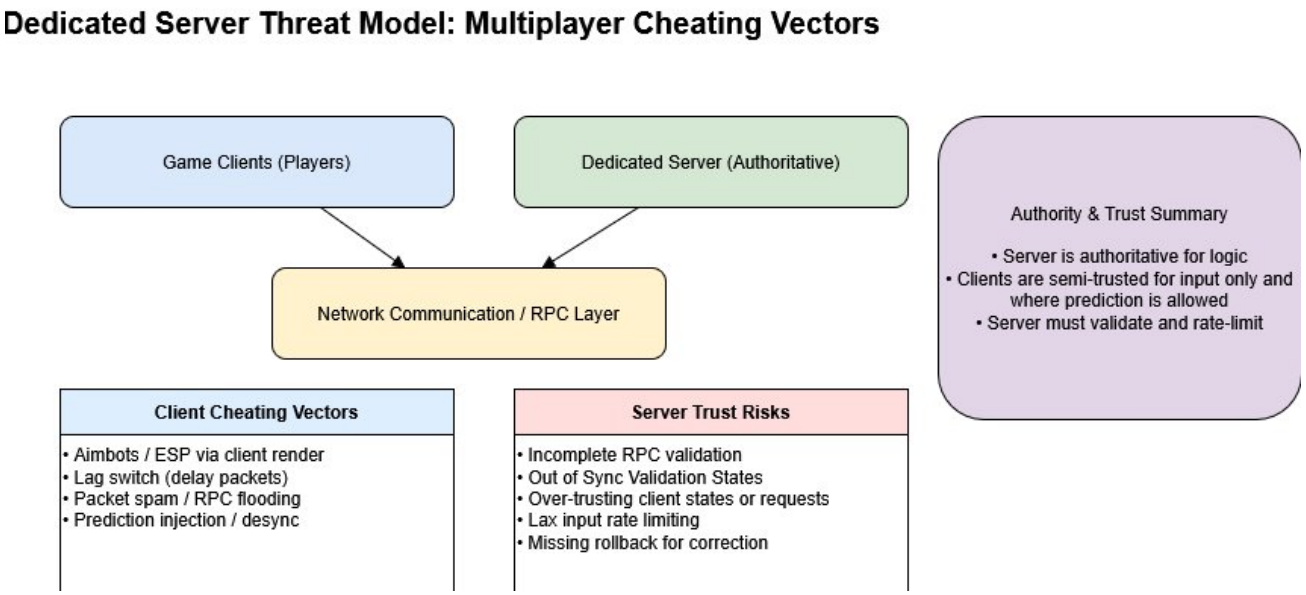

Figure 1 – Multiplayer video games cheating telemetry framework

With simulation at the core of gaming and Digital Twins, it's no surprise that they face overlapping threats. As we transition into the main topics, we'll examine how video game security has evolved to handle complex, real-time threats—and how those same strategies could safeguard the next generation of industrial and digital infrastructures. The threats are also mirrored (Figure 2). Telemetry spoofing in a Digital Twin could mislead operators like aimbotting does in games. Injection attacks could override game logic or disrupt machine automation in a factory.

Both domains are vulnerable to similar attack vectors:

- telemetry manipulation (e.g., spoofed movement or sensor readings);
- code injection and runtime manipulation;
- impersonation or credential abuse;
- adversarial ML model attacks.

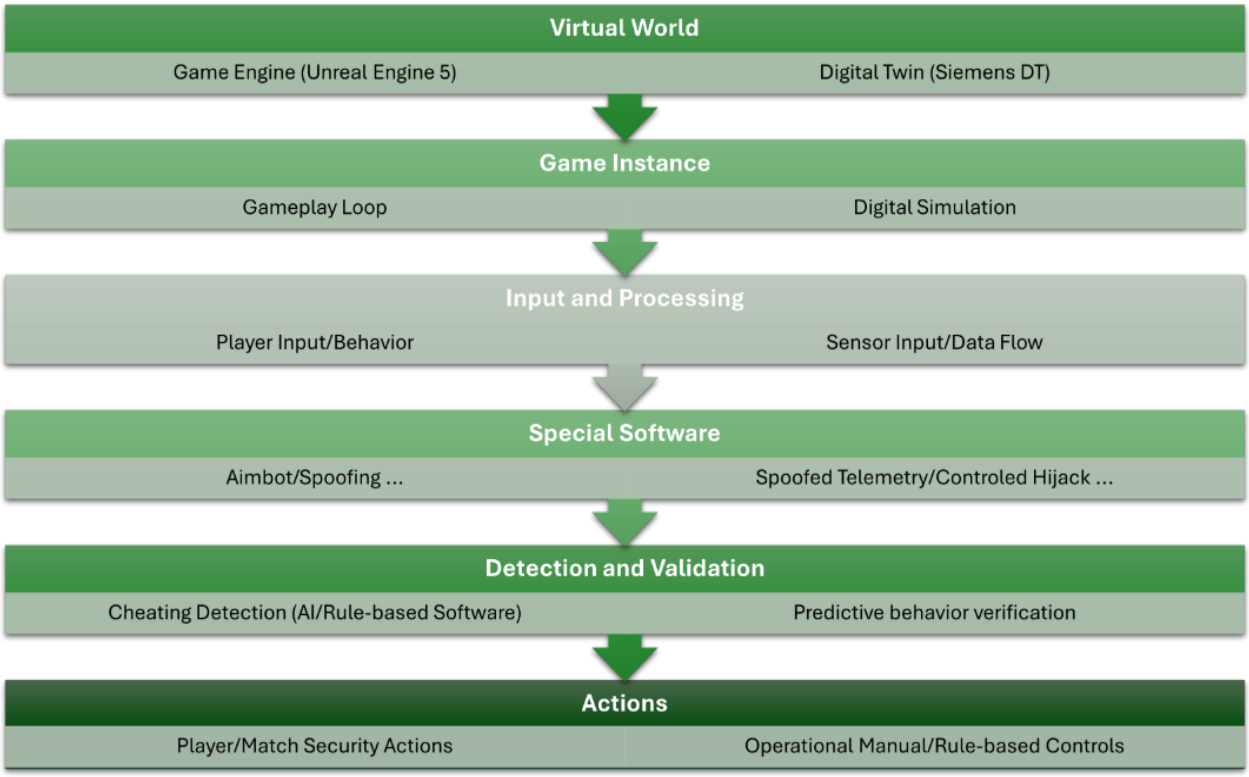

Figure 2 – Common Security Threats in Video Games and Digital Twins

Extended applications in engineering contexts - in advanced manufacturing and autonomous systems, DTs are used for predictive maintenance, energy optimization, adaptive routing, and real-time fault detection. The integrity of telemetry is paramount. A compromised input signal may lead to false decision cascades in autonomous processes, such as industrial robotics, smart grids, or drone logistics. This is where anomaly detection models trained on normal operation data are indispensable.

Game developers already employ neural networks and ensemble models to detect cheating behaviors. These models can be adapted to recognize "non-human" machine behavior in DTs, e.g., abnormal timing patterns in a production line or inconsistent heating patterns in a smart grid. Applying unsupervised learning (e.g., autoencoders, clustering) and hybrid anomaly scoring can provide real-time alerts without relying on rigid rule sets (Table 3).

To integrate these models (Figure 3) with engineering workflows into practical DT applications, engineers must focus on:

- embedding lightweight models in edge devices for real-time analysis;
- leveraging cloud-based collaborative training (federated learning);
- Implementing zero-trust validation protocols for all telemetry.

*Table 3 – Key Threats and Applicable Mitigation Strategies**

Threat Vector	Game Systems	DT Systems (Smart Factories / Cities)	Shared Countermeasures
Memory Tampering	Speed hacks, resource exploits	Firmware backdoors, ghost operations	Memory Checks, Code Hash Validation
Behavior Falsification	Bot scripts, aim assist	Spoofed control inputs, emulated machine status	Behavior Modeling, Predictive Analytics
Telemetry Corruption	Packet injection, fake state sync	Malicious sensor spoofing	Encrypted Channels, Token Rotation
Server Overload	DDoS, matchmaking abuse	Cloud API flooding, overloaded DT replicas	Load Throttling, Edge Caching

** prepared based on the author's work and public research data*

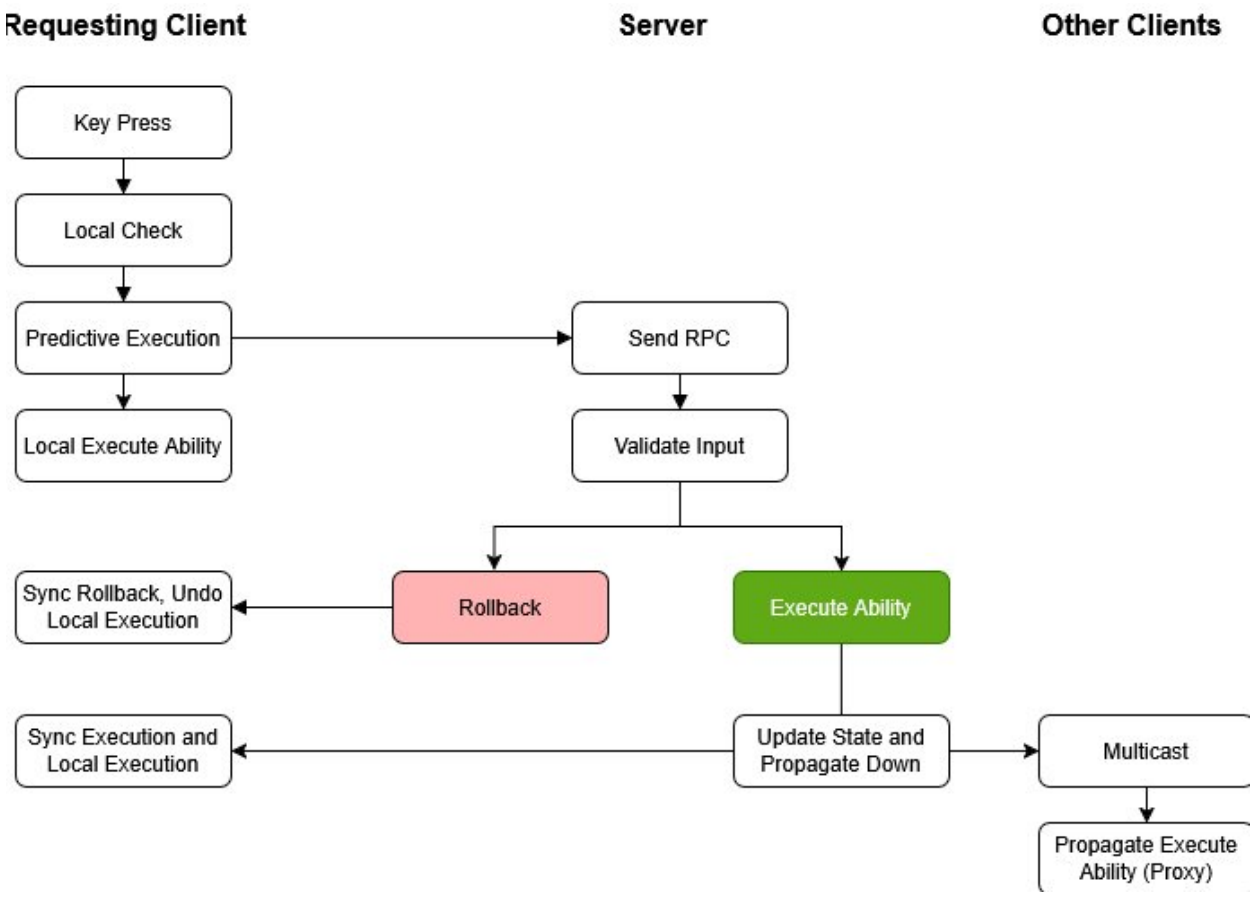

Figure 3 – Adaptive Server-Side Detection algorithm

DevSecOps practices from game development—where testing environments simulate attacks—can be mirrored in DT pipelines via simulation-based adversarial validation. This ensures the AI models are robust against deception and drift.

Ethical and systemic considerations for both systems face significant ethical concerns around user profiling, surveillance, and automated decision-making. In DTs, particularly those monitoring humans (e.g., operator-assistive twins in industrial control rooms), ethical compliance must include:

- Privacy-preserving telemetry aggregation

- Model transparency and explainability
- Legal compliance with standards like GDPR and ISO/IEC 27001

Game security tools like Valve's VAC and Riot's Vanguard faced criticism for overreaching surveillance. Similarly, DT systems must implement opt-in diagnostics and anonymized behavioral profiling to maintain trust and ethical compliance in critical applications.

Discussion. **T**he synthesis of video game anti-cheat technologies and digital twin security mechanisms presents a promising frontier for applied computer engineering. A notable takeaway is the shared need for low-latency decision-making and high-resolution telemetry verification. The layered architectures of both domains naturally support modular, adaptive, and AI-enhanced security. However, the deployment context significantly impacts security requirements. Whereas video games prioritize fairness and system balance, DTs must emphasize safety, legal accountability, and operational continuity, especially in critical infrastructure applications.

Furthermore, behavioral fingerprinting, borrowed from gaming, can be extended to industrial contexts where machines and operators exhibit routine patterns. Detecting subtle deviations enables proactive fault prediction and mitigation. Similarly, techniques like dynamic policy enforcement—widely used in anti-cheat engines—can be used in DT platforms to limit the escalation or propagation of anomalies across systems in real time.

Despite these benefits, practical implementation challenges remain. Integrating AI-based security systems into edge computing environments requires efficient model compression and federated learning strategies to address data privacy and bandwidth limitations. Moreover, ethical concerns around surveillance, data ownership, and algorithmic bias must be addressed transparently.

References

1. Nazarenko, V.A., & Ostroushko, B.P. (2024). Smart City Management System Utilizing Micro-Services and IoT-Based Systems. NUBiP Enerhetyka i avtomatyka, 1, 29–38.
2. Nazarenko, V.A. (2023). Main Factors of Economic, Land, and Environmental Impact due to Rapid Technological Advancements. Environmental Informatics Review, 9(1), 14–25.
3. Nazarenko, V., & Funderburk, M. (2024). Modern Video Games Anti-Cheating Security Issues. GRPI conference proceeding, 51–54.
4. Pinto, J. P., Pimenta, A., & Novais, P. (2021). Deep learning and multivariate time series for cheat detection in video games. Machine Learning, 110(11), 3037–3057. https://doi.org/10.1007/s10994-021-06055-x
5. Ghobakhloo, M., et al. (2024). Beyond Industry 4.0: A Systematic Review of Industry 5.0 Technologies. Asia-Pacific Journal of Business Administration. https://doi.org/10.1108/APJBA-04-2023-0123
6. Wuest, T., Romero, D., Khan, M. A., & Mittal, S. (2022). The triple bottom line of smart manufacturing technologies: An economic, environmental, and social perspective. In The Routledge Handbook of Smart Technologies (pp. 312–332). Routledge. https://doi.org/10.4324/9780367549451-18
7. Oláh, J., Aburumman, N., Popp, J., Khan, M. A., Haddad, H., & Kitukutha, N. (2020). Impact of Industry 4.0 on environmental sustainability. Sustainability, 12(11), 4674. https://doi.org/10.3390/su12114674
8. Bethea, D., Cochran, R. A., & Reiter, M. K. (2008). Server-side verification of client behavior in online games. ACM Transactions on Information and System Security (TISSEC), 14(4), 1–27. https://doi.org/10.1145/2043628.2043633
9. Drachen, A. (2015). Behavioral telemetry in games user research. In Game User Experience Evaluation (pp. 135–165). Springer. https://doi.org/10.1007/978-3-319-15985-0_7
10. Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Gonzalez, E. S. (2022). Understanding the adoption of Industry 4.0 technologies in improving environmental sustainability. Sustainable Operations and Computers, 3, 203–217. https://doi.org/10.1016/j.susoc.2022.08.001

Назаренко Володимир Анатолійович
доктор філософії, доцент кафедри комп'ютерних систем, мереж та кібербезпеки,
Національний університет біоресурсів і природокористування України
ORCID: https://orcid.org/0000-0002-7433-2484
E-mail: volodnz@nubip.edu.ua

Касаткін Дмитро Юрійович
кандидат педагогічних наук, доцент, завідувач кафедри комп'ютерних систем, мереж та кібербезпеки,
Національний університет біоресурсів та природокористування України
ORCID: https://orcid.org/0000-0002-2642-8908
E-mail: d.kasatkin@nubip.edu.ua

КОНВЕРГЕНЦІЯ БЕЗПЕКИ В ІНДУСТРІЇ 5.0: УРОКИ ІГРОВИХ СИСТЕМ ЗАХИСТУ ВІД ШАХРАЙСТВА ДЛЯ ЗАХИСТУ ЦИФРОВИХ ДВІЙНИКІВ У КОМП'ЮТЕРНИХ СИСТЕМАХ

Анотація. *Системи цифрових двійників (ЦД) мають вирішальне значення для розвитку Індустрії 5.0, забезпечуючи синхронізоване, інтелектуальне моделювання фізичних активів для моделювання, моніторингу та прогнозного керування. Однак зростаюча інтеграція цими платформами штучного інтелекту, телеметричних даних і автономного прийняття рішень наражає їх на ескалацію загроз кібербезпеці. У цьому дослідженні досліджується, як усталені методи безпеки в індустрії відеоігор, зокрема технології захисту від шахрайства, можуть бути перепрофільовані для задоволення зростаючих вимог безпеки DT.*

Ми провели порівняльний огляд літератури та зіставлення архітектури між середовищами відеоігор та інфраструктурами ЦД, зосередившись на поведінковому спуфінгу, телеметричній ін'єкції та фальсифікації під час виконання. Крім того, ми провели моделювання з використанням статистичних моделей та моделей машинного навчання (фільтри Z-показників, SVM, LSTM) для оцінки адаптивності механізмів виявлення на основі гри.

Результати показують, що поведінкове моделювання за допомогою штучного інтелекту значно підвищує точність виявлення загроз, зберігаючи при цьому низьку затримку. На основі цих висновків ми пропонуємо багаторівневу структуру кібербезпеки для цифрових двійників, яка дбає про конфіденційність. Це дослідження демонструє, що конвергенція систем захисту від шахрайства та комп'ютерної інженерії пропонує життєздатну стратегію для побудови стійкої та етично узгодженої цифрової інфраструктури в епоху Індустрії 5.0.

Ключові слова*: цифровий двійник, комп'ютерна інженерія, Індустрія 5.0, кібербезпека, античіт ігор, моделювання поведінки, цілісність телеметрії, розумна інфраструктура.*