SYNCHROINFO JOURNAL

www.media-publisher.eu/synchroinfo-journal

THE DIGITAL TWIN OF THE CYBER-STUDY ENTERPRISE: NEW METHODS FOR SIMULATING THE MOST COMPLEX ATTACKS

Victoria A. Zakharova [1], **Anastasia Y. Kudryashova** [2]

[1] MAI, Moscow, Russia;
zakharova062002@mail.ru

[2] MTUCI, Researcher, Moscow, Russia;
a.i.kudriashova@mtuci.ru

ABSTRACT

The study investigates novel methods for modeling complex cyberattacks based on enterprise "digital twin" technology. The aim is to analyze the concept of a "digital twin" as a tool for cyber exercises, compare it with tradition-al cyber ranges, identify current cybersecurity challenges arising from the use of digital twins, and propose methods for addressing them. The research employs comparative analysis, problem systematization, and the design of architecture-oriented solutions based on technologies such as blockchain, swarm intelligence, adversarial attack defense methods, and approaches to verifiable AI explainability. Key advantages of digital twins over traditional cyber ranges have been identified, including dynamic synchronization, modeling accuracy, and predictive capabilities. Fundamental challenges have been systematized, encompassing issues of data reliability, integration, and telemetry processing, as well as new threat classes such as ensuring cyber resilience in "swarms" of interconnected digital twins and securing embedded artificial intelligence. To address these challenges, a comprehensive approach has been proposed, involving decentralized trust systems, collective defense mechanisms, multi-layered AI protection, and verifiable explainability systems. The proposed methods and architectural solutions enable a shift from reactive to proactive cybersecurity strategies, facilitate the creation of self-organizing defense systems, enhance trust in autonomous AI decisions, and lay the foundation for legally compliant auditing in critical infra-structures. The novelty of the work lies in the identification and in-depth analysis of new problem classes related to digital twin ecosystems ("swarms") and the security of integrated AI, as well as in the proposal of comprehensive, technology-driven solutions, which defines the direction for the development of next-generation cybersecurity systems.

KEYWORDS: *digital twin; cybersecurity; cyber studies; attack modeling; cyberpolygon.*

DOI: 10.36724/2664-066X-2025-11-5-18-27

Received: 20.08.2025
Accepted: 21.10.2025

Citation: Victoria A. Zakharova, Anastasia Y. Kudryashova, "The digital twin of the cyber-study enterprise: new methods for simulating the most complex attacks", *Synchroinfo Journal* **2025**, vol. 11, no. 5, pp. 18-27.

Licensee IRIS, Vienna, Austria.

1 Introduction

The modern era of digital transformation is characterized by the rapid increase in complexity of cyber-physical systems and corporate information infrastructures. In the context of the growing number of sophisticated cyberattacks and the expanding attack surface, traditional security approaches based on reactive measures and the analysis of past incidents demonstrate their insufficient effectiveness.

One of the most promising paradigms opening new horizons in this field is the concept of the "digital twin". A digital twin is an extremely advanced simulation used in computer engineering. Originally developed for the design and management of complex engineering objects, this technology is finding increasingly widespread application in the realm of cybersecurity.

2 The Concept of the "Digital Twin" in Cybersecurity

A "Digital Twin" creates a unique secure environment – a kind of "cyber range" where attacks can be modeled, incident response scenarios can be practiced, and the consequences of implementing new technologies can be assessed without threatening the operation of the original. A digital twin is a dynamic, software-based virtual model of a physical object, system, or process that is synchronized with it through continuous data exchange in real or near-real time.

In the context of cybersecurity, a digital twin is not merely a static copy but a "living" digital shadow of the protected infrastructure (e.g., an enterprise's operational technology network, IT landscape, or IoT device). This model continuously evolves, reflecting not only the current state of components (software versions, configurations, network connections) but also their behavior, workflows, and cyber-physical interactions [1].

A digital twin possesses the following characteristics:

1. Virtual R resentation.

The twin is an exact digital analog that reproduces the architecture, components, connections, and operational logic of the physical system. This includes modeling network topology, servers, workstations, active network equipment, and even user behavior.

2. Bidir tional Data Synchronization.

The foundation of the twin's existence is a constant flow of data from the real world. This ensures the model's relevance and allows for analysis of the current situation, rather than retrospective data.

3. Autonom and Simulation Capability.

The twin must function as an independent system capable of performing complex simulations based on the data and algorithms loaded into it. This allows for predicting system behavior under various conditions without interfering with the real object.

4. Scalabilit and Modularity.

A digital twin can be created for an individual device (e.g., an industrial controller) as well as for an entire complex distributed system (e.g., a Smart City or digital production facility). It is often built on a modular principle, where each physical component has its own digital "twin."

5. Integratio with Analytical Systems and AI.

To process vast amounts of data and identify complex, hidden anomalies and cyberattacks, digital twins are closely integrated with big data analytics systems, machine learning (ML), and artificial intelligence (AI). This transforms them from a passive model into an active tool for predictive analytics [2].

Thus, the concept of a "digital twin" represents a qualitative leap from static modeling to the creation of a dynamic, living digital entity, inextricably linked to its physical prototype. Its key value in cybersecurity lies precisely in the comprehensiveness of its characteristics: it is an autonomous, real-time synchronized, and predictively capable modeling environment.

3 Comparison of a "Digital Twin" with Traditional Cyber Ranges

Traditional cyber ranges have long been the standard for training specialists, testing security tools, and practicing incident response. However, with the emergence of the "digital twin" concept, a new, more advanced paradigm has formed. Despite the shared goal — creating an isolated environment for cybersecurity — these approaches have fundamental differences in their foundation, capabilities, and applicability to the realities of modern complex infrastructure.

Table 1 presents the results of the analysis of differences between a "digital twin" and traditional ranges.

Table 1

Comparison of a "Digital Twin" with Traditional Cyber Ranges

Criterion	Traditional Cyber Range	Digital Twin
Foundation and Realism	An assembled, often standard or training environment built on template configurations. Reproduces general, not unique, characteristics of a specific object.	A highly accurate virtual copy of a specific physical system with its unique architecture, connections, software versions, and configurations.
Data Relevance	A static or periodically updated environment. Data becomes outdated between testing sessions and does not reflect the current state of the real object.	Dynamic synchronization in real or pseudo-real time. The model is constantly up-to-date and "breathes" the same data as the real system.
Primary Function	Simulation and training: practicing responses to known scenarios, team drills.	Predictive analysis and proactive testing: modeling unknown threats, assessing consequences before they occur, optimizing the operation of the real system.
Flexibility and Cost of Implementing Changes	Implementing significant changes to the range's architecture requires manual effort, time, and resources.	High flexibility. Changes in the real system are automatically or with minimal effort reflected in the twin. "Cloning" the environment for various tests is simplified.
Connection with the Physical Object	Absent or one-way. Test results from the range require manual interpretation and transfer to production.	Two-way. Modeling and analytics results can be directly applied to adjust configurations and security policies of the real object.

While traditional cyber ranges remain a valuable tool for fundamental training and practicing standard procedures, "digital twins" open the door to proactive protection of unique, complex, and critical infrastructure.

A key advantage of the "digital twin" lies in the fact that an attack successfully repelled on a standard range may prove useless against the specific configuration of a real industrial controller or corporate network. At the same time, a vulnerability identified and investigated in a "digital twin" most likely exists in the real object as well, meaning that its elimination will have an immediate practical effect [3].

Thus, the "digital twin" does not merely replace but expands and deepens the concept of a cyber range, transforming it from a training ground into a strategic command center for proactive cyber risk management and ensuring business resilience in the digital age.

4 Problems of Using Digital Twins in Cybersecurity Tasks

The concept of digital twins, dynamic virtual copies of physical objects, has firmly entered the arsenal of modern technologies, promising a revolution in predictive maintenance, process optimization, and, crucially, in ensuring cybersecurity. The ability to conduct cyberattacks on an exact digital copy of a critical asset, without fear of real-world consequences, appears to be an ideal tool for proactive protection. However, a digital twin itself is not a panacea; its implementation and operation generate a whole range of problems.

To date, among the most common are the problems presented in Figure 1.

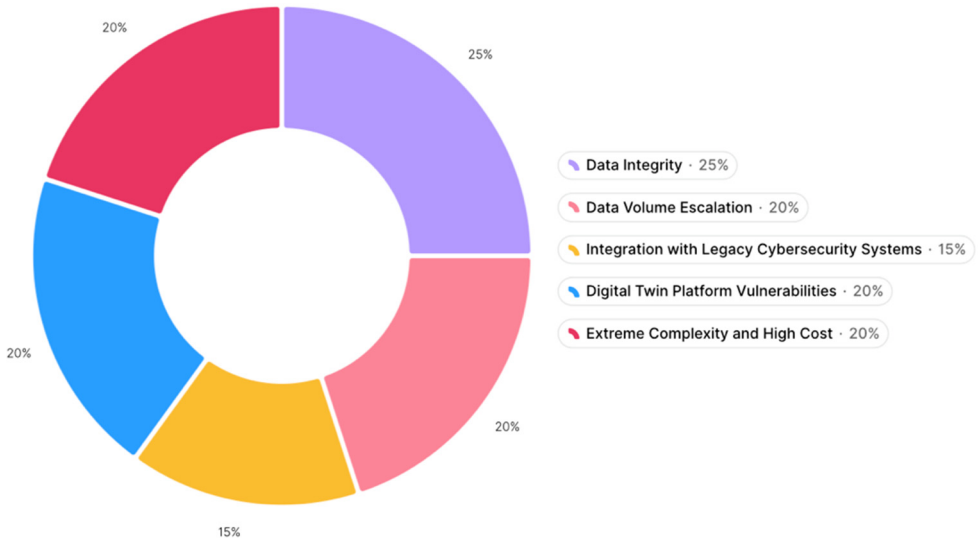

Figure 1. Problems of Using Digital Twins

Let's examine each problem in detail.

1. Data Integrity. The digital twin is entirely dependent on information coming from sensors, controllers, and systems of the physical object. If this information is compromised, inaccurate, or deliberately distorted, then all conclusions drawn by the twin become false. Receiving these false readings, the twin may fail to recognize an approaching catastrophe, leading to a real accident, or, conversely, generate a false alarm, causing a costly and unjustified shutdown of the entire production line. Thus, the twin, intended to enhance security, becomes a tool of disorientation [4].

2. Data Volume Escalation. To maintain the adequacy and accuracy of its virtual copy of the physical object, a digital twin requires continuous ingestion, processing, and analysis of data streams. These streams are formed from high-frequency telemetry from thousands of sensors, operational logs of controllers, metadata about the external environment, and records. However, this very vital flow of information creates systemic bottlenecks and critical vulnerabilities. A paradox arises: to increase the twin's accuracy and usefulness, it is necessary to increase the volume and frequency of data, but this very increase undermines its security and operational efficiency. Network communication channels, even with high bandwidth, become a problematic point, and data preprocessing and verification systems fail to process incoming streams in real-time. This creates windows of vulnerability – periods when the state of the digital twin does not correspond to the actual state of the physical asset. Under such conditions, mechanisms for proactive detection of cyberattacks and anomalies, such as intrusion detection systems and behavioral analyzers, lose their effectiveness because they operate on outdated, incomplete, or already compromised data. An attacker can exploit this delay to carry out targeted attacks.

3. Integration with Legacy Cybersecurity Systems. The lack of standardized API interfaces for integrating the digital twin (DT) with legacy security systems (SIEM, SOAR, IDS) leads to the formation of "semantic gaps." The diversity of protocols and data formats hinders the correct correlation of cybersecurity events between the cyber-physical level and its digital representation. As a result, an attack detected at the DT level cannot be adequately interpreted and escalated by the protection systems of the physical infrastructure, rendering the deployment of comprehensive security systems pointless.

4. Digital Twin Platform Vulnerabilities. The platform itself is a complex software suite, often stitched together from heterogeneous technologies – IoT platforms, simulation systems, cloud services, and artificial intelligence modules. Each of these components potentially contains vulnerabilities. Hacking the twin's platform opens up truly unique opportunities for an attacker. They gain access not just to operational data, but to the complete digital model of the object. By studying the twin, the attacker can conduct deep analytics, identifying the most vulnerable and critical points of the real system for subsequent targeted and destructive attacks [5].

5. Extreme Complexity and High Cost. This applies not only to creation but, more importantly, to maintaining a digital twin. Building a high-precision model of a complex system, such as a power grid or an entire manufacturing plant, requires colossal investments in modeling, integration, and computing resources. However, the real problem begins at the operational stage: any physical object has its own life – it is modernized, components are replaced, software and firmware are updated. Each such change must be immediately and accurately reflected in the digital twin. The slightest discrepancy between the original and its virtual copy accumulates over time, making the twin an unreliable copy, and its forecasts and analysis – useless or even dangerous from a security perspective [6].

Based on the studied sources, the following unresolved problems can be identified:

1. The active development of the digital twin concept marks a transition from isolated replicas of individual assets to complex ecosystems – "swarms" of coordinated digital twins. Managing such complex objects as smart energy systems, smart cities, or distributed production forms a new class of cyber-physical systems, the security of which cannot be ensured by traditional approaches. The problem lies in ensuring the cyber resilience of a digital twin "swarm" against cascade effects arising from the compromise of one or several of its elements. The problem manifests in three interconnected aspects:

1) The lack of reliable mechanisms for inter-twin trust. In a heterogeneous environment where digital twins of various architectures exchange critical data, standard authentication protocols prove insufficient;

2) The acute need for predictive modeling of cascade failures. Static vulnerability analysis methods are ineffective for dynamically changing connection graphs;

3) The challenge of creating decentralized systems of collective defense. Centralized monitoring becomes a single point of failure. A promising direction is the implementation of swarm intelligence principles, where each digital twin participates in forming global defensive behavior based on local data and limited information from neighbors.

2. Integration of Artificial Intelligence into Digital Twins. A problem is adversarial attacks on machine learning, specific to the cyber-physical context of digital twins. Unlike classical computer systems where such attacks target pattern recognition, in digital twins an attacker can create targeted perturbations of telemetry input data, which are practically indistinguishable from legitimate signals but lead to catastrophic errors in the operation of predictive models.

Simultaneously, there is a problem of ensuring the explainability and interpretability of decisions made by the digital twin's artificial intelligence. In critical applications, such as managing energy systems or medical devices, it is not enough to receive a prediction from the model – an understanding of the cause-and-effect relationships that led to this decision is necessary. However, modern artificial intelligence itself becomes a target for attacks when an attacker can manipulate the provided explanations, hiding the real causes of erroneous decisions. This creates a situation where the operator loses trust in the system, even if its basic predictions remain accurate.

5 Ways to Solve Cybersecurity Problems in Digital Twin Systems

The systemic vulnerabilities identified in the previous section, related to ensuring the security of digital twin swarms and the integration of artificial intelligence, require the development of new specialized protection mechanisms. Traditional cybersecurity approaches demonstrate insufficient effectiveness in conditions of dynamically changing connection graphs between digital twins and in countering targeted attacks on machine learning systems.

Table 2 presents ways to solve the identified cybersecurity problems in digital twin systems.

Table 2

Ways to Solve Cybersecurity Problems

Problem		Solutions
1	Transition from isolated replicas of individual assets to swarms of coordinated digital twins	Development of a decentralized trust system based on blockchain technology
		Implementation of a decentralized collective defense system based on swarm intelligence principles
2	Integration of artificial intelligence into digital twins	Multi-layer system for protection against adversarial attacks

Let's examine each proposed solution in more detail.

1. evelopment of a Decentralized Trust System Based on Blockchain Technology

This represents a comprehensive solution to the problem of ensuring secure interaction within a swarm of digital twins. The core idea is to create a fault-tolerant infrastructure that eliminates the need for a central trust authority and ensures transparency of all transactions between digital twins.

A fundamental element of such a system is the use of a distributed ledger, where each digital twin receives a unique digital identifier based on cryptographic keys. These identifiers are registered on the blockchain upon the twin's initialization in the system, creating a reliable foundation for subsequent authentication.

Smart contracts are an important component of the system, automating the processes of data integrity verification and security policy compliance control. Smart contracts check each transaction against pre-established security rules. For example, when one digital twin attempts to transfer data to another, the smart contract automatically verifies the validity of both parties' digital certificates, the legitimacy of the requested operation, and the compliance of the data with established formats.

Particular attention should be paid to implementing decentralized identification mechanisms, which allow digital twins to authenticate each other without contacting a central server. This is achieved through the use of asymmetric cryptography and verifiable credentials stored in the distributed ledger. Each twin has a private key for signing outgoing messages and a public key, accessible to all participants, for verifying authenticity [7].

From a practical implementation standpoint, it is proposed to deploy a private blockchain based on the "Hyperledger Fabric" platform, which provides the necessary performance and access control. Integration with existing digital twin platforms is achieved through specialized API gateways that convert internal data formats into standardized blockchain transactions.

Implementing such a system yields several key advantages. First, the overall system's resilience to the compromise of individual nodes is significantly increased, as an attacker would need to gain control over a majority of the network to forge transactions. Second, complete traceability of all interactions between digital twins is ensured due to the immutability of the transaction log. Third, dependency on centralized authentication authorities is reduced, eliminating single points of failure in the system.

2. Development and Implementation of a Decentralized Collective Defense System Based on Swarm Intelligence Principles

This represents a promising approach to ensuring the cyber resilience of digital twin ecosystems. This methodology is based on organizing autonomous interaction between individual digital twins, where each node of the system is capable of independently analyzing threats and coordinating its defensive actions with other network participants without the need for centralized management.

The fundamental principle of the system is the ability for collective decision-making, which emerges from the interaction of many simple agents. In the context of cybersecurity, this means that each digital twin functions as an autonomous agent equipped with local anomaly detection and threat analysis mechanisms. These agents exchange signals about potential cyberattacks using a lightweight communication protocol based on a modified STIX/TAXII format, adapted for operation under conditions of limited bandwidth and requirements for minimal data transmission delay.

An important component of the system is the decision-making algorithms. These algorithms allow the system to dynamically adapt to changing cyber threat conditions without the need for global reconfiguration. For example, upon detecting a compromised node, neighboring digital twins automatically form an "isolation zone," rerouting information flows along alternative paths and temporarily tightening security policies to prevent the spread of the attack.

To implement multi-lateral security mechanisms, zero-knowledge proof protocols are used, allowing digital twins to authenticate each other and exchange critical information without disclosing confidential data about their internal structure or current state. This ensures the necessary balance between the requirement for transparency of interaction within the swarm and the protection of trade secrets and intellectual property embedded in individual digital twins [8].

Practical implementation of the system requires solving several technological challenges, including developing effective distributed machine learning algorithms for the joint improvement of threat detection models, ensuring compatibility with heterogeneous digital twin platforms, and creating standardized interfaces for inter-twin interaction. However, the successful implementation of this approach opens new possibilities for creating truly scalable and resilient next-generation cyber-physical systems.

Implementing such a system yields several key advantages. First, the fault tolerance of the digital twin ecosystem is significantly increased by eliminating single points of failure. Second, the system demonstrates an ability for self-organization and adaptive response to previously unknown types of attacks. Third, the operational burden on human operators is reduced, as the majority of routine defensive operations are performed autonomously.

3. Develo ent of a Multi-Layer Defense System Against Adversarial Attacks

This represents a comprehensive approach to ensuring the resilience of digital twin artificial intelligence to targeted perturbations of input data. This system is based on creating a multi-layered security architecture, where each level implements specific mechanisms for detecting and neutralizing various types of adversarial influences.

The fundamental principle of the system is the sequential processing of data through a series of specialized validation and filtering modules:

1) The first level implements mechanisms for preprocessing input signals based on "Feature Squeezing" and spatial data compression technologies. These methods allow for the elimination of potentially malicious perturbations even before they reach the main machine learning model, while preserving the informativeness of legitimate signals. At this stage, color space compression, quantization, and smoothing algorithms are applied, which effectively eliminate high-frequency components characteristic of most adversarial examples.

2) The second level of the system is an anomaly detector built on deep "Autoencoders" trained exclusively on legitimate data about the operation of physical equipment. These neural networks form a latent representation of the system's normal operating modes, allowing for the computation of reconstruction error for incoming signals. Any significant deviation from the benchmark, exceeding a predetermined threshold, is flagged as a potential adversarial attack.

3) The third evel of protection implements system resilience through the parallel use of several independently trained machine learning models. Each of these models has a different architecture and was trained on slightly modified datasets, ensuring diversity in their vulnerabilities to adversarial attacks. The system's decision function analyzes the consistency of predictions from all models – significant discrepancies between their outputs when processing the same input data serve as a reliable indicator of an attempted adversarial attack.

4) The fourth level of the system is a digital testing ground for the continuous testing and improvement of model robustness. On this testing ground, various types of adversarial examples – from classic FGSM and PGD attacks to specialized perturbations that account for the physical constraints of cyber-physical systems – are generated in real-time and applied to the current operational models [9].

The technological foundation of the system consists of specialized machine learning libraries with support for "adversarial robustness," stream processing systems such as "Apache Kafka or Apache Flink" for handling high-frequency telemetry streams, and distributed databases for storing reference patterns of normal equipment behavior.

Practical implementation requires significant computational resources to maintain redundant models and operate the testing ground but provides an unprecedented level of protection for critical cyber-physical systems managed by AI-powered digital twins.

4. Develo ent of a Verifiable AI Explainability System

This system is designed to ensure trust in autonomous decisions made by digital twins in critical infrastructures. This approach overcomes the fundamental limitations of contemporary explainable AI (XAI) methods by creating an architecture where decision interpretation processes are protected from manipulation through cryptographic protocols, formal verification methods, and immutable audit systems.

The core of the system is the concept of cryptographically guaranteed decision traceability, where every AI output is accompanied by a digital explanation certificate containing three interconnected components:

– the factual data that influenced the decision;

– the logical rules nd dependencies identified by the model;

– a quantitat ve assessment of each factor's contribution to the outcome.

These certificates are generated using asymmetric cryptography algorithms, where the private key is stored in a secure hardware module (HSM), and the public key is available for verification by all authorized parties.

Functionally, the system implements a multi-tier explanation model, adaptable to the competencies of different users. At the operational level, simplified interpretations in natural language with color-coded criticality indicators are generated, allowing operators to quickly understand the system's recommendations. For technical specialists, detailed reports are provided with visualizations of influence graphs, feature importance heatmaps, and statistical distributions.

To ensure the authenticity of explanations, the system integrates mechanisms of formal verification based on methods of abstract interpretation and symbolic execution. These methods allow for mathematically proving the correspondence between the source data, the internal states of the model, and the provided explanations.

A technological innovation is the implementation of a distributed explanation ledger, where each generated certificate is hashed and recorded on a blockchain with timestamps. This architecture ensures three critically important properties:

– immutability of the decis on history;

– transp rency for auditors and regulators;

– the ability to ana yze decision-making chains [10].

The practical implementation of this system overcomes the main barrier to AI adoption in critical areas – the problem of blind trust – replacing it with a model of verifiable and justified trust based on mathematically rigorous proofs and cryptographic guarantees of integrity.

The technological requirements include specialized libraries for formal verification

(Isabelle/HOL, Coq), an infrastructure of distributed ledgers with support for confidential computing, and integration gateways for connecting to heterogeneous digital twin platforms.

Implementing this system ensures:

– a reduction in the time for operators to make informed decisions due to the increased clarity of AI rcommendations [11-13];

– a decrease in the likelihood of erroneous decisions resulting from distrust of the "black box";

– the creatio of a legally significant evidence base for incident investigations.

Conclusion

The conducted research confirms that digital twin technology represents an innovation in the field of cybersecurity. A comparative analysis with traditional cyber ranges has revealed key advantages of the digital twin:

– reation of a dynamic, up-to-date copy of a specific system;

– ca ability for autonomous modeling and two-way communication with the object.

However, the implementation of this promising technology is accompanied by a set of fundamental problems.

The basic problems include:

– critical de endence on the integrity of incoming data;

– occurr nce of errors during the processing of large volumes of telemetry;

– difficulties n integrating with legacy security systems.

A deeper analysis allowed for the identification of two new, poorly studied classes of problems:

– the problem of ensuring cyber resilience in swarms of interconnected digital twins, where the threat of cascade failures is exacerbated by the lack of inter-twin trust mechanisms;

– the problem of security of embedded artificial intelligence, including the risks of adversarial attacks on machine learning models and a crisis of trust due to unverifiable explainability of decisions [14].

6 Conclusion

To address these problems, a set of architecture-oriented solutions has been proposed. A decentralized trust system based on blockchain technology is designed to provide cryptographically secure authentication and data integrity in heterogeneous ecosystems. A collective defense system based on swarm intelligence principles allows for the creation of a self-organizing and adaptive environment that eliminates single points of failure and is capable of autonomous threat response. For protecting artificial intelligence, a multi-layer system combining data filtering, resilience, and testing has been proposed, along with a system of verifiable explainability based on formal verification methods and a distributed ledger to ensure trust and auditability.

The comprehensive implementation of these solutions will enable the automation of a significant portion of routine defensive operations, reduce incident response time, and create a foundation for legally significant auditing of autonomous system actions. The main obstacles to practical implementation remain significant computational costs, the lack of industry standards, and the need for new interdisciplinary competencies. Nevertheless, the proposed methods lay the theoretical foundation for the next generation of digital twins.

REFERENCES

[1] A. S. Minzov, A. Yu. Nevskiy, O. R. Baronov, S.V. Nemchaninova, “Digital Twins in Systems,” *Cybersecurity Issues*. 2024, No. 2(60), pp. 29-35. DOI: 10.21681/2311-3456-2024-2-29-35.

[2] A. V. Fedorova, V. N. Shvedenko, “The Concept of Applying Digital Twin Technology for Integrating Information Systems of Several Enterprises in Merger Conditions,” *Information and Economic Aspects of Standardization and Regulation*. 2023, No. 1 (71), pp. 46-51.

[3] I. S. Khorzova, “Application of Cyber Range Capabilities for Training and Advanced Training of Information Security Specialists,” *Topical Issues of Security Systems and Secure Telecommunications Systems Operation: Proceedings of the All-Russian Scientific and Practical Conference* (Voronezh, June 10, 2021). Voronezh, 2021, pp. 46-47.

[4] E. S. Mityakov, “Digital Twins and Critical Information Infrastructure Security,” *Information Security*. 2024, pp. 29-34. DOI: 10.37468/2307-1400-2024-4-29-34.

[5] E. S. Mityakov, “Problems of Using Digital Twins in Ensuring Information Security of Critical Information Infrastructure Objects,” *Information Technologies and Telecommunications*. 2023, pp. 36-47. DOI: 10.31854/2307-1303-2023-11-4-36-47.

[6] A. R. Kasimova, V. V. Zolotarev, L. Kh. Safiullina, A. S. Balyberdin, “Using a Digital Twin in Information Security Management Tasks. Information Protection Methods and Systems,” *Information Security*. 2023, pp. 49-60. DOI: 10.54398/20741707_2023_1_48.

[7] G. Uteev, R.F. Gibadullin, “Development of a Decentralized Identification System Using Blockchain Technology,” *Informatics and Information Processes*. 2024, pp. 1-16. DOI: 10.23670/IRJ.2024.142.6.

[8] N. M. Ershov, “Development and Research of Distributed Control Algorithms for Swarm Intelligence Systems,” *Mathematical Modeling, Numerical Methods and Software Complexes*. 2022, pp. 21-34. DOI: 10.33693/2313-223X-2022-9-2-21-34.

[9] Adversarial Attacks and Defenses in Generative AI [Electronic resource]. URL: https://translated.turbopages.org/proxy_u/en-ru.ru.58e779a5-692dfe10-a7f83868-74722d776562/https/www.geeksforgeeks.org/artificial-intelligence/adversarial-attacks-and-defenses-in-generative-ai (Accessed: 25.11.2025).

[10] N. V. Shevskaya, “Explainable Artificial Intelligence and Methods for Interpreting Results,” *Modeling, Optimization and Information Technologies*. 2021, pp. 1-12. DOI: 10.26102/2310-6018/2021.33.2.024.
[11] S. S. Galizdra, “Method of biometric identification of a person by a row of teeth based on a photograph with an open smile / S. S. Galizdra, A. Yu. Kudryashova,” *Systems for synchronization, formation and processing of signals*. 2024. Vol. 15, No. 6, pp. 34-39.
[12] A. Y. Kudriashova, S. S. Galizdra and N. V. Toutova, "Designing Implementation of Additional Modules to Increase the Security and Stability of the Biometric Identification System," *2025 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF)*, St. Petersburg, Russian Federation, 2025, pp. 1-5, doi: 10.1109/WECONF65186.2025.11017218.
[13] N. V. Toutova, A. Y. Kudriashova, and S. S. Galizdra, "Implementation of Additional Modules to Increase the Security and Stability of the Biometric Identification System," *2025 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF)*, St. Petersburg, Russian Federation, 2025, pp. 1-5, doi: 10.1109/WECONF65186.2025.11017156.
[14] A. Yu. Kudryashova, V. A. Zakharova, “Development of information security measures for defense industry enterprises to implement the Digital Economy 2030 policy,” *Telecommunications and Information Technologies.* 2024. Vol. 11, no. 2, pp. 45-51.