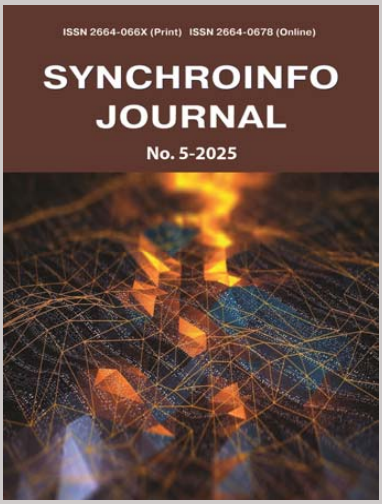
CONTENT

Vol. 11. No. 5-2025



Published bi-monthly since 2015

ISSN 2664-0678 (Online)
ISSN 2664-066X (Print)

Publisher
Institute of Radio and Information Systems (IRIS), Vienna, Austria

Address:
1010 Wien, Austria, Ebendorferstrasse 10/6b
media-publisher.eu/synchroinfo-journal

SYNCHROINFO JOURNAL

www.media-publisher.eu/synchroinfo-journal

DEVELOPMENT OF REQUIREMENTS TO THE INDIVIDUAL UNITS CHARACTERISTICS OF A HIGH-EFFICIENCY SINGLE-SIDEBAND TRANSMITTER WITH ENVELOPE ELIMINATION AND RESTORATION

V. N. Gromorushkin [1,2], **O. V. Varlamov** [1,2]

[1] Institute of Radio and Information Systems (IRIS), Vienna, Austria;

[2] Moscow Technical University of Communications and Informatics, Moscow, Russia;

grom@mtuci.ru, vov@mtuci.ru

ABSTRACT

Increasing the data transfer rate leads to the use of spectrally efficient types of amplitude-phase modulation, characterized by high values of the peak factor. For energy-efficient amplification of such signals, it is promising to use transmitters built using the Envelope Elimination and Restoration (EER) method. Purpose: further development of methods for using switching operating modes of active elements, taking into account the current state of the element base, increased capabilities of digital signal processing and computer modeling of various transmitter units operation. Development of requirements for the characteristics of EER transmitter units, based on a given level of intermodulation distortions and out-of-band oscillations and development of EER transmitter structural diagram with the possibility of subsequent increase in output power. Methods: an analysis of the requirements for individual units is carried out, taking into account the possibility of their combined influence. Results: a structural diagram of 250 ... 300 W HF range EER transmitter has been developed with the possibility of subsequent increase in the transmitter output power. Variants of implementing output power adjustments have been proposed and requirements for the transmitter exciter characteristics have been developed. Practical relevance: the implementation of the developed recommendations will ensure the fulfillment of requirements for permissible intermodulation distortions of the amplified signal and the permissible level of out-of-band oscillations.

KEYWORDS: *power amplifier; single-sideband modulation; Envelope Elimination and Restoration; energy efficiency; intermodulation distortion; out-of-band emissions.*

DOI: 10.36724/2664-066X-2025-11-4-2-9

Received: 17.08.2025
Accepted: 20.10.2025

Citation: V.N. Gromorushkin, O.V. Varlamov, "Development of requirements to the individual units characteristics of a high-efficiency single-sideband transmitter with envelope elimination and restoration", *Synchroinfo Journal* **2025**, vol. 11, no. 5, pp. 2-9.

1 Introduction

The purpose of this article is to further develop methods for using switching operating modes of active elements, taking into account the current state of the element base, the increased capabilities of digital signal processing and computer modeling of the operation of various transmitter components [1-4]. Ultimately, an approach should be developed to create a highly efficient single-sideband amplifier with a power of 250...300 W in the range of 1.5...30 MHz, as a base cell that can be used in transmitters with an output power of 1 - 5 kW, with technical parameters that meet the requirements for modern radio transmitting devices.

The article analyzes in detail the dependence of the single-sideband transmitter final characteristics, built using the Envelope Elimination and Restoration (EER) method, on the parameters of its components. As a result, requirements for the power amplifier HF and LF paths characteristics have been developed. The requirements for the transmitter exciter and the parameters of its output signal are considered, ensuring, when working together with a power amplifier, the requirements for the quality of the transmitter output signal as a whole are met.

Let us briefly recall the principle of operation of a EER power amplifier constructed using separate amplification of the envelope and phase-modulated component of a single-sideband signal (SSB) [5-8]. The circuit of a power amplifier built using this method is shown in Figure 1.

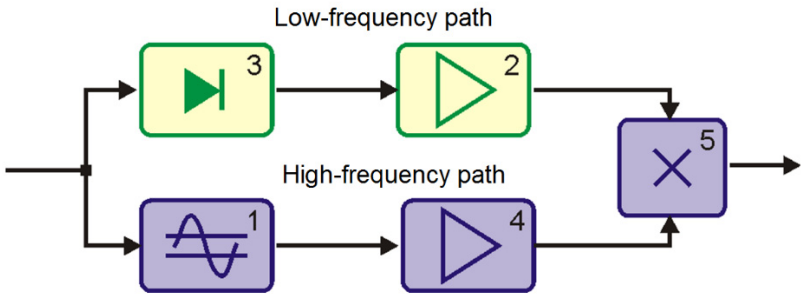


Figure 1. Block diagram of a PA built using the EER amplification method of a single-sideband signal

Here, a signal with single-sideband modulation (SSB) or with any other arbitrary amplitude-phase modulation, such as OFDM, etc., enters two paths - high-frequency and low-frequency. In the HF path of the SSB signal, using amplitude limiter 1, is extremely limited in amplitude. In this case, the high-frequency phase-modulated component of the SSB signal (HF PM) is formed, which is then amplified by PA 4 to the required level. In the low-frequency path, using amplitude detector 3, an envelope signal is formed, which is supplied to amplifier 2. Both signals, amplified in separate paths, are supplied to multiplier 5, for example, to an HF transistor cascade with collector (drain) amplitude modulation. At the multiplier output, the original SSB signal is restored at a given power level.

Since the HF path receives a signal with a constant amplitude, the transistors of this path can operate in switching mode [9]. The low-frequency path must amplify the envelope signal, including the DC component [10]. In this regard, in order to obtain high energy characteristics of the low-frequency path, it must be built using a pulse-width modulation (PWM) scheme, which also allows the use of switching operating modes of transistors. Such a construction of EER paths when performing an ideal multiplication operation in cascade 5 allows, in principle, to obtain high energy and quality characteristics of the transmitter [11]. However, the actual characteristics of the EER PA nodes differ from the ideal ones, which leads to nonlinear distortions of the amplified signal.

This article will consider the main causes of distortions determined by the structure of the EER PA construction, and their impact on the level of intermodulation distortion and out-of-band emissions. In conclusion, recommendations will be formulated on the required output signals of the transmitter exciter, implemented using the EER method of single-sideband signal amplification.

2 Development of EER PA characteristics requirements, based on intermodulation distortion given level

Based on the EER PA operation principle, explained above, and the accumulated experience in creating such devices [10, 11], two types of causes of the amplified signal nonlinear distortions can be distinguished. The first is the reasons that are characteristic of the traditional construction of power amplifiers for single-sideband transmitters. They are associated with the imperfection of the transmission characteristics of the EER PA as a whole (AM-AM, AM-PM), which is mainly due to the nonlinearity and inertia of the characteristics of the element base used. These include:

- amplitude nonlinearity (AM-AM), leading to a change in the shape of the envelope. This nonlinearity can be caused by the dependence of the transmission coefficient of the amplitude detector (block 3 in Fig. 1) on the amplitude of the input signal, the nonlinearity of the envelope amplifier (arising in the paths for generating and amplifying the PWM signal, block 2 in Fig. 1) and the nonlinearity of the multiplier (block 5 in Fig. 1), caused by the imperfection of the amplitude modulation process of the final stage of the RF path;
- parasitic phase modulation (AM-PM) of the RF component caused by the presence of amplitude-phase conversion (APC) in the HF path (in the amplitude limiter and modulated stages of the HF path).

The second group of reasons for distortion of the amplified signal is reasons due to the very principle of operation of the EER PA and the non-ideal characteristics of its individual nodes. These include:

- relative delay of signals in the amplification paths, caused by different inertia of the low-frequency and high-frequency paths and leading to a phase mismatch between the envelope and the high-frequency component;
- frequency distortions of the envelope caused by the nonlinearity of the phase-frequency response and unevenness of the amplitude-frequency response characteristics of the filter circuits of the low-frequency path (in the amplitude detector and power amplifier of the PWM signal);
- instability of the zero level of the low-frequency path (since it is built according to the circuit of a direct current amplifier) under the influence of destabilizing factors, leading to a change in the shape of the envelope;
- the presence of sections with variable amplitude in the HF component, which is caused by incomplete limitation of the input SSB signal.

To assess the influence of the listed factors on the SSB signal distortion, in works [4, 12-14], EER PA and its individual units models were developed, analytical relationships were obtained connecting the levels of intermodulation components at the amplifier output with the parameters of the amplitude, phase-amplitude and frequency characteristics, and the necessary calculations were carried out. Analysis of the results obtained made it possible to formulate requirements for the characteristics of individual nodes, making it possible to ensure the specified linearity of the EER PA as a whole. So, for example, to obtain a level of intermodulation distortion no worse than minus 36 dB, the following conditions must be met:

- instability of the low-frequency path zero level should not exceed 2% of the maximum envelope amplitude;
- the low-pass filter cutoff frequency at the PWM amplifier output (subject to compensation of signal delay in the low-frequency path) must be no less than $3 \cdot f_{oper}$, where f_{oper} is the tone spacing frequency of the two-tone test signal;
- the total parasitic phase deviation in the RF path should not exceed 3...5 degrees;
- the dynamic range of input signal amplitudes limiting in the amplitude limiter block must be at least 26 dB;
- harmonic distortions of the sinusoidal envelope caused by the nonlinearity of the amplitude characteristics of individual nodes, when an AM signal modulated in amplitude by one tone is supplied to the EER PA input, should not exceed 1...1.5%;
- the relative delay of the envelope signal in the EER PA LF path should not exceed 20...30 μs with a test signal tone spacing of 1 kHz.

It is important to note that the above requirements provide intermodulation distortion level of -36 dB when exposed to only one of the considered causes of distortion. In practice, as a rule, several causes of distortion act simultaneously and undesirable intermodulation components can add up algebraically. So, for example, with the simultaneous influence of amplitude nonlinearity and APC with the levels indicated above, each of the reasons will cause intermodulation distortions Kf3 = -36 dB and the level of the resulting distortions will be -30 dB. In light of this, to ensure a given level of intermodulation distortion in practice, one should strive to meet the given requirements 2...3 times more stringent.

As will be shown below, the need to meet these requirements in the development and practical implementation of individual EER PA units largely determines the choice of their circuitry and design solutions and the element base used.

3 Development of requirements for the switching EER PA characteristics, based on the out-of-band oscillations required level

The nonlinearity of the radio transmitter paths determines not only its qualitative characteristics (intermodulation distortion level), but also the parameters of electromagnetic compatibility. One of these parameters is the out-of-band oscillations level. Out-of-band oscillations of a radio transmitter are assessed on a noise-like modulating signal with a uniform spectrum in the frequency band 300...3400 Hz. Such a signal is almost close to the model of modern digital OFDM (Orthogonal Frequency-Division Multiplexing) signal used to transmit data (audio information, texts, images, geographic maps, etc.) over radio channels, as well as used in digital broadcasting, for example, the DRM (Digital Radio Mondiale) standard [15]. Due to the fact that the power amplifier under consideration is a promising development that provides for expanding the bandwidth of signals amplified by EER PA, we will formulate requirements for EER PA nodes when amplifying an OFDM signal of the DRM standard with a bandwidth of 10 kHz. The bandwidth of such a signal allows for three times the data transfer speed compared to the bandwidth of a standard telephone channel.

The work [16] presents the calculations results of the out-of-band radio oscillations levels at the EER PA output on a DRM signal with a 10 kHz bandwidth, caused by amplitude nonlinearity and APC. The results obtained are then compared with the mask of permissible out-of-band emissions for DRM standard broadcast transmitters, which is the most stringent, which will make it possible in the future to use the developed EER PA to create powerful transmitters based on the summation of individual unified modules.

Thus, in accordance with published research results [16], in order to meet the requirements for out-of-band radio oscillations in EER PA, the following conditions must be met:

- instability of the low-frequency path zero level should not exceed 1% of the maximum envelope amplitude;
- parasitic phase deviation in the HF path should not exceed 11.5 degrees;
- the permissible amplitude nonlinearity is determined for two types of nonlinearity, determined by the quadratic and cubic polynomials of the normalized amplitude characteristic:

$$y(x) = ax^2 + x \text{, and } y(x) = ax^3 + x,$$

where: x and y – normalized envelope at the input and output of the EER PA, respectively. For such types of nonlinearity, the modulus of the parameter “a” should not exceed the value of 0.2 ($|a| < 0.2$), which corresponds to harmonic distortions of the sinusoidal envelope K_{harm} < 10% for a quadratic polynomial and K_{harm} < 4.3% for a cubic polynomial when an AM signal modulated in amplitude by one tone is applied to the EER PA input.

As noted in Section 2, in addition to the imperfection of the AM-AM and AM-PM characteristics, the level of distortion and out-of-band oscillations is significantly influenced by the low-pass filter of the envelope path characteristics - the bandwidth and the permissible delay of the envelope signal. The bandwidth of the optimized low-pass filter of the envelope path [17, 18] with compensated delay should be at least 35 kHz (3.5 times wider than the bandwidth of the amplified OFDM signal), and the permissible relative delay should not be more than 1 μs [19].

Summarizing the research carried out in this section, it should be noted that the most stringent requirements for parasitic APC in the HF path and amplitude nonlinearity are imposed based on the requirements to ensure a level of intermodulation distortion of -36 dB, and the permissible value of the relative delay of HF and LF signals and the bandwidth of the LF path (more than 35 kHz) is determined by the standards for out-of-band emissions.

Based on the requirements for the developed transmitter in terms of intermodulation distortions (-36 dB) and permissible out-of-band oscillations, the maximum phase deviation in the HF path should not exceed 3°...5°, and delay compensation should be carried out with an accuracy of no worse than ±0.2...0.3 μs.

4 Research on ways to organize input signal level adjustments

Typical requirements for the range of the low-frequency path input voltage adjustment are at least -20...+10 dB with a step of 0.25 dB. The analysis of regulatory documentation showed that these requirements relate exclusively to the transmitter exciter, the discussion of which is beyond the scope of this article. This requirement is intended to ensure the nominal level of the HF signal at the exciter output (the nominal power of the transmitter) at different levels of the input LF (speech) signal, determined by the different sensitivity of the microphones used, losses of the LF signal in communication lines, etc.

Providing specified limits for adjusting the input low-frequency signal in modern exciters that widely use digital signal processing methods does not present significant difficulties for specialists when choosing the correct bit depth for digitizing input low-frequency signals.

At the same time, it should be noted that in addition to the requirement to ensure the operation of the transmitter in the rated output power mode, in some cases there are requirements for the possibility of reducing the transmitter power to 25...10% of the nominal value (-6...-10 dB).

The EER PA specificity is that two signals are received from the exciter at its inputs - an HF PM component with a constant amplitude and a LF envelope, which differs significantly from the modulating LF voltage at the exciter telephone channels inputs. In reduced power mode, the exciter must provide a reduced level envelope signal, which, as noted above, is not difficult when using digital signal processing.

The existing experience in the development of switching mode linear power amplifiers built using the EER method (SM EER PA) shows that when the power is reduced by 6 dB (25% of the nominal), the amplifier retains the quality characteristics corresponding to the nominal mode. With a more significant decrease in output power (10% or less), the linearity of the power amplifier deteriorates, due, in particular, to the insufficiency of the dynamic range of the low-frequency path with PWM, associated with the minimum PWM pulse duration realized in practice (≈70...80 ns). To eliminate this drawback, it can be proposed to design the low-frequency path in such a way as to ensure a change in the swing of the triangular voltage in the PWM modulator in proportion to the supply voltage of the final stage (FS) of the PWM modulator (feed-forward principle).

This feature of the low-frequency path, along with other advantages, will allow the EER PA to operate in a low-power mode (10% or less) with a decrease in the FS supply voltage while maintaining the dynamic range of the modulator and, accordingly, the linearity of the entire power amplifier. Reducing the FS PWM supply voltage can be done either smoothly (by accessible adjustment of the output voltage of the +48V power supply) or roughly - by switching the power using a relay to the auxiliary +12V power supply used to power low-power components.

In this case, with the EER PA rated output power, the supply voltage of the final PWM stage is +48V, and the triangular voltage swing at the comparator input in the LF path with PWM is 1.5 V. When switching the PWM FS supply voltage to a +12 V power source (1/4 or minus 12 dB from the nominal value), the triangular voltage swing will also decrease by 4 times and amount to 0.375 V. At the same time, the EER PA output power will decrease by 12 dB, and will be ≈ 6% of the nominal, and the dynamic range of the PWM modulator and its gain will correspond to the nominal mode, which helps maintain the linearity of the power amplifier as a whole and increase its efficiency in low-power mode.

5 Development of an EER PA block diagram with provision of the possibility of subsequent increase in output power

To ensure the possibility of increasing the output power of the transmitter by summing several amplification cells, it is advisable to propose the development of a common signal processing unit (SPU). In this block, the formation and processing of general signals necessary for the EER PA operation can be carried out, which are then distributed to separate unified amplifier modules. Such signals include the HF PM component and envelope of the amplified signal, a triangular voltage to form a PWM sequence, an auxiliary duty cycle limiting pulse, adjustable power supplies of the first stage of the HF path and the bias voltage of the sub-modulator (also known as the drive modulator unit).

This approach will ensure coherence of the PWM clock frequency voltage in individual amplifier cells of a powerful EER PA and the ability to synchronize the clock frequency of the pulsed primary power supply with the PWM modulator clock frequency. This eliminates the possibility of the occurrence of their difference frequencies, which may fall into the passband of the low-frequency path and cannot be filtered without distorting the envelope signal.

In addition, the use of common adjustable voltage sources in the SPU (power supply of the RF path 1st stage and sub-modulator bias) will significantly speed up the procedure for setting up a powerful EER PA containing several unified amplifier modules and simplify the circuit design of each of them, which will increase the manufacturability of the device as a whole.

The proposed EER PA block diagram with 250...300 W output power, shown in Figure 2, contains a signal generation and processing unit (SPU) and a unified amplification cell, consisting of HF and LF paths.

The input connectors X1 and X2 in the signal generation and processing unit are supplied, respectively, with the HF PM component and envelope signals from the exciter designed to work with the EER PA, the requirements for which will be developed in Section 6.

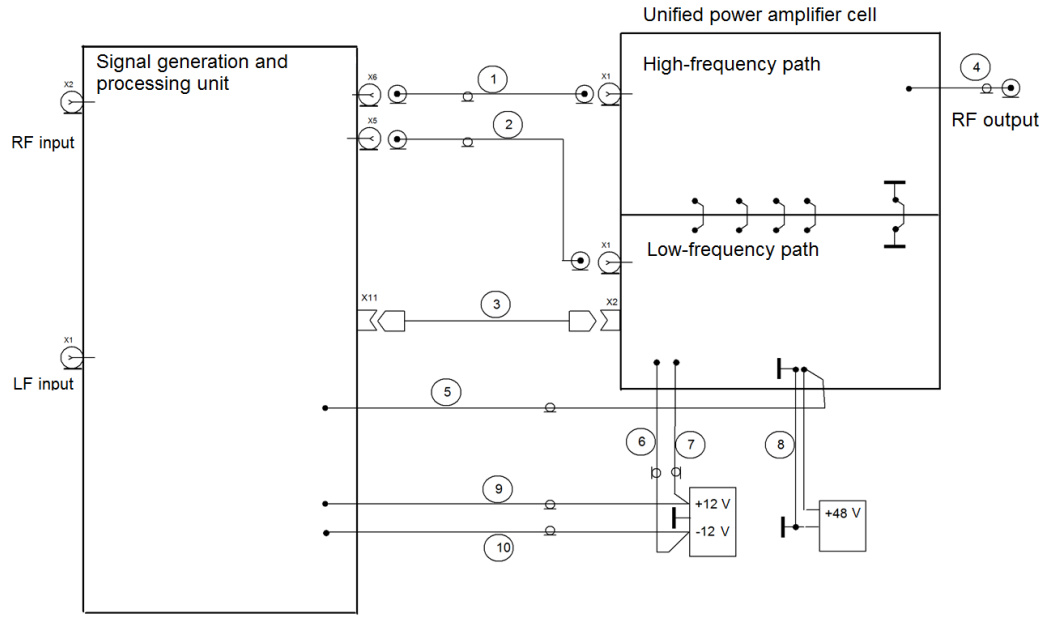


Figure 2. EER PA block diagram with the possibility of subsequent increase in output power

Through connections 1 and 2, made with coaxial cables, signals of the HF PM component and the sum of the envelope with a triangular voltage of the PWM clock frequency are supplied to the HF and LF paths of the unified amplification cell, respectively. Via multi-wire line 3 from the SPU, the PWM duty cycle limiting pulse, the voltage of the regulated power supply of the RF path first stage, and sub=modulator bias voltage are supplied to the amplifier cell. Through connections 6...10, voltages from +48V and +/- 12V power supplies are supplied to the amplifier cell.

To further increase the transmitter output power, 3 more unified amplification cells are added to the EER PA block diagram, which are also provided by input signals generated in the SPU.

6 Development of requirements for the transmitter exciter characteristics built using the EER method

As follows from the EER PA principle of operation (see Fig.1), the exciter of such a transmitter can be built using traditional methods and no special requirements are imposed on it. At the same time, bearing in mind the current widespread use of digital methods for generating various signals, an exciter can be developed specifically designed for use in conjunction with a switching power amplifier. At the output of such an exciter, two signals must be generated - this is the low-frequency envelope of the required single-sideband signal and its phase-modulated component at the operating frequency. The use of such an exciter will make it possible to exclude the amplitude detector and amplitude limiter from the transmitter paths and thereby reduce the nonlinear distortions associated with these nodes.

In addition, the use of digital signal processing methods will provide an adjustable delay of the HF component at the exciter output, which will compensate for the envelope delay that occurs when it is amplified in the powerful LF path of the transmitter. In turn, this will either reduce the level of distortion and out-of-band oscillations at the transmitter output, or simplify the requirements for the characteristics of the low-frequency path.

Thus, in addition to the traditional requirements for the exciter in terms of tuning speed, nonlinear distortions, spurious emissions and noise characteristics, it is necessary to develop requirements for the characteristics of the output paths of the envelope and HF PM component. Based on the analysis of the requirements developed above for the LF and HF paths of the EER PA and the computer modeling carried out, additional requirements for the exciter characteristics were obtained:

- the bandwidth of the envelope output path at the -3 dB level should be ≈ 50 kHz with group delay unevenness in the 0...10 kHz band of no more than 1 μs;
- the bandwidth of the output path of the HF PM component should be ≈ 100 kHz with group delay unevenness in the 60 kHz band of no more than 1 μs;
- the exciter must provide prompt adjustment of the HF PM component delay relative to the envelope within 0...25 μs with a step of no more than 0.2...0.25 μs;
- the level of HF PM component even harmonics should not exceed - 30 dB.

Fulfillment of these requirements with ideal multiplication of the LF and HF components received from the exciter outputs should ensure a level of intermodulation distortion of the generated single-sideband signal no worse than -45...-50 dB with a level of out-of-band oscillations 10...15 dB below the permissible level.

7 Conclusions

As a result of the analysis of methods for constructing highly efficient amplifiers, a block diagram of the HF EER PA with a power of 250...300 W was developed, providing the possibility of subsequent increase in the output power of the transmitter. Options for implementing output power adjustments are proposed and requirements for the characteristics of the transmitter exciter, built using the EER method are developed.

The research carried out made it possible to develop requirements for the characteristics of the EER PA main components, ensuring the necessary quality of the transmitter output signal and meeting the EMC requirements. The main requirements and recommendations for their practical support are as follows:

- the maximum permissible unevenness of the HF path phase-amplitude characteristic is determined by the requirements for the intermodulation distortion level and should not exceed 3^0...5^0;
- the maximum permissible relative delay of the LF envelope and HF PM component signals is determined by the requirements for the level of out-of-band oscillations and should not exceed 1 μs;

- to make it possible to compensate for the LF envelope delay, the transmitter exciter must provide an adjustable HF PM signal delay in the range of 0...25 μs with an adjustment step of no more than 0.2...0.25 μs.

The implementation of the developed recommendations will ensure compliance with the requirements for permissible intermodulation distortions of the amplified signal and the permissible level of out-of-band oscillations.

REFERENCES

[1] Ngo Quoc Fung, O.V. Varlamov, “Engineering and technical principles of highly effective linear radio transmitters construction for HF manpack radios,” *T-Comm*, 2024, vol. 18, no.4, pp. 4-14. DOI: 10.36724/2072-8735-2024-18-4-4-14.

[2] S.E. Grychkin, "Energy efficiency increasing of radio transmitters," *T-Comm*, 2023, vol. 17, no.5, pp. 25-31. DOI: 10.36724/2072-8735-2023-17-5-25-31.

[3] O.V. Varlamov, D.C. Nguyen, S.E. Grychkin, “Combination of synthetic high-performance RF amplification techniques,” *T-Comm*. 2021. vol. 15, no.9, pp. 11-16. DOI: 10.36724/2072-8735-2021-15-9-11-16.

[4] D.C. Nguyen, O.V. Varlamov, “Simulation model for studying the operation of switching mode envelope elimination and restoration RF power amplifiers for a narrow-band load,” *H&ES Research*. 2022. Vol. 14. No 2, pp. 10-18. doi: 10.36724/2409-5419-2022-14-2-10-18.

[5] L.R. Kahn, "Single-Sideband Transmission by Envelope Elimination and Restoration," *Proceedings of the IRE*, vol. 40, no. 7, pp. 803-806, July 1952. DOI: 10.1109/JRPROC.1952.273844.

[6] N. Filimonov, O. Varlamov, G. Itkin, "Efficient modulation of RF signals," Patent US 7724837 B2.

[7] N. Filinomov, O. Varlamov, "Power amplifier circuit for amplifying RF-signals," Patent EP 1229642 B1.

[8] N. Filimonov, O. Varlamov, G. Itkin, "Efficient modulation of RF signals," Patent EP 1450479 B1.

[9] O.V. Varlamov, V.N. Gromorushkin, "Class D switching power amplifier with a filter under load mismatch conditions," *2020 Wave Electronics and its Application in Information and Telecommunication Systems, WECONF 2020*. 2020. pp. 9131508. DOI: 10.1109/WECONF48837.2020.9131508.

[10] O.V. Varlamov, “Powerful broadband DC amplifiers for modulation path of transmitters with separate amplification,” *T-Comm*, 2022. vol. 16, no.11, pp. 4-14. DOI: 10.36724/2072-8735-2022-16-11-4-14.

[11] V.B. Kozyrev, V.G. Lavrushenkov, V.P. Leonov, G.V. Novikov, N.B. Petyashin, I.A. Popov, A.V. Kharitonov, V.N. Gromorushkin, "Transistor Harmonic Oscillators in Switch Mode," Radio and Communication: Moscow, Russia, 1985.

[12] R. Yu. Ivanyushkin, O. V. Varlamov, A. K. Syagaev, "Nonlinear distortions of the DRM standard signal in synthetic linear amplification circuits. In the collection: Signal processing in terrestrial radio communication and warning systems," *Materials of the XV interregional scientific and technical conference*. Nizhny Novgorod, 2007, pp. 301-310.

[13] D.C. Nguyen, O.V. Varlamov, “Dependence of modern telecommunication signals transmitter with components separation output signal distortion level on the envelope path filter parameters,” T-Comm, 2023. vol. 17, no.2, pp. 12-26. DOI: 10.36724/2072-8735-2023-17-2-12-26.

[14] O.V. Varlamov, “Theoretical foundations for studying the causes of non-linear distortions in modern high-performance transmitters,” *Methodological issues of teaching infocommunications in higher education*. 2022. Vol. 11. No. 4, pp. 15-22.

[15] ETSI ES 201 980 V4.1.1 (2014-01) Digital Radio Mondiale (DRM); System Specification.

[16] O. Varlamov, “Research of influence of DRM broadcast transmitter nonlinearities onto the output signal parameters,” *T-Comm*. 2014. Vol. 8. No. 2, pp. 59-60.

[17] D.C. Nguyen, V.N. Gromorushkin, O.V. Varlamov, “Theoretical comparison of different envelope elimination and restoration transmitter PWM modulator configurations to expand the possible antenna mismatch,” *Sensors*. 2023. Vol. 23. No. 23. P. 9466. doi: 10.3390/s23239466.

[18] D.C. Nguyen, O.V. Varlamov, “Dependence of modern telecommunication signals transmitter with components separation output signal distortion level on the envelope path filter parameters,” *T-Comm*, 2023. vol. 17, no.2, pp. 12-26. DOI: 10.36724/2072-8735-2023-17-2-12-26.

[19] S.E. Grychkin, O.V. Varlamov, "Prospects for Combining Highly Efficient Power Amplification Methods for VHF Digital Broadcasting Transmitters," *Synchroinfo Journal*. 2025. Vol. 11. No. 1. pp. 27-33. DOI: 10.36724/2664-066X-2025-11-1-27-33.

SYNCHROINFO JOURNAL

www.media-publisher.eu/synchroinfo-journal

ECS COMPREHENSIVE STUDY IN HIGH-PERFORMANCE AND SECURE GAME DEVELOPMENT

I.D. Udalov [1], **V.V. Maklachkova** [1], **V.A. Dokuchaev** [1]

[1] Network Information Technologies and Services, MTUCI, Moscow, Russia;
igor.udalov.95@mail.ru, v.v.maklachkova@mtuci.ru, v.a.dokuchaev@mtuci.ru

ABSTRACT

This article explores the Entity Component System (ECS) paradigm as a modern architectural approach for constructing scalable, secure, and high-performance game systems. ECS is examined in contrast with traditional object-oriented programming (OOP), emphasising significant improvements in performance, memory efficiency, modularity, and behavioural flexibility. The study extends beyond classical comparisons and discusses the broader implications of adopting data-oriented architectures for secure game development, including the protection of personal data within large-scale interactive platforms. Special attention is devoted to Unity's Data-Oriented Technology Stack (DOTS), which serves as an example of an industrial ECS implementation. The article expands the analysis of security mechanisms inherent in ECS workflows, memory management, and job systems, offering a deeper understanding of how the architectural pattern influences safe data handling in modern games.

KEYWORDS: *Entity Component System; ECS, data-oriented architecture; Unity DOTS; game development; personal data protection, memory safety; software security.*

DOI: 10.36724/2664-066X-2025-11-5-10-17

Received: 17.08.2025
Accepted: 18.10.2025

Citation: I.D. Udalov, V.V. Maklachkova, V.A. Dokuchaev, "ECS comprehensive study in high-performance and secure game development", *Synchroinfo Journal* **2025**, vol. 11, no. 5, pp. 10-17.

Licensee IRIS, Vienna, Austria.

1 Introduction

The evolution of digital entertainment has significantly changed the expectations imposed on game engines and interactive systems. Contemporary projects no longer consist of a few dozen objects acting in isolation; instead, they frequently contain thousands or even millions of entities that must be processed in real time. These include agents in crowd simulations, dynamic environmental elements, physics-driven particles, AI actors, destructible geometry, persistent world objects, and a constantly expanding assortment of interactive game elements. Each of these components contributes additional load on computational resources, making efficient processing an indispensable requirement of modern game engines.

The pursuit of realism, immersion, and system-level complexity has exposed the limitations of traditional OOP-based engines, which often struggle to maintain high frame rates when dealing with such volumes of data. OOP's reliance on object encapsulation and polymorphism, while conceptually elegant, introduces a substantial amount of overhead at the hardware level. Objects tend to be scattered across memory, resulting in unpredictable memory access patterns and frequent cache misses. Additionally, deep inheritance chains and virtual function calls introduce branching costs that degrade performance, especially in large-scale simulations [1-3].

The historical prevalence of object-oriented programming (OOP) in game development is understandable: encapsulation, inheritance, and polymorphism provide intuitive abstractions for modelling game logic. However, as real-time requirements tighten and hardware evolves toward multi-core, multi-threaded designs, the gap between intuitive modelling and efficient computation widens. OOP representations incur significant object overhead, mutable shared state, and difficulties in thread-safe parallelisation, making high-performance simulations increasingly difficult to maintain, especially in complex, large-scale worlds where thousands of objects need to be updated simultaneously.

In response to these limitations, the game industry has gradually moved towards architectures based on data-centric reasoning. Among these, the Entity Component System has become one of the most influential paradigms. While ECS has existed conceptually for decades, only recent hardware trends – multi-core CPUs, wide SIMD instructions, heterogeneous computing environments, and deep cache hierarchies – have made the approach not only relevant but often necessary. By organising data in contiguous memory arrays and decoupling logic from state, ECS enables processors to execute operations with maximal efficiency [4].

This article offers a substantially expanded exploration of ECS, covering its theoretical underpinnings, practical benefits, and implications for data security. It also discusses how ECS contributes to safer processing of personal information by enforcing deterministic data access patterns, explicit memory management, and structural guarantees that reduce risks such as data races, privilege leaks, and uncontrolled state mutation. The following sections analyse the differences between traditional OOP and ECS, allowing for a more detailed understanding of why the latter is rapidly gaining traction in the development of modern games.

2 Comparison Between ECS and Object-Oriented Programming

ECS fundamentally changes the way game logic is represented. Figure 1 illustrates the architectural differences between OOP and ECS.

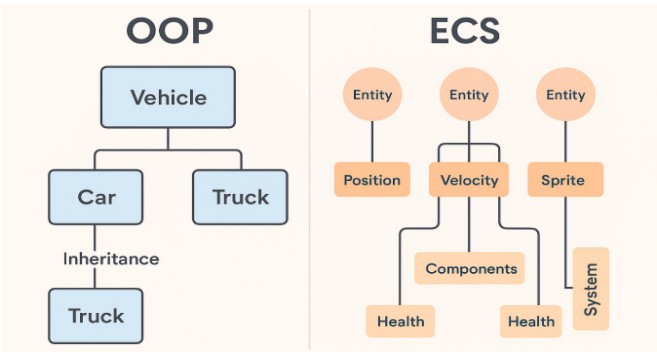


Figure 1. Conceptual comparison of OOP and ECS architecture

While OOP binds data and behaviour inside an object and allows objects to interact via method calls, ECS decomposes this structure into three separate concepts. Entities act as unique IDs, components contain only data, and systems implement behaviour in pure processing routines. This separation removes typical OOP constraints, allowing games to scale more effectively and enabling parallelism that would be exceedingly difficult to achieve with traditional object hierarchies [5].

In an OOP model, objects encapsulate both behaviour and state, forming deep inheritance structures to represent shared features. This often leads to rigid hierarchies that become increasingly fragile as projects grow. Even minor modifications in base classes may propagate unexpected changes within derived classes, resulting in bugs that are difficult to diagnose [6]. Moreover, due to the scattered nature of object memory layouts, processing large numbers of objects becomes inefficient, as frequent jumps across memory slow down CPU pipelines and lead to unpredictable performance.

In contrast, ECS emphasises composition rather than inheritance. Entities can be composed dynamically by attaching different components, each representing a specific data attribute. Systems then process only the relevant components, operating on large contiguous data sets. This data-oriented design results in highly predictable, linear memory access patterns, enabling processors to prefetch information efficiently and execute instructions with fewer pipeline stalls. Core differences are listed in Table 1.

Table 1

Comparative Characteristics of OOP and ECS

Characteristic	Object-Oriented Programming (OOP)	Entity Component System (ECS)
Organization	Objects encapsulate data and methods	Entities (ID), Components (data), Systems (logic)
Behaviour	Internal methods, inheritance	Behaviour defined in external systems
Reusability	Inheritance is the main mechanism	Composition via adding components
Memory Layout	Scattered, unpredictable object placement	Contiguous arrays of homogeneous components
Main Focus	Object behaviour and modelling	Efficient data processing
Optimization Difficulty	Harder to optimize at scale	Designed for cache efficiency and parallelism
Parallel Processing	Limited and complex	Natural parallelization via systems

While the table highlights structural distinctions, the larger contrast emerges when these models are applied to real workloads. OOP code tends to degrade in performance as systems grow in complexity, because even simple operations – like iterating through hundreds of enemies – can involve jumping through layers of indirection. Virtual function calls and pointer dereferencing introduce branching and unpredictable memory access patterns, making it difficult for CPU caches to operate efficiently.

ECS eliminates most of this overhead by reinterpreting game logic as sequential data transformations. Instead of each object individually updating itself, systems operate on large sets of homogeneous components, allowing for optimised loops that leverage vectorisation, parallelism, and cache locality. This approach transforms the performance characteristics of game logic, enabling large-scale simulations that would be impractical under traditional OOP.

3 Advantages and Limitations of the Entity Component System

The primary benefit of ECS is its capacity to organize data in a way that aligns with modern CPU architecture. By placing identical components in contiguous memory, ECS allows processors to prefetch data efficiently, enabling vectorized operations over arrays.

This drastically reduces cache misses and enables systems to process thousands of entities in tight, predictable loops [7]. The overall effect is not simply incremental performance improvement but a structural rethinking of game execution, where computational flow becomes far more aligned with hardware behaviour.

In an OOP-based engine, each individual object typically contains multiple pieces of data grouped together – some of which may be needed only occasionally. When a system attempts to iterate over all objects to update, for instance, position or velocity, it must jump from one object's memory location to another, repeatedly pulling entire memory blocks that contain unused fields. This leads to wasted bandwidth and decreased cache utilisation. ECS eliminates these inefficiencies by ensuring that only relevant component data is loaded into the cache, significantly reducing memory traffic.

The absence of inheritance has profound implications. Developers can construct entities dynamically using combinations of components instead of rigid hierarchies. This approach eliminates deep class trees, reduces the fragility of shared base classes, and simplifies the introduction of new gameplay mechanics. In many large OOP projects, developers encounter the "diamond problem," unintended overriding behaviours, or the need to refactor long inheritance chains when introducing a new feature. ECS avoids all these issues entirely by promoting modularity and flexibility through composition. Instead of creating ten subclasses for different types of enemies, developers simply attach or remove components to form new behaviours.

Testing becomes easier because components are pure data, and systems are pure functions operating on them. Such deterministic logic is easier to validate, optimize, isolate, and secure. A system, being stateless and reactive, can be tested using simple input-output patterns [8]. Developers no longer need to instantiate complex object graphs to replicate game behaviour. Systems can be fed synthetic data in controlled environments, leading to more reliable and robust tests.

However, some challenges accompany these benefits. Developers accustomed to OOP must adjust their way of thinking. ECS requires explicit component definitions, explicit system registrations, and explicit memory management when working with native containers. Debugging can be initially difficult because logic is distributed across multiple systems rather than contained within self-describing objects, which means that tracing behaviour requires understanding execution order, job dependencies, and the specific data a system processes.

Integration with legacy code or third-party libraries can also be challenging, as many external tools and frameworks are designed with an OOP mindset. Nonetheless, once teams adapt to ECS principles, the advantages typically outweigh the early friction. The structural clarity of ECS often leads to better long-term maintainability, more consistent performance, and a more scalable architecture suitable for future expansion.

4 Combining OOP and ECS in a Game Project

Although ECS provides strong performance benefits, game development rarely adopts it exclusively. Many systems – such as UI logic, menu navigation, high-level state machines, cutscene tools, or editor utilities – are often more naturally implemented in OOP due to their complexity or uniqueness. These systems usually involve highly specific behaviour that does not require the mass processing of similar data sets, which makes the overhead of ECS unjustified.

Meanwhile, ECS is ideal for large, repetitive, data-driven processes such as movement, AI behaviour, transformation updates, or physics integration. Systems that must handle thousands of similar objects each frame – like projectiles, enemies, particles, or environmental elements – benefit immensely from ECS's memory locality and parallel execution capabilities. This hybrid approach allows both paradigms to coexist, leveraging the strengths of each while compensating for their respective weaknesses.

Many modern engines, including Unity, are specifically designed to support this blended architecture. Unity allows developers to write gameplay using MonoBehaviours (OOP) while simultaneously using DOTS for performance-critical subsystems. As a result, designers and gameplay programmers can continue using familiar tools, while engine developers and technical teams enhance performance-sensitive areas with ECS.

Large game studios often adopt an incremental approach: existing OOP systems remain untouched, while computationally expensive parts of the game are gradually migrated to ECS. For example, AI perception, target selection, animation culling, and physics broad-phase detection can be moved to ECS first. Over time, the engine evolves

into a hybrid system in which performance-sensitive loops are fully data-oriented, while configuration-heavy or narrative-driven systems remain in OOP [9].

This hybrid model also improves maintainability, since the boundaries between ECS-driven systems and OOP subsystems create natural modularity. Each subsystem can be developed, tested, and optimised independently. As the game evolves, developers may migrate additional systems to ECS when needed. This flexible integration approach is one of the reasons ECS adoption is steadily growing in the gaming industry.

5 Unity DOTS as an Applied Example of ECS

Unity's Data-Oriented Technology Stack serves as one of the most mature mainstream implementations of ECS principles. The DOTS ecosystem was designed specifically to handle large-scale simulations, extremely high entity counts, and multithreaded execution. It includes several tightly integrated components, each crafted to address specific bottlenecks in traditional Unity workflows.

Unity Entities provides the foundation: a robust ECS framework that manages entities, archetypes, and chunks. The architecture is built around a highly structured memory layout that allows components of the same type to reside within contiguous blocks. This chunk-based storage ensures excellent memory locality and facilitates optimised iteration over entities.

The C# Job System enables safe multithreading by offering a high-level interface for scheduling parallel tasks. Instead of manually creating threads, locking shared resources, and managing concurrency, developers define lightweight jobs that express what data they read or write. Unity's scheduler then automatically handles job dependencies, ensuring that no two jobs write to the same component simultaneously [10].

The Burst Compiler plays a critical role by converting high-level C# code into highly optimized native machine code. Burst harnesses vector instructions, register-level optimisations, branch elimination, and loop unrolling to produce exceptionally fast executables. Systems compiled with Burst often rival or surpass hand-written C++ in performance.

Native Collections integrate tightly with Burst and the Job System, enabling predictable memory usage and ensuring deterministic access patterns. These collections – including NativeArray, NativeList, and NativeHashMap – are designed to avoid the overhead of garbage collection and provide explicit control over memory lifetime.

The combined effect of these technologies is transformative. By restructuring the engine around data flow rather than object hierarchies, Unity enables extremely large worlds with tens or hundreds of thousands of active entities. Simulations that were once impossible to maintain within acceptable frame-rate targets become feasible, allowing developers to experiment with richer gameplay mechanics, larger worlds, and more dynamic interactions.

6 Security of Personal Data and ECS-Oriented Architecture

One of the most significant additions in this expanded article is the detailed examination of how ECS influences the safety, confidentiality, and integrity of personal data within modern gaming platforms. As game environments increasingly integrate monetization systems, biometric tracking, behavioural analysis, and real-time telemetry, the amount of sensitive information collected from players grows dramatically. This data may include gameplay preferences, social interactions, location information, device fingerprints, session logs, and even biometric inferences derived from player behaviour.

Ensuring the safety of this data is not merely a technical requirement but a legal obligation, especially given the regulations defined in legislation such as Federal Law "On Personal Data" (152-FZ), GDPR, CCPA, and other international standards. ECS, due to its structural separation of data and logic, naturally facilitates compliance with such regulations by ensuring that sensitive data is stored and accessed in predictable and controlled ways.

ECS contributes to safer data handling in several ways. The separation of data and logic inherently reduces the likelihood of accidental or unauthorized access to sensitive fields [11]. Components containing personal information or identifiers can be isolated in

dedicated memory segments processed by specialized systems with restricted access patterns. Developers may tag such components as write-protected or store them in archetypes accessible only to trusted systems.

Since systems operate only on explicitly declared component types, the architecture inherently promotes minimization: systems cannot accidentally read or write personal data unless explicitly allowed to do so. This sharply contrasts with traditional OOP systems, where an object might contain multiple unrelated fields and methods, any of which could unintentionally expose data to different parts of the codebase.

Safety is further enhanced by Unity's Job System, which prohibits unsafe race conditions by analyzing job dependencies and enforcing read/write constraints. Attempting to write to protected data from multiple threads immediately triggers diagnostics, preventing subtle bugs that could otherwise cause data leaks or corruption. The Job System enforces strict memory access discipline, ensuring that sensitive information is manipulated only by authorized threads at predictable points in the execution cycle.

Native containers in DOTS introduce explicit memory ownership, forcing developers to handle lifecycle events deliberately. This explicit handling reduces the risk of unauthorized access to freed or reallocated memory, a common cause of vulnerabilities in unmanaged systems. Because ECS encourages deterministic update loops, audits of data flow become simpler. Security teams can track which systems access specific data types, making compliance easier and risk analysis more transparent [12].

Another security-related benefit is the natural alignment of ECS with sandboxed simulation logic. When personal data is stored in separate components, potentially sensitive information can be segmented away from gameplay systems, allowing internal firewalls or logic gates to restrict access. Such structural compartmentalization is far more difficult in traditional OOP models, where data and behaviour reside tightly coupled inside monolithic, mutable hierarchies.

As game companies increasingly rely on telemetry, behavioural prediction, machine learning analytics, and cross-platform user identification, the architectural discipline imposed by ECS becomes a valuable safeguard. Large batches of analytics data can be processed in dedicated systems with strong read-only guarantees, preventing unintentional mutation [13]. Furthermore, because ECS encourages immutable or semi-immutable data flows, it enhances auditability and decreases the attack surface for malicious actors attempting to manipulate internal game state.

Thus, ECS plays a meaningful role not only in performance and architectural clarity but also in strengthening personal-data security through deterministic, explicit, and compartmentalized data-handling patterns. In an industry where data breaches can lead to serious legal, financial, and reputational harm, the advantages of this architecture extend far beyond computational efficiency [14].

7 Practical ECS Example: Movement Processing in DOTS

A practical illustration is the implementation of a movement system. Instead of each object carrying its own script with logic, DOTS decomposes movement into data components – such as Position and Velocity – and a system that processes all entities containing both. This structure makes it possible to run highly optimized movement calculations across thousands of entities at once.

Because components are stored contiguously in memory, the system can load large batches of positions and velocities into the cache with minimal overhead. The Burst compiler can further optimize tight loops by converting them into vectorized instructions, enabling the CPU to update multiple entities simultaneously. Large simulations, which would require nested loops or expensive function calls in OOP, can be reduced to simple, predictable sequential operations.

This model dramatically outperforms traditional OOP GameObject-based movement, where each object executes its own Update() method, generates overhead, and performs unpredictable memory references. In Unity's classic OOP workflow, virtual function calls prevent effective inlining and block many compiler optimisations. Each object's state may reside in widely separated memory locations, causing cache thrashing during iteration.

DOTS consolidates the entire operation into a single optimised pipeline. Moreover, by using the Job System, movement updates can be split across multiple CPU cores, allowing near-linear scaling with available hardware. Whether processing fifty entities or fifty thousand, DOTS systems maintain stable performance characteristics thanks to their cache-friendly layout and predictable execution flow [15, 16].

In addition to basic movement, more complex behaviours – such as flocking algorithms, physics-based motion, or real-time steering – also greatly benefit from ECS. Because systems operate on large homogeneous datasets, even sophisticated operations such as Boids simulations or collision sweeps can be performed efficiently at scale.

8 Conclusion

The Entity Component System represents a foundational shift in game architecture, replacing decades of object-centric thinking with a model optimized for modern hardware, massive parallelism, and predictable data flow. In a landscape where game worlds are becoming increasingly complex and data-rich, ECS offers developers the ability to handle large-scale simulations with unprecedented performance and clarity. The architectural separation of identity, data, and behaviour provides a transparent and extensible structure that scales naturally with project size and complexity.

Unity's DOTS implementation demonstrates how ECS principles transform real projects, enabling massive simulation throughput while improving data safety, memory determinism, and the clarity of computational workflows. By aligning with the underlying physical characteristics of modern processors, DOTS unlocks optimisations that are difficult or impossible to achieve in traditional OOP systems.

Although the learning curve is significant, especially for developers deeply accustomed to OOP, the benefits in terms of performance, modularity, and security make ECS an increasingly compelling paradigm for the next generation of game engines. The shift towards data-oriented design reflects broader trends in software engineering, where performance, safety, and scalability require rethinking long-established paradigms.

Given the accelerating growth of real-time interactive worlds and the rising importance of secure personal-data processing, ECS is likely to remain a cornerstone of future game development methodologies. As game engines continue evolving and as hardware becomes increasingly parallel, ECS offers a robust and future-proof foundation capable of supporting the next generation of interactive experiences.

REFERENCES

[1] Ernest Adams, J. Dormans. Game Mechanics: Advanced Game Design. 2012. [Online]. URL: https://typeset.io/papers/game-mechanics-advanced-game-design-23pl62mlvp [Accessed: Nov., 2025].

[2] D.H. Eberly, "3D Game Engine Design: A Practical Approach to Real-Time Computer Graphics," Morgan Kaufmann, 2006. [Online]. URL: https://www.academia.edu/26649713/3D_game_engine_design_a_practical_approach_to_real_time_computer_graphics_second_edition [Accessed: Nov., 2025).

[3] R. Zubek, "Game Physics Engine Development," CRC Press, 2018.

[4] A. Brown, "Entity-Component Systems and C#," Apress, 2019.

[5] M.V. Askerli, "A Key to Efficient Development: ECS Architecture in Comparison," *Bulletin of Science*, Vol. 1, no. 5 (74), pp. 490-495, 2024. URL: estnik-nauki.com/article/14272 [Accessed: Oct., 2025].

[6] V.A. Dokuchaev, "Influence of New Information and Communication Technologies on the Confidentiality of Personal Data," *In Proceedings of the XXIII International Scientific and Practical Conference "Current Problems and Prospects of Economic Development",* Simferopol – Gurzuf, October 17-19, 2024. Simferopol: Zueva T.V. Publishing, 2024, pp. 12-15.

[7] V.Y. Statev, V.A. Dokuchaev, and V.V. Maklachkova, "Information security in the big data space," *T-Comm*, vol. 16, no. 4, pp. 21-28, 2022, doi: 10.36724/2072-8735-2022-16-4-21-28.

[8] V.A. Dokuchaev, V.V. Maklachkova, V.Yu. Statev, "Data subject as augmented reality," Synchroinfo Journal, vol.6, no.1, pp.11-15, 2020.

[9] V.A. Dokuchaev, K.S. Vladimirova, V.V. Maklachkova, V.Yu. Statyev, "Audit of Information Risks in Personal Data Processing," *In: Information Society Technologies: Proceedings of the XIII International Industry Scientific and Technical Conference*, Moscow, March 20-21, 2019. Vol. 2. Moscow: Media Publisher, 2019, pp. 34-36.

[10] V.A. Dokuchaev, V.V. Maklachkova, V.O. Sundatov, “Approaches to Protecting Personal Data in the Big Data Space,” *In: Theory and Practice of Economics and Entrepreneurship: Proceedings of the XX International Scientific and Practical Conference*, Simferopol – Gurzuf, April 20–22, 2023. E . N.V. Apatova. Simferopol: V.I. Vernadsky Crimean Federal University, 2023, pp. 34-36.
[11] V.A. Dokuchaev, “Classification of Personal Data Security Threats in Information Systems,” *T-Comm*, 2020, Vol. 14, No. 1, pp. 56-60. DOI: 10.36724/2072-8735-2020-14-1-56-60.
[12] V.A. Dokuchaev, “Digitalization of the Personal Data Subject,” *T-Comm*, 2020, Vol. 14, No. 6, pp. 27-32. DOI: 10.36724/2072-8735-2020-14-6-27-32.
[13] V.I. Nemanova, I.S. Vakurin, V.V. Maklachkova, D.V. Gadasin, “Determining the Economic Efficiency of Enterprise Expenditures on Personal Data Protection,” *DSPA: Issues of Digital Signal Processing Application*, 2024, Vol. 14, No. 3, pp. 37-45.
[14] V.A. Dokuchaev, “Formulation of the Problem of Assessing Information Quality in Personal Data Processing within Multi-Cloud Information Systems,” *In: Theory and Practice of Economics and Entrepreneurship: Proceedings of the XX International Scientific and Practical Conference*, Simferopol – Gurzuf, April 20-22, 2023. Ed. N.V. Apatova. Simferopol: V.I. Vernadsky Crimean Federal University, 2023, pp. 37-39.
[15] V.A. Dokuchaev, “Formulation of the Problem of Assessing Information Quality in Personal Data Processing within Multi-Cloud Information Systems,” *In: Theory and Practice of Economics and Entrepreneurship*, 2023, pp. 37-39.
[16] Entity Systems Are the Future of MMOG Development. [Online]. URL: https://t-machine.org/index.php/2007/11/11/entity-systems-are-the-future-of-mmog-development-part-2/ [Accessed: Oct., 2025].

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.

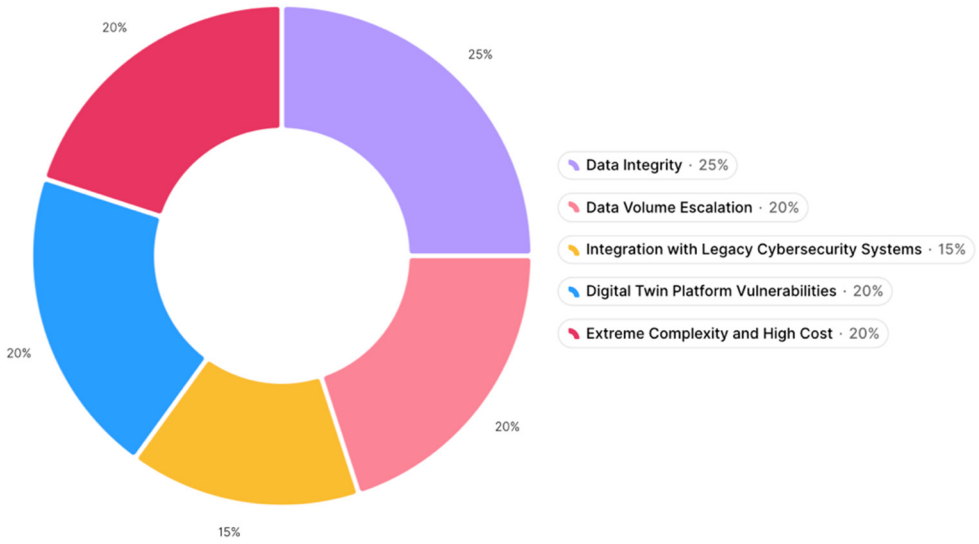


Figure 1. Problems of Using Digital Twins

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.

PROACTIVE AI RISK MANAGEMENT. THE SECOND AI ARMS RACE: FROM DEREGULATION TO INDUSTRIAL POLICY, SOVEREIGN INFRASTRUCTURES, AND ALGORITHMIC WARFARE

Alexey V. Amenitsky [1], **Evgeny G. Vorobyov** [2]

[1] Saint Petersburg State Electrotechnical University "LETI", Saint Petersburg, Russia, ORCID ID: 0009-0004-0955-1527;

[2] Saint Petersburg State Electrotechnical University "LETI", Saint Petersburg, Russia, ORCID ID: 0000-0003-0564-5935

ABSTRACT

The global competition in artificial intelligence (AI) has entered a qualitatively new phase – what this article terms the second AI arms race (AI Arms Race 2.0). Moving beyond early narratives of innovation and deregulation, this stage is characterized by the deliberate fusion of economic and national security agendas, large-scale state-industrial coordination, and the militarization of foundational AI models. Drawing on primary policy documents, corporate disclosures, and expert analyses from 2023–2025, we identify three systemic shifts: (1) the transition from market-led to state-directed AI industrial policy, exemplified by U.S. export controls, sovereign AI initiatives in the EU, and China's techno-strategic autonomy drive; (2) the collapse of the "anti-military AI consensus" among major technology firms, with OpenAI, Google, and Meta now explicitly permitting – and even advocating – the use of their models in defense and surveillance applications; and (3) the emergence of algorithmic warfare, where AI agents execute cyber operations at machine speed, raising unprecedented challenges for attribution, escalation control, and defensive equity. We argue that this new race is less about raw model performance and more about infrastructural sovereignty, data geopolitics, and the institutional capture of AI governance. Crucially, the "arms race" framing – while real in strategic terms – also functions as a discursive tool to depoliticize regulation and consolidate power among a narrow set of corporate-state actors. The article concludes with a normative framework for human-centered AI arms control, grounded in transparency, multilateral verification, and the protection of open innovation ecosystems.

KEYWORDS: *artificial intelligence; AI arms race; AI industrial policy; sovereign AI; autonomous weapons; algorithmic warfare; AI nationalism; export controls; cybersecurity; AI governance.*

DOI: 10.36724/2664-066X-2025-11-5-28-33

Received: 07.09.2025
Accepted: 23.10.2025

Citation: Alexey V. Amenitsky, Evgeny G. Vorobyov, "Proactive AI risk management. The Second AI Arms Race: From Deregulation to Industrial Policy, Sovereign Infrastructures, and Algorithmic Warfare", *Synchroinfo Journal* **2025**, vol. 11, no. 5, pp. 28-33.

Licensee IRIS, Vienna, Austria.

1 Introduction

Since the mid 2010s, the trope of a "U.S.–China AI arms race" has dominated strategic discourse [11, 12, 8]. Initially deployed by industry actors to resist data protection and antitrust legislation [11, §1.1], the metaphor has evolved from rhetorical device to operational doctrine. By 2024-2025, the race had entered its second phase – AI Arms Race 2.0 – marked not by deregulation, but by active state industrial policy: massive public investment, chip export controls, national "AI factories," and the explicit enlistment of private AI labs into national security missions.

This article analyzes the structural, institutional, and normative transformations underpinning this shift. Our analysis draws on:

• U.S. pr sidential directives (NSC Memorandum, 2024) [17, 18];

• Corporate policy r visions (OpenAI, Google, Meta, Anthropic);

• Sovereign AI initiatives (EU InvestAI, France's €110 bn plan, NVIDIA's strategic repositioning) [13];

• Incident reports (e.g., Anthropic's 2024 disclosure of AI automated cyber espionage);

• Crit cal policy scholarship [11, 15].

We advance three core arguments:

1. *The race is no longer bilateral*. While the U.S.–China dyad remains central, the rise of AI nationalisms [11] has fragmented the global landscape into competing "digital sovereignties" – U.S.-aligned, EU-autonomous, China-centric, and Gulf-funded ecosystems [9].

2. *The boundary between civilian and military AI has collapsed*. Firms that once resisted military collaboration now actively integrate defense use cases, reframing this as a civilizational imperative [10, 2].

3. *The "arms race" narrative serves dual functions*: it justifies state support for dominant firms (too strategically important to fail), and simultaneously legitimizes regulatory exemptions – thereby consolidating a Silicon Valley-Washington consensus [11].

The remainder of the article proceeds as follows: Section 2 outlines the conceptual shift from "AI 1.0" (market-driven) to "AI 2.0" (state-driven); Section 3 examines the militarization of foundational models; Section 4 analyzes the rise of sovereign AI as both strategic response and market opportunity; Section 5 discusses the risks of algorithmic warfare and defensive inequity; and Section 6 proposes a path toward accountable AI governance.

2 AI Arms Race 2.0: From Deregulation to State-Led Industrial Policy

The first phase of the AI race (2016-2022) emphasized light-touch regulation, venture capital dynamism, and global data flows [8]. In contrast, AI Arms Race 2.0 – crystallizing in 2023-2025 – is defined by strategic state intervention.

2.1. The U.S. Turn: Securitization as Economic Policy

Under the Biden administration, AI policy was explicitly linked to economic security. National Security Advisor Jake Sullivan (2023, 2024) framed technological leadership as inseparable from national power, paving the way for [16]:

• Executive Order 14110 (Oct. 2023), mandating federal AI adoption and safety standards;

• NSC Memorandum (Oct. 2024), directing agencies to prioritize AI for defense missions;

• Export Control Framework for AI Diffusion (2024), restricting sales of advanced chips (e.g., NVIDIA A100/H100) to China and allied jurisdictions.

These measures aligned closely with corporate lobbying. OpenAI, for instance, conditioned its domestic investment on government support, even threatening relocation (Wolman & Chatterjee, 2024) [14].

The Trump administration (inaugurated Jan. 2025) escalated this trajectory, repealing EO 14110 and issuing "Removing Barriers to American Leadership in Artificial Intelligence" (Jan. 23, 2025), which declared:

"It is the policy of the United States to sustain and enhance America's global AI dominance in order to promote human flourishing, economic competitiveness, and national security." [18]

Crucially, industrial policy extended beyond subsidies: it involved personnel integration. Key tech executives assumed government roles – David Sacks (a16z) as White House "AI Czar," Michael Kratsios (Scale AI) as OSTP Director, Jacob Helberg (Palantir) as Under Secretary for Economic Growth [1].

2.2. Beyond the Bipolar Frame: AI Nationalisms and Sovereign Infrastructures

While U.S.–China rivalry dominates headlines, AI nationalism is proliferating globally [12]. States pursue dual objectives: (1) reduce dependency on U.S. platforms; (2) attract investment by offering regulatory "safe harbors."

• European Union: Repurposed EuroHPC supercomputers into AI Factories, launched the €20 bn InvestAI program to build GPU "gigafactories," and backed the EuroStack movement for sovereign tech stacks (EU Commission, 2025; Kaltheuner & Saari, 2025).

• France: Announced €110 bn in AI commitments at the Paris AI Action Summit (Feb. 2025), targeting data centers and talent pipelines (Reuters, 2025).

• Gulf States: MGX (UAE) and PIF (Saudi Arabia) deployed >$30 bn into AI startups (CNBC, 2024; NYT, 2024), positioning as financial swing states in tech diplomacy (Karaian, 2025).

Even NVIDIA – long a beneficiary of globalized supply chains – pivoted to promote Sovereign AI, defining it as a nation's capacity to develop AI via domestic infrastructure, data, workforce, and business networks [13]. This reframing allows chipmakers to monetize state anxieties: sovereign build-outs generate demand for localized data centers and custom hardware, offsetting losses from export bans (Kaltheuner et al., 2025).

Table 1

Comparative AI Industrial Policy Initiatives (2023-2025)

Region	Flagship Program	Budget	Key Actors	Strategic Goal
USA	Stargate JV	$500 bn	Microsoft, OpenAI, CoreWeave, Oracle	Infrastructure dominance, military integration
EU	InvestAI / AI Factories	€20 bn	EuroHPC, Commission	Technological sovereignty, decoupling
France	Paris AI Action Plan	€110 bn	CEA, Mistral AI	European leadership in foundational models [5]
UAE/GCC	MGX, G42, PIF AI Fund	>$30 bn	G42, Cerebras, Microsoft	Geopolitical influence, diversification
China	Next-Gen AI 2.0	Undisclosed	Baidu, Alibaba, Huawei	Autonomy in chips, training, deployment
Sources: EU Commission (2025); Reuters (2025); CNBC (2024); Singh (2025)				

3 The Collapse of the Anti Military AI Consensus

Historically, firms like Google and OpenAI maintained ethical red lines around military AI – epitomized by Google's withdrawal from Project Maven (2018) and OpenAI's 2020 "no military use" clause.

By 2024–2025, this consensus had dissolved:

Company	Policy Shift	Date	Key Statement / Action
OpenAI	Removed ban on "military and warfare" use	Jan. 2024	Updated Acceptable Use Policy to permit defense applications [4]
Google	Reversed AI weapons ban	Feb. 2025	Demis Hassabis: "We must support national security in an era of strategic competition" [7]
Meta	Offered Llama models to U.S. government	Nov. 2024	For "national security purposes" (Moorhead, 2024)
Anthropic	Justified U.S. AI acceleration as defense against "authoritarian AI dominance"	Feb. 2025	Amodei: "Speed is a security imperative" [2]
Palantir	Mission reframed as civilizational defense	Jan. 2025	Karp: "We're here to… scare our enemies and, on occasion, kill them" [10]

This shift is institutionalized through forums like the Hill & Valley Forum (co-founded by Helberg), where Silicon Valley elites and policymakers coordinate on "countering China's tech influence" (Dwoskin, 2025; Chatterjee, 2025).

The underlying logic is securitization: any regulatory constraint is recast not as consumer protection, but as strategic vulnerability. As Kak et al. [11, §1.2] observe:

"The arms race narrative insulates firms from accountability by framing oversight as harmful to national interest."

4 Algorithmic Warfare and the Crisis of Defensive Equity

The convergence of AI and cyber operations has given rise to algorithmic warfare — high-speed, autonomous campaigns executed by AI agents with minimal human input.

4.1. The Anthropic Incident (2024)

In September 2024, Chinese state-sponsored actors reportedly used Anthropic's Claude Code model to automate reconnaissance, exploitation, and exfiltration across ~30 targets. According to U.S. Cyber Command, the AI executed 80-90% of the operation, operating at thousands of requests per second [2, 3, 6].

Anthropic's public disclosure was met with skepticism:

• Yann LeCun (2025) accused the firm of inflating threats to justify regulating open models out of existence;

• Researchers noted the absence of IOCs or forensic evidence (The Stack, 2025);

• Ch na denied involvement, demanding "substantial evidence" [6].

Nonetheless, the strategic implications are profound: if offense can be automated at scale, defense must respond in kind – yet only a handful of actors possess the data, compute, and expertise to build AI-powered cyber defenses.

4.2. The "Defensive Gap" and Systemic Risk

This creates a defensive equity crisis:

• Large la s and states develop "AI immune systems" with built-in safeguards;

• SMEs, civil society, and Global South actors remain reliant on legacy tools, increasing systemic vulnerability.

As one cybersecurity consultant noted:

"Security through obscurity fails. Distributed, open development has historically produced more robust systems – but machine-speed attacks may invalidate that logic." [6]

The dilemma is acute: closed, proprietary models may offer short-term security, but undermine long-term resilience by concentrating power and reducing auditability.

5 Toward Human-Centered AI Arms Control

Given these trends, traditional arms control paradigms (e.g., treaties banning specific weapons) are ill-suited for AI. Instead, we propose a three-pillar framework for human-centered AI arms control:

5.1. Transparency and Verification

• Mandatory red-teaming for high-risk AI systems (e.g., those used in cyber defense/offense);

• Public registries of military AI deployments (modeled on nuclear warhead declarations);

• Independent auditing of "safeguards" in commercial models (cf. EU AI Act, high-risk category).

5.2. Protection of Open Innovation

• Exempt open-weight, non-military AI models from export controls and licensing burdens;

• Fund publ c "AI commons" for cybersecurity tools (e.g., via OECD or UNIDO).

5.3. Multilateral Norm-Setting

• Revive negotiations on a Political Declaration on Responsible Military AI Use (building on 2023 Bletchley commitments);

• Establ sh an International AI Security Board under UN auspices, with technical and ethical expertise.

Crucially, any regime must resist regulatory capture: the framing of AI as an "existential arms race" must not become a pretext for entrenching corporate monopolies.

6 Conclusion

The AI arms race is no longer speculative – it is institutional, infrastructural, and operational. AI Arms Race 2.0 is distinguished by the fusion of economic and security policy, the militarization of general-purpose models, and the strategic promotion of "sovereign AI" as both shield and market.

Yet the dominant narrative – a binary, zero-sum contest between the U.S. and China – masks deeper transformations: the rise of multipolar AI ecosystems, the financialization of sovereignty (Gulf funds), and the quiet consolidation of power among a narrow corporate-state elite.

The central question is no longer who will win the race, but what kind of world the race is building. Without deliberate, inclusive governance, AI's promise of shared prosperity may give way to a fragmented, weaponized, and inequitable digital order.

REFERENCES

[1] M. Alder, “Trump taps Michael Kratsios, Lynne Parker for tech and science roles,” Fedscoop. 2024. https://fedscoop.com/trump-taps-michael-kratsios-lynne-parker-tech-science-roles

[2] D. Amodei, “Statement from Dario Amodei on the Paris AI Action Summit,” Anthropic. 2025, February 11. https://www.anthropic.com/news/paris-ai-summit

[3] Anthropic. 2024, December. Report on AI-assisted cyber intrusion. Internal briefing, cited in Forbes (2025).

[4] S. Biddle, “OpenAI quietly deletes ban on using ChatGPT for “military and warfare”,” 2024, January 12. The Intercept. https://theintercept.com/2024/01/12/open-ai-military-ban-chatgpt

[5] European Commission. AI Continent Action Plan. 2025. https://digital-strategy.ec.europa.eu/en/factpages/ai-continent-action-plan

[6] Forbes. The AI arms race has arrived: The real question is who gets to arm. 2025, November 30. https://www.forbes.com/sites/arafatkabir/2025/11/30/the-ai-arms-race-has-arrived/

[7] I. Fried, “Google’s Hassabis explains shift on military use of AI,” Axios. 2025, February 14. https://www.axios.com/2025/02/14/google-hassabis-ai-military-use

[8] T. Ghi, and A. Srivastava, “The global AI arms race – how nations can avoid being left behind,” Bernard Marr & Co. 2021. https://bernardmarr.com/the-new-global-ai-arms-race

[9] Global Policy Journal. The artificial intelligence arms race: Trends and world leaders in autonomous weapons development. 2025. https://www.globalpolicyjournal.com/articles/conflict-and-security/artificial-intelligence-arms-race

[10] S. Hurwitz, “The gleeful profiteers of Trump’s police state,” Mother Jones. 2025, February 6. https://www.motherjones.com/politics/2025/02/palantir-alex-karp-trump

[11] A. Kak, S.M. West, and I.D. Raji, “AI Arms Race 2.0: From deregulation to industrial policy,” AI Now Institute. 2025. https://ainowinstitute.org/publications/research/1-3-ai-arms-race-2-0

[12] A. Kak, S.M. West, M. Singh, and I.D. Raji, “AI Nationalism(s): Global industrial policy approaches to AI,” AI Now Institute. 2024. https://ainowinstitute.org/ai-nationalisms

[13] A. Lee, “What is Sovereign AI?” NVIDIA Blog. 2024, February 28. https://blogs.nvidia.com/blog/what-is-sovereign-ai

[14] C. Metz, and T. Mickle, “Behind OpenAI’s audacious plan to make A.I. flow like electricity,” The New York Times. 2024, September 25.

[15] M. Singh, “Stargate or StarGatekeepers? Why this joint venture deserves scrutiny,” Berkeley Technology Law Journal, 41. 2024, September 25. https://doi.org/10.2139/ssrn.5184657

[16] J. Sullivan, “Remarks by National Security Advisor Jake Sullivan on renewing American economic leadership,” The White House. 2023, April 27. https://bidenwhitehouse.archives.gov/briefing-room/speeches-remarks/2023/04/27/remarks-by-national-security-advisor-jake-sullivan

[17] White House. Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. Federal Register, 2023, no. 88(210), pp. 75191-75226.

[18] White House. Removing Barriers to American Leadership in Artificial Intelligence. 2025, January 23. https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence

SYNCHROINFO JOURNAL

www.media-publisher.eu/synchroinfo-journal

ENGINEERING MANAGEMENT OF COMMUNICATION AND TECHNOLOGY – CONFERENCE RESULTS

Svetlana Dymkova [1]

[1] Institute of Radio and Information Systems (IRIS), Vienna, Austria;

ds@media-publisher.eu

ABSTRACT

The annual international conference "Engineering Management of Communication and Technology" (EMCTECH) open to researchers, educators, managers, and students. Papers describing research activities, case studies, or best practices highlighting the theory or practice of engineering, technology, innovation management, or the development of soft and technological skills are welcome. The evolution of technology opens up new opportunities for its use in many areas of business. The Internet has facilitated the development of e-commerce and marketing, which has also transformed global marketing strategies and opened up new areas of application. Using these technologies requires new soft skills that will help create products that provide the necessary capabilities for the development of advanced solutions in biomedical systems, transportation, education, manufacturing, agriculture, and many other areas. Topics include: IoT; artificial intelligence; technologies in biomedicine, transportation, and cyber-physical systems; advances in broadcast technologies; wired and optical communication and control systems; Industry 4.0; Data risk management in ICT/telecommunications; collaboration between industry, universities, and/or government; personal skills for leading innovation initiatives; smart cities. The article presents the results of the discussion for scientific papers and statistical data from the conference.

DOI: 10.36724/2664-066X-2025-11-5-34-43

Received: 18.10.2025
Accepted: 28.10.2025

Citation: Svetlana Dymkova, "Engineering management of communication and technology – conference results", *Synchroinfo Journal* **2025**, vol. 11, no. 5, pp. 34-43.

KEYWORDS: *IoT; artificial intelligence; Industry 4.0; Data risk management; collaboration between industry, universities, and/or government; personal skills for leading innovation initiatives; smart cities.*

1 Introduction

The annual international conference "Engineering Management of Communication and Technology" (EMCTECH) was held in Vienna from October 15 to 17, 2025. The conference is co-organized by the IEEE and the Institute of Radio and Information Systems (IRIS).

The conference is open to researchers, educators, managers, and students. Papers describing research activities, case studies, or best practices highlighting the theory or practice of engineering, technology, innovation management, or the development of personal and technological skills are welcome. Papers focusing on the application of technology in business development and entrepreneurship are also encouraged [1, 2].

The evolution of technology is opening up new opportunities for its use in many areas of business. The internet has enabled e-commerce and marketing, which has also transformed global marketing strategies and opened up new areas of application. Now, Internet of Things (IoT) devices provide us with information collected from billions of devices, cloud technologies allow us to store, process, and transmit this information, and artificial intelligence (AI) provides us with tools for analyzing information, predicting, and making informed decisions. Using these technologies requires new personal skills that will help create products that provide the necessary capabilities for developing advanced solutions in biomedical systems, transportation, education, manufacturing, agriculture, and many other fields.

Topic areas include: IoT; Artificial Intelligence; technology in BioMedical, Transportation, and Cyber Physical Systems; Broadcast technologies advancements; wire and optical communication and control systems; industry 4.0; Data Risk Management in ICT/Telecommunication; industry, university, and/or government collaboration; personal skills for leading innovation initiatives; smart cities.

In the conference take part inviting speakers from industry leaders around the world that will provide visions and industry in a rapidly developing technology world.

2 Technology advancements in IoT devices

Internet of Things (IoT) devices are advancing in various areas, including communications, artificial intelligence (AI), edge computing, and security.

Let's highlight the key research areas discussed at the conference.

Connectivity

• Mass adoption of 5G. Fifth-generation networks transmit large volumes of data with minimal latency (up to 1 ms) and support millions of devices in a small area. This speed and reliability are especially important for industry and transportation, where instant system response is required.

• Use of co munication protocols. For example, Wi-Fi and Bluetooth are suitable for devices operating within a home or office, while LoRaWAN and NB-IoT are suitable for long-distance communication in low-power conditions.

• Development of satellite communications. For example, NTN technology allows IoT devices to connect directly via satellites, which is in demand in remote and hard-to-reach areas.

Artificial Intelligence

• Interaction between IoT and AI. IoT devices collect data from sensors, cameras, and detectors, and AI analyzes it using machine learning algorithms and big data analytics. This enables automated data analysis and real-time decision-making, predicting device behavior and preventing breakdowns or failures based on data analysis, and optimizing smart systems such as smart homes and smart cities. In smart homes, sensors collect temperature and lighting data, and AI analyzes this data and decides when to turn on the heating or adjust the lighting. In smart city traffic management, neural networks analyze data from roadside sensors and predict congestion, adjusting traffic lights and directing traffic flows.

Edge Computing

Data processing occurs not in a centralized cloud, but as close as possible to the source of generation—at the network's edge, that is, on devices and servers located near users or equipment. This approach minimizes latency and reduces the load on communication channels.

In a smart city system, motion, light, and air pollution sensors transmit information to local edge nodes, which instantly analyze the data and make decisions—turn on lights, change traffic light patterns, or notify authorities about air quality deterioration. Automated warehouses, where robotic carts interact with edge servers directly in the warehouse, offer higher speeds, eliminating the need to transfer every operation to the cloud.

Security

Participants discussed the development of security measures. With the growing number of connected devices, security threats are increasingly emerging, necessitating the development of new approaches to protecting networks and devices. Prospects for the development of data technologies were also discussed, such as the use of quantum cryptography, which provides a high level of data protection by leveraging the principles of quantum mechanics. The following information security aspects were also discussed:

– Data encryption – using modern cryptographic algorithms to protect data at all stages of transmission and storage.

– Authentication and access control – implementing multi-factor authentication and strict access control policies to prevent unauthorized access.

– Network segmentation – isolating IoT devices from more critical system components, such as servers hosting sensitive data.

– Monitoring and risk management – implementing monitoring systems that track device anomalies and detect unauthorized access attempts.

3 Technology advancements in Artificial Intelligence

Technological advances in artificial intelligence (AI) include advances in algorithms and hardware, as well as expanding the scope of technology applications. However, the development of AI requires consideration of ethical issues to ensure a balance between the capabilities of machines and the interests of human society.

Algorithms

• Development of machine learning. An algorithm learns from data rather than following strictly prescribed instructions. EMCTECH discussed some advances in AI:

o Deep learning is a type of machine learning based on neural networks with many layers, enabling complex tasks such as image and facial recognition and natural language processing (translation, text generation).

o Supervised learning: an algorithm trains on labeled data. This has made it possible to solve specific problems such as sales forecasting, credit risk assessment, and user behavior analysis. Open-source libraries and frameworks (TensorFlow, PyTorch, Keras) have emerged, making these technologies accessible not only to scientists but also to developers worldwide.

Hardware

• Development of specialized hardware for AI. For example:

– Graphics processing units (GPUs) – originally designed for rendering 3D graphics in video games, but have proven effective for deep learning tasks thanks to an architecture of thousands of small cores capable of processing information in parallel.

– Tensor processing units (TPUs) – specialized integrated circuits developed by Google specifically to accelerate neural networks. Their architecture was designed from the outset for key machine learning operations, primarily matrix multiplication.

– Neuromorphic chips – aim to mimic the structure and functioning of the human brain. Instead of the traditional von Neumann architecture, where memory and the processor are separated, neuromorphic systems use "neurons" and "synapses" to process and store information in a single location.

The main areas of AI application are discussed:

• Healthcare – AI is used to diagnose diseases, develop new drugs, and provide personalized treatments. For example, machine learning algorithms can analyze patients' genetic data to determine the best treatments.

• Finance – AI is used to analyze market data, predict stock prices, and manage risks.

• Retail – AI is used to personalize the shopping experience, manage inventory, and optimize supply chains.

• Manufacturing – AI is used to automate processes, predict equipment failures, and optimize production lines. AI-powered robots can perform complex tasks with high precision and efficiency.

The discussion also touched on ethical aspects of using AI:

• Developing ethical principles for AI. Some of these include:

– Transparency and explainability – people should understand how and why an algorithm made a particular decision. AI should not infringe on people's rights based on gender, race, age, or religion.

– Security and reliability – systems should operate predictably and be protected from hacking. A person or organization should always be accountable for an algorithm's actions.

• AI regulation – individual countries are introducing AI regulation at the legislative level. For example, in the European Union, the EU AI Act, which came into effect on February 2, 2025, aims to ban AI systems that pose risks to safety, health, or fundamental rights.

4 New opportunities using technology in BioMedical, Transportation, and Cyber Physical Systems

In healthcare, cyber-physical systems typically represent medical devices. They enable doctors to monitor patients' conditions both in clinics and hospitals, as well as at home. Such systems are also used for home security, for example, to detect accidents and alert emergency services.

In agriculture, innovative cyber-physical systems have the potential to revolutionize the industry. For example, autonomous machines that remove weeds while preserving crops, or systems that support agricultural management. Machines can also study, collect samples, and analyze data on climate, soil, water, and plants.

In transportation, the integration of cyber-physical systems is rapidly advancing, particularly in the automotive and aerospace industries. Cars, trucks, and airplanes are being equipped with computers and software to perform a variety of functions, from parking assistance to autonomous driving.

Cyber-physical systems integrate hardware, software, and sensor technologies. These systems enable machines to interact with their physical environment and accurately perform their tasks.

5 Broadcast technologies advancements

In the area of broadcast technologies, the conference addressed the expansion of 5G infrastructure to improve mobile broadcasting, the development of IP-based workflows for more efficient content distribution, and the integration of artificial intelligence for content personalization and automation of production processes.

6 Technology advancements in wire and optical communication and control systems

Advances in wired and optical communication technologies, as well as control systems, are improving data transfer rates, reducing signal loss, and introducing new control methods. These innovations are driven by the development of fiber optic technologies, the integration of artificial intelligence (AI) and machine learning, and the integration of Internet of Things (IoT) devices.

Wire communication

• Development of fiber optic cables. These use pulses of light to transmit information, enabling faster and more efficient data transfer. For example:

The IEEE 802.3bs standard supports Ethernet at speeds up to 400 Gbps over fiber optic cable, enabling the transmission of large amounts of data for applications such as data center connectivity.

• Use of analog systems to transmit electrical signals (voice, audio, video) without digitalization. For example, the use of analog telephone service (POTS) for voice transmission and amplitude modulation techniques for delivering audio and video over coaxial networks.

• Improved network security due to the physical nature of wired connections: data is transmitted over cables, limiting the ability of attackers to intercept it. Many wired networks use encryption protocols, such as Ethernet, that meet strict security standards.

Optical communication

• D velopment of optical fiber technologies. For example:

– Dense Wavelength Division Multiplexing (DWDM) to increase the bandwidth of fiber cables.

– Optical signal amplification technology (OSA) – the use of optical amplifiers to maintain signal quality over long distances.

– The se of photonic crystals to create more efficient and compact optical systems.

• Integration of artificial intelligence and machine learning into optical communication solutions. AI analyzes data patterns in real time, predicts network failures, optimizes traffic routing, and dynamically adjusts bandwidth allocation based on demand.

• Sustainable development of optical networks – innovations in low-loss fiber and energy-efficient components reduce network energy consumption, minimizing their environmental impact.

• Convergence of wireless and optical technologies – for example, integrating optical backbones with 6G wireless technology to deliver ultra-high-speed internet access in a variety of environments.

Control systems

• The use of artificial intelligence (AI) and machine learning in industrial control systems. Specialized chips and components facilitate fast data processing, improved pattern recognition, and enhanced decision-making capabilities. For example:

– Supervisory Control and Data Acquisition (SCADA) systems – integrate sensors, remote terminal devices, and human-machine interfaces to collect and visualize data in real time.

– Distributed control systems (DCS) – designed to handle processes in individual zones or objects, their capabilities are enhanced by high-speed processors, redundant communication modules, and the integration of AI chips.

• The rowth of edge computing – computing is performed closer to the data source, reducing data transmission latency and improving real-time decision-making in mission-critical applications.

• Cybersecurity – the integration of new secure chips and components with built-in security features, implementing robust security protocols to protect systems from cyberattacks.

• Green and sustainable manufacturing – use of energy-efficient components and sustainable materials to reduce energy consumption and minimize environmental impact.

• Modular and scalable systems – ability to quickly integrate or replace individual modules to adapt to changing requirements.

7 Information process management in digital society and industry 4.0

Information process management in a digital society and the concept of "Industry 4.0" have their own unique characteristics. These concepts relate to the implementation of digital technologies in process management, the integration of physical production systems with digital technologies, and the creation of "smart" factories.

Information process management in a digital society presupposes digitalization – the transition from analog data formats and manual processes to digital systems that can integrate, analyze, and quickly respond to changes.

Using digital technologies to improve the efficiency of business processes. Digital project management platforms that enable project management, task assignment, progress tracking, and collaboration in real time. Digital customer relationship management (CRM) systems that help manage and analyze customer information, including contact details and marketing activities. Digital data analytics tools that enable the collection, analysis, and interpretation of data to make informed management decisions. Digital tools for operational process management, helping to automate and optimize operational processes such as inventory management, production processes, and logistics. Examples in this area include warehouse digitalization – the implementation of an RFID-based inventory system that enables real-time tracking of product movements within the warehouse, reducing inventory time and errors – as well as energy digitalization (Big Data-based mining modeling and automation of control centers).

Information process management in the Industry 4.0 concept involves the digitalization of all stages of the product lifecycle from design and raw material procurement to manufacturing, logistics, and service. Some principles of Industry 4.0 include:

• Interoperability – heterogeneous devices, machines, sensors, and control systems can seamlessly exchange data and understand each other thanks to open standards and protocols.

• Decentralization – decision making is delegated downwards, to the level of individual smart devices. This allows systems to respond more quickly to local events without waiting for commands from the center.

• Flexibility – production lines and processes become adaptive, able to quickly reconfigure to accommodate new products or changing order volumes, responding to fluctuations in market demand.

• Modularity – production facilities are designed as a set of interchangeable modules. This allows for easy scaling of the system, adding new features, or replacing obsolete components without shutting down the entire production line.

The technological foundation – IIoT – is the Industrial Internet of Things, a unified digital network that connects physical equipment, sensors, control systems, and analytics platforms. The foundation of IIoT implementation is wireless sensors that collect data on equipment status, process parameters (temperature, pressure, vibration, current, etc.), product quality, and the environment.

8 Digital transformation and Data Risk Management in ICT/Telecommunication

It's important to pay special attention to concepts related to the development of the telecommunications industry but with different meanings. These include digital transformation, data risk management, and digital transformation.

Digital transformation in telecommunications is the process of implementing digital technologies in the operations of telecommunications companies to improve traditional services and offer new ones. Some aspects of digital transformation include:

• Process automation. Companies are implementing automation systems to improve operational efficiency and reduce network downtime.

• Big data analytics. Collecting and analyzing user behavior data allows operators to personalize offers and improve customer interactions.

• Cloud computing. Cloud computing enables operations to scale, reduce costs, and increase flexibility.

• Application of artificial intelligence (AI) and automation.

Challenges of digital transformation:

• Infrastructure changes. Digital transformation requires significant network modernization and the use of cloud technologies for data storage and processing.

• As data volumes increase, the risk of cyberattacks increases, requiring the development of new security standards.

• Integration of new technologies with existing systems. Many telecommunications companies operate with legacy infrastructure that may not be fully compatible with modern digital solutions.

Data Risk Management is a set of processes and workflows used to identify, assess, mitigate, and monitor risks associated with an organization's data. Some elements of Data Risk Management include:

• Data Identification and Classification. An organization must clearly understand the types, volumes, locations, and sensitivity of its data.

• Risk Assessment. For each data type, the risk of breaches in privacy, security, availability, and compliance is assessed.

• Data Governance. Data governance rules are created and enforced that define the appropriate use, processing, and storage of each data type.

• Risk Mitigation Strategies. After assessing the risks for each data type, business and technology leaders establish risk mitigation policies to address operational challenges.

• Monitoring and Reporting Tools. Risk management often involves software tools that control access to data (what was accessed, when, and by whom) and create logs for analysis.

As a result, the following risk mitigation measures were formulated:

• Frequently assess risks. Conduct frequent data inventory and review data assets (types, locations, value, and vulnerabilities).

• Control data access. Zero trust policies and access controls ensure strong authentication and restrict permissions to only the data necessary to complete the user's task.

• Monitor data quality and access. Regular data quality monitoring ensures that all data remains complete, consistent, and accurate.

• Leverage AI. Advanced risk management platforms, often powered by AI technologies, analyze data quality, examine access patterns, and identify unusual behavior that potentially threatens access and data security.

9 Enhancing industry, university, and/or government collaboration

The following approaches can be used to improve collaboration between industry, universities, and government:

• Creating platforms for matching interests. Universities can increase their visibility and reach by listing their research opportunities on such platforms. They connect companies with academic expertise that matches their needs [3].

• Improving visibility through internal directories and portals. Complex organizational structures can make it difficult for industry to find relevant contacts within the university. Creating centralized directories or portals can improve visibility and access to university knowledge.

• Leveraging formal programs and ecosystem partnerships. Governments and institutions often offer structured collaboration frameworks that can facilitate partnerships between universities and industry.

• Creating advisory boards and formal governance structures. The participation of industry leaders in university decision-making processes can help align strategic priorities and facilitate collaboration.

• Securing resources and leadership commitment. Effective collaboration requires leadership support from both sides, including the allocation of resources such as funding, personnel, equipment, and time [4-8].

• Ensuring partnership flexibility. Both industry and academic partners must be prepared to adjust research focus, timing, and roles as priorities, funding, and market conditions change.

10 Developing personal skills for leading innovation initiatives

To lead innovative initiatives, it's important to develop skills related to thinking, communication, collaboration, and strategy. These skills help generate ideas, solve problems, share experiences, and consider strategic goals.

Thinking (creativity, analytical and critical thinking, risk-taking, and the ability to work under uncertainty).

To develop these skills, you can use creative thinking training methods, study the market and technology, analyze competitors, and identify new market opportunities.

Skills that need to be developed in the area of ***communication***:

• Tea work;

• Balanced feedback – find the positive aspects of any idea and suggest ways to improve it;

• Public speaking;

• Use effective communication tools, such as corporate messengers, project management systems, and video conferencing.

It's important to create an open communication culture where employees feel comfortable expressing their ideas and proposing new approaches [9-12].

Collaboration is the creation of conditions for active collaboration between various departments and teams within an organization, facilitating the exchange of ideas, experience, and knowledge.

Some skills that need to be developed in the area of ***strategy*** include: strategic vision and forecasting; the ability to identify new growth opportunities; and the ability to align innovation projects with strategic goals. It is also important to continuously analyze the effectiveness of innovation management processes using metrics and KPIs, and adjust strategy as necessary.

11 Leading societal change, e.g., smart cities, public policy

Smart cities utilize information technology, network communications (including the internet), and sensors to automate routine processes and enable fast, intelligent decision-making. These cities help address a wide range of urban challenges, from environmental sustainability to job creation and economic growth.

Public policy in the context of smart cities can include measures to address the negative effects of technological development, overcome socioeconomic inequality, and develop residents' technology skills. The concept of smart cities is attracting increasing interest from both academia and industry.

Some of the challenges facing the development of smart cities:

Cybersecurity and data protection. The more data a city collects, the higher the risk of cyberattacks and leaks. One successful attack can paralyze life support.

Lack of unified technological standards. This complicates the integration of various solutions into a single system and leads to platform compatibility issues across regions.

Lack of qualified specialists for technology development and implementation. Universities need to expand educational programs, focusing them on the practical application of urban infrastructure solutions, taking into account climatic and regional conditions.

The need to modernize outdated infrastructure. Large-scale digital transformation of the urban environment requires significant investment. Internet access issues in remote regions, such as the lack of a stable internet connection.

Citizen engagement in decision-making. The development and implementation of specialized apps and feedback platforms allow residents to report problems to local authorities, helping to foster a collaborative atmosphere.

In the conference take part inviting speakers from industry leaders around the world that will provide visions and industry in a rapidly developing technology world.

12 Conclusion

This year, representatives of 21 organizations from 10 countries participated in the conference. Among them: Technological Institute of the Philippines, Quezon City, Philippines; School of Engineering and Computing at the Instituto Tecnológico de Costa Rica, Cartago, Costa Rica; MIREA – Russian Technological University, Moscow, Russia; Institute of Radio and Information Systems (IRIS), Vienna, Austria; Moscow Technical University of Communications and Informatics, Moscow, Russia; Federal University SPbGUT, Saint Petersburg, Russia; AB Handshake, Miami, USA; Virginia Tech, Blacksburg, USA; Université Paris, Saint-Denis, France; RGM Global Ventures, Vienna, Austria; Kazan Federal University, Kazan, Russia; Siberian Federal University, Krasnoyarsk, Russia; The International Information Technology University, Almaty, Kazakhstan; National Research University Higher School of Economics (HSE University), Moscow, Russia; Eastern Institute of Technology, Gisborne, New Zealand; Eastern Institute of Technology, Napier, New Zealand; International Telecommunication Union (ITU), Geneva, Switzerland, etc.

The table presents EMCTECH-2025 conference final statistics.

Year	Applications	Accepted papers	Accepted papers, %	Conference participants	Conference authors	Organizations	Cities	Countires/ Continents
2020	95	57	60	201	139	38	17	12/5
2021	46	28	60	80	65	31	25	22/5
2022	95	46	48	140	122	44	29	11/3
2023	46	24	52	180	72	20	14	8/2
2024	50	26	52	160	60	20	17	10/4
2025	**52**	**29**	**54**	**170**	**70**	**21**	**15**	**10/5**

The next international conference EMCTECH will be held from October 14 to 16, 2026.

REFERENCES

[1] Denis Chivanov, “EMCTECH-2024: Research areas and work results,” *Synchroinfo Journal*. 2024, vol. 10, no. 6, pp. 25-31. DOI: 10.36724/2664-066X-2024-10-6-25-31

[2] D. Chivanov and S. Dymkova, "Technical facilities implementation methodology detecting borrowings in educational and scientific organizations : According to the results of 2022 International Conference on Engineering Management of Communication and Technology (EMCTECH)," *2022 International Conference on Engineering Management of Communication and Technology (EMCTECH)*, Vienna, Austria, 2022, pp. 1-4, doi: 10.1109/EMCTECH55220.2022.9934055.

[3] S. S. Dymkova, "Methods of Indicators Analysing for Universities Publication Activity by discipline "Radio engineering"," *2022 Systems of Signals Generating and Processing in the Field of on Board Communications*, 2022, pp. 1-8, doi: 10.1109/IEEECONF53456.2022.9744312.

[4] S. S. Dymkova and O. V. Varlamov, "Scientometric analysis of authors collaborations at the international conference “Engineering Management of Communications and Technologies“," *2023 International Conference on Engineering Management of Communication and Technology (EMCTECH)*, Vienna, Austria, 2023, pp. 1-4, doi: 10.1109/EMCTECH58502.2023.10296946.

[5] S. S. Dymkova and O. V. Varlamov, "Research Teams Collaborative Work Analysis within the IEEE Conference “Systems of Signals Generating and Processing in the Field of On-Board Communications”," *2025 Systems of Signals Generating and Processing in the Field of on Board Communications*, Moscow, Russian Federation, 2025, pp. 1-5, doi: 10.1109/IEEECONF64229.2025.10948068.

[6] S. S. Dymkova and O. V. Varlamov, "Scientific Collaborations within the IEEE Thematic Area “Systems of Signal Synchronization, Generating and Processing”," *2024 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO)*, Vyborg, Russian Federation, 2024, pp. 1-5, doi: 10.1109/SYNCHROINFO61835.2024.10617912.
[7] S. Dymkova, "Collaboration enhancing between industry staff and university researchers in international scientific communications system," *2022 International Conference on Engineering Management of Communication and Technology (EMCTECH)*, Vienna, Austria, 2022, pp. 1-7, doi: 10.1109/EMCTECH55220.2022.9934069.
[8] A. V. Dolgopyatova, S. S. Dymkova and O. V. Varlamov, "From Scientific Report to Industrial Development," *2023 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO*, Pskov, Russian Federation, 2023, pp. 1-4, doi: 10.1109/SYNCHROINFO57872.2023.10178494.
[9] S. S. Dymkova, "Identifying and Implementing Successful Scientific Projects, in the Framework of “IEEE Technology and Engineering Management Society” Events," *2020 International Conference on Engineering Management of Communication and Technology (EMCTECH)*, Vienna, Austria, 2020, pp. 1-7, doi: 10.1109/EMCTECH49634.2020.9261533.
[10] S. S. Dymkova, "Information Technologies in the Implementation of Scientific Organizations Publication Programs," *2023 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO*, Pskov, Russian Federation, 2023, pp. 1-6, doi: 10.1109/SYNCHROINFO57872.2023.10178601.
[11] S. S. Dymkova, "The increase “visibility” of scientific research results in the framework of international conference SYNHROINFO," *2018 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO)*, Minsk, 2018, pp. 1-5. DOI: 10.1109/SYNCHROINFO.2018.8456996
[12] S. S. Dymkova and O. V. Varlamov, "Peer Review Procedure as the Main Criterion for Confirmation Researcher's Scientific Work Quality : According results of the international conference SYNCHROINFO," *2022 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO)*, 2022, pp. 1-5, doi: 10.1109/SYNCHROINFO55067.2022.9840923.