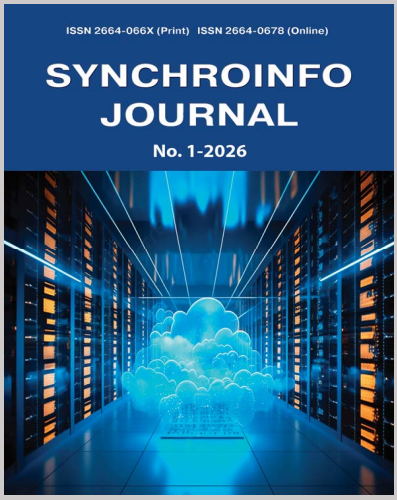
CONTENT
Vol. 12. No. 1-2026



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

STUDY OF HF BROADBAND DIGITAL RADIO LINE SIGNALS COHERENT RECEPTION DEVICE NOISE IMMUNITY

Vladimir Varlamov[1]

[1] Moscow Technical University of Communications and Informatics, Moscow, Russia;
f.vvo@bk.ru

ABSTRACT

This article presents the results of testing a software model of a wideband digital voice radio signal receiving device using an ionospheric channel model. This model was used to develop scientifically based recommendations for the application of a coherent algorithm in a digital voice radio signal receiving device and to compare its noise immunity with the prototype software model. During modem testing, scientifically based recommendations were developed for the application of an optimal filtering algorithm in real-world conditions. These recommendations consist of restarting the optimal filter upon receiving a new radiogram and setting the Doppler spreading value used in the optimal filter synthesis to 2 Hz under conditions of a priori uncertainty regarding the Doppler spreading value in the channel. The results of the study showed that the device, which differs from the known ones by the use of a coherent processing algorithm with optimal filtering of the coefficients of a multipath ionospheric channel and operating taking into account the recommendations presented in this work for the conditions of a priori uncertainty about the dynamics of changes in the state of the channel, makes it possible to increase the noise immunity of a wideband radio line for transmitting voice messages, which is quantitatively expressed in a decrease in the proportion of unreceived radiograms by 31 percent compared to the prototype when processing broadcast recordings.

DOI: 10.36724/2664-066X-2026-12-1-2-14

Received: 20.11.2025
Accepted: 27.01.2026

Citation: Vladimir Varlamov, "Study of hf broadband digital radio line signals coherent reception device noise immunity," *Synchroinfo Journal* **2026**, vol. 12, no. 1, pp. 2-14.

KEYWORDS: *HF communication, voice transmission, Kalman filter, ionospheric channel*.

Introduction

Decameter-wave radio communication is one method for constructing operational communications systems, along with backup communications and high-power broadcasting systems. For operational communications systems, the ability to reuse frequency resources (due to the congestion of the decameter range in general, and the presence of a significant number of users in relative proximity in particular) and ensuring the confidentiality of information transmission (which can be ensured, in addition to cryptographic protection methods, by operating with complex signals in a wide frequency band) are important.

The use of an alphabet of orthogonal wideband phase-shift keyed signals, in conjunction with modern non-binary error-correcting coding algorithms and speech compression algorithms, enables the implementation of wideband voice radio links with increased noise immunity to meet these requirements. The main challenges in constructing decameter-wave radio links are predicting the state of the ionospheric channel, as well as assessing and compensating for the distortions it introduces into the useful signal under conditions of multipath propagation. The use of wideband signals allows for the detection, separation, and summation of multipath signal components, implementing the principles of optimal coherent diversity reception to improve the link's noise immunity [1,2]. However, coherent diversity reception requires assessing and tracking changes (filtering) in the values of the complex channel coefficients for each multipath component during radiogram reception under the a priori uncertainty that arises when using an alphabet of orthogonal wideband phase-shift keyed signals.

This paper examines the testing of a software model of a device using an ionospheric channel model to develop scientifically based recommendations for the application of a coherent reception algorithm using channel transmission coefficient estimates refined by an optimal filtering algorithm in a digital voice radio signal receiving device and a comparison of noise immunity with the prototype software model.

Description of the hf range digital voice radio link signal receiving device operation

Figures 1 and 2 show the block diagrams of devices for receiving digital voice radio line signals with incoherent signal processing for each of the received beams (prototype) and coherent processing with optimal filtering of channel coefficients using the algorithm described in [3] (proposed device). When receiving a radiogram before demodulating symbols with useful information, it is necessary to solve the problems of detection and estimation of signal parameters. In [4, 5], an algorithm for detecting a wideband signal with simultaneous estimation of many of its parameters was developed, including the delay and frequency shift of the signal, as well as the slope of the dispersion characteristic (DC) of the ionospheric channel, which characterizes the degree of dispersion distortion of the signal. The prototype modem implements a reception algorithm that includes the above-mentioned principle of signal detection with independent estimation of the signal parameters for each multipath component during multipath signal propagation. Frequency shift compensation is implemented by multiplying the received signal samples by a complex harmonic signal with a frequency equal to $-\overline{\hat{f}}_d$. Compensation for the ionospheric channel dispersion distortions is implemented in accordance with [6] and is applied to the signal samples after the frequency shift has been eliminated. The dispersion distortion compensator uses the DH slope value estimated during detection. Next, the decision statistics are calculated as correlation sums of the received samples and the samples of the ensemble sequences, taking into account the initial delay of the radiogram for each of the beams. For the matrix of decision statistics, the posterior probabilities of receiving each of the code block symbols are calculated as [7]:

$$P\left(c_k / \mathbf{y}_1, \mathbf{y}_2, ..., \mathbf{y}_{N_p}\right) = \frac{1}{\sum_{l=1}^{2^m} \left(\frac{|\dot{y}_l|^2}{|\dot{y}_k|^2} \right)^{\frac{1-N_p}{2}} I_{N_p-1}\left(\sqrt{\frac{|\dot{y}_l|^2}{\sigma_{ш}^2} \frac{E_s^2 \sum_{j=1}^{N_p} |\dot{h}_j|^2}{\sigma_{ш}^2}} \right) \left[I_{N_p-1}\left(\sqrt{\frac{|\dot{y}_k|^2}{\sigma_{ш}^2} \frac{E_s^2 \sum_{j=1}^{N_p} |\dot{h}_j|^2}{\sigma_{ш}^2}} \right) \right]^{-1}}, \quad (1)$$

where c_k is the expected received symbol, $k = 1, ..., M$, M is the number of orthogonal signals in the alphabet used, $|\dot{y}_k|^2 = \sum_{j=1}^{N_p} |\dot{y}_{k,j}|^2$ and $|\dot{y}_l|^2 = \sum_{j=1}^{N_p} |\dot{y}_{l,j}|^2$ are the correlator responses for the j-th diversity branch, is the number of diversity branches (N_p is the number of multipath components), $I_{N_p-1}(x)$ is the modified Bessel function of the first kind, order $N_p - 1$, $|\dot{y}_l|^2$ and $|\dot{y}_k|^2$ are the results of square summation of the correlator responses over all diversity branches.

Thus, expression (1) implements the quadratic beam summation scheme in the channel. The calculated posterior probabilities are fed to the LDPC decoder, which extracts the payload bits.

The coherent reception scheme shown in Figure 2 differs from the incoherent one in terms of calculating the posterior probabilities and estimating the coefficients. Estimates of the channel coefficients are required for coherent beam summation and calculating the posterior probabilities from the real part of the combined decision statistics. For this purpose, the Kalman filter is fed with complex values $\dot{y}_{k,j}$ of the correlation sums and the values of the correlation sums $\mathbf{y}_{pr}$ for the preamble sequences, calculated at the signal detection stage. Based on these values, in accordance with the algorithm described in [3], refined estimates of the channel coefficients $\hat{h}_{k,j}$ are calculated. The calculation of the posterior probabilities, taking into account $\hat{h}_{k,j}$, is implemented as follows [8]:

$$P\left(c_k / \mathbf{y}_1, \mathbf{y}_2, ..., \mathbf{y}_{N_p}\right) = \frac{1}{\sum_{l=1}^{2^m} e^{\sum_{j=1}^{N_p} \frac{E_s \operatorname{Re}\left(\left(\dot{y}_{l,j} - \dot{y}_{k,j} \right) \hat{h}_{k,j}^* \right)}{\sigma_{ш}^2}}}. \quad (2)$$

After that, similar to the algorithm with non-coherent reception, the payload bits are calculated as a result of decoding the LDPC code.

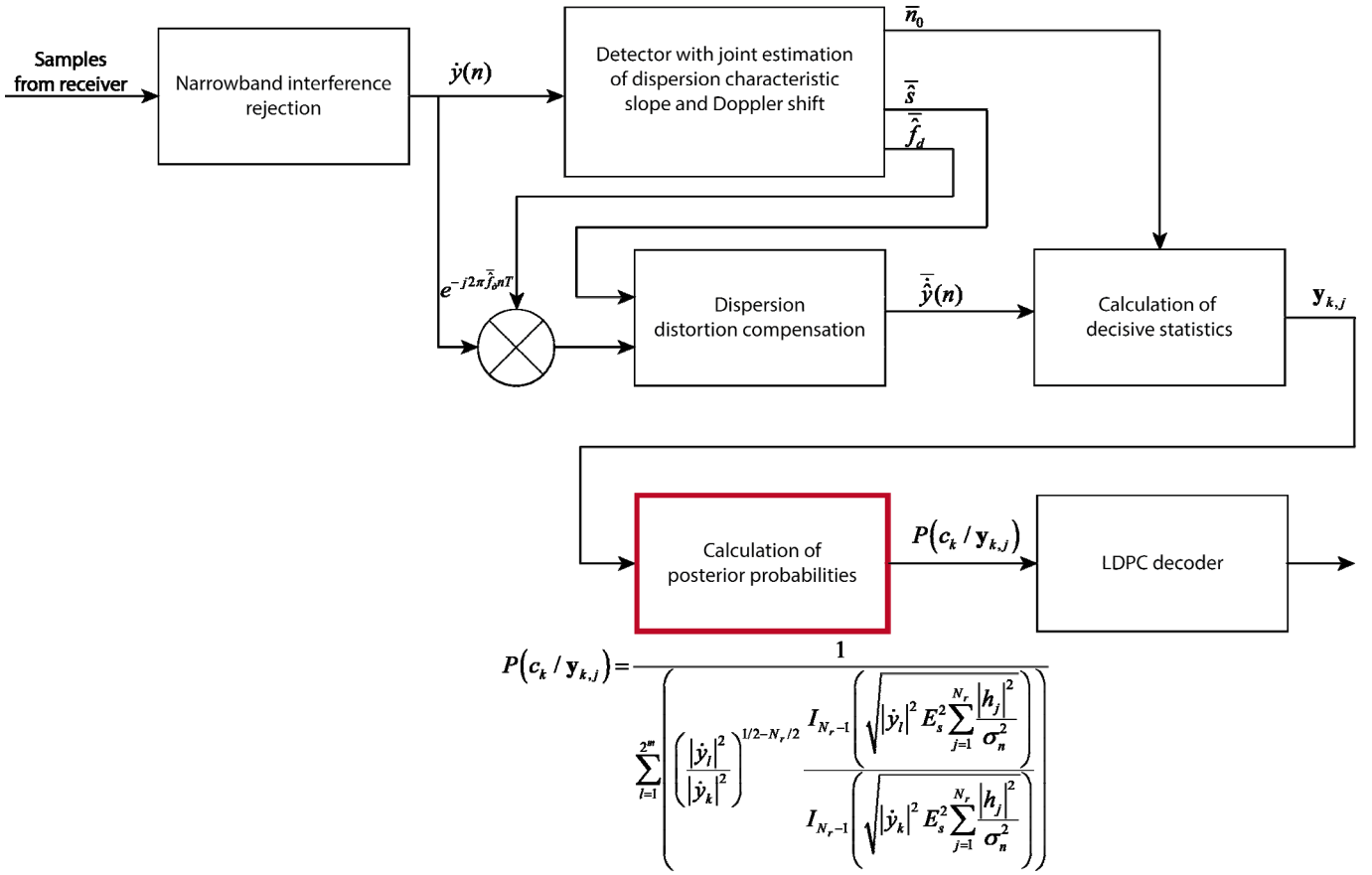


Figure 1. Block diagram of a device for non-coherent reception of a digital voice radio link signal in the HF range.

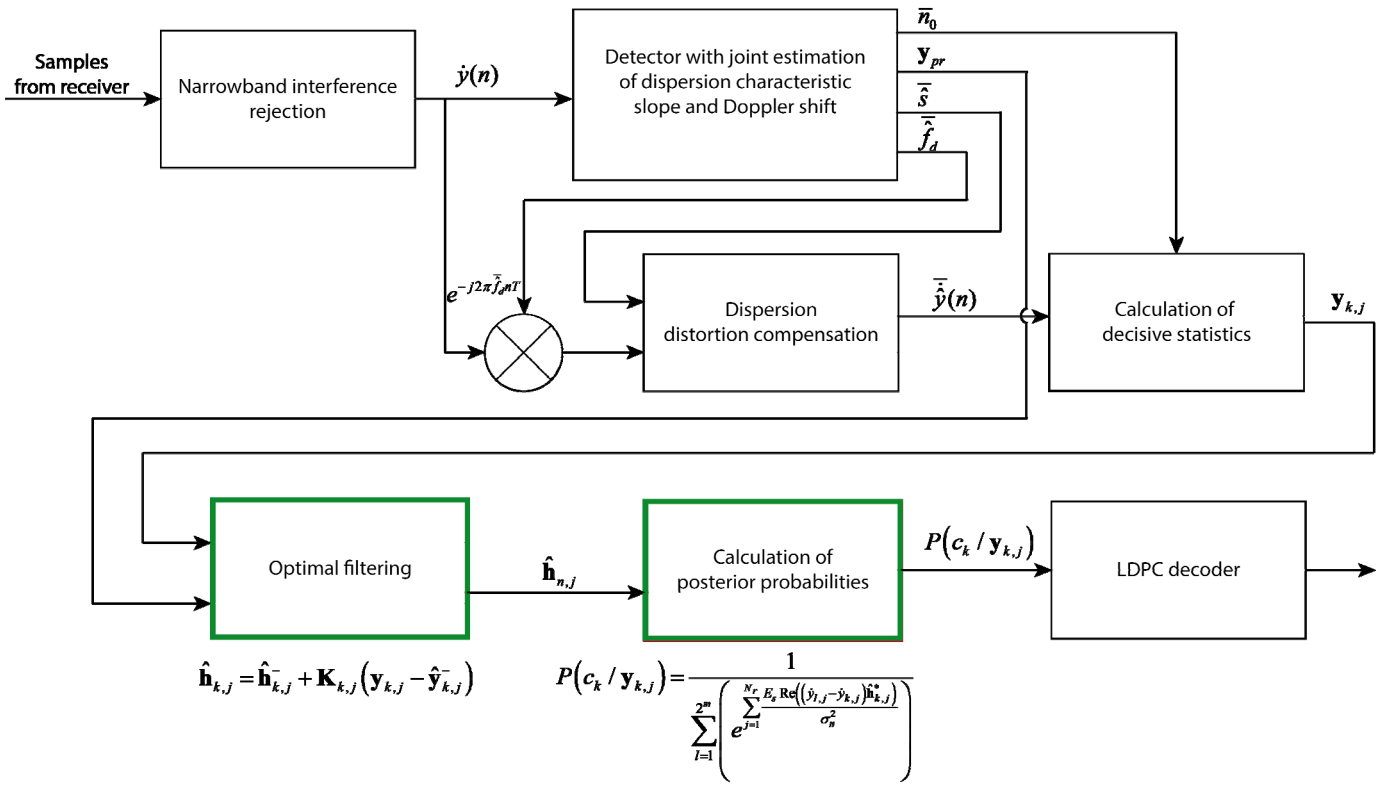


Figure 2. Block diagram of a device for coherent reception of signals from a digital voice radio link in the HF range.

Assessment of the gain from using an optimal filtering algorithm as part of a digital voice radio link signal receiver

In the receiving device, each radiogram is detected and received independently. Therefore, it is impossible to guarantee the continuity of symbols received from adjacent radiograms, and it is impossible to correctly take into account the information contained in the Kalman filter memory when processing a new radiogram. Consequently, it is necessary to restart the optimal filter when receiving a new radiogram.

To evaluate the noise immunity gain achieved by using the developed algorithm for optimal filtering of the channel gain under ionospheric propagation conditions in the HF range, taking into account the limitations imposed by the implementation of the receiving algorithm, a numerical experiment was conducted using the developed software model of a device for demodulating signals from a wideband digital voice radio line, as well as a software model of the prototype modem. The receiving device for which the model was developed differs from that implemented in the prototype modem by the addition of a module for optimal filtering of channel coefficient estimates and refined estimates when calculating the posterior probabilities of receiving code block symbols using a coherent scheme in accordance with expression (2). Figure 3 shows the diagram of the simulation experiment carried out to compare the reception algorithms, where device 02-01 is a modulator that generates complex readings of the quadratures of radiograms, device 01-02 is an AWGN generator with a given dispersion, device 02-02 is a Watterson channel simulator corresponding to the model described in section 1.1.2, device 04-02 is an adder, devices 03-04 and 03-05 are a module for calculating the signal power to noise power ratio and a display module, devices 04-04 and 04-05 are a counter for the number of transmitted radiograms and a display module, devices 01-07 and 01-08 are a demodulator with quadratic addition of beams, the structural diagram of which is shown in Figure 1 and a statistics display module, devices 03-07 and 03-08 are a demodulator with an estimate and optimal filtering of the channel transmission coefficients and coherent addition rays, the structural diagram of which is shown in Figure 2 and the statistics display module.

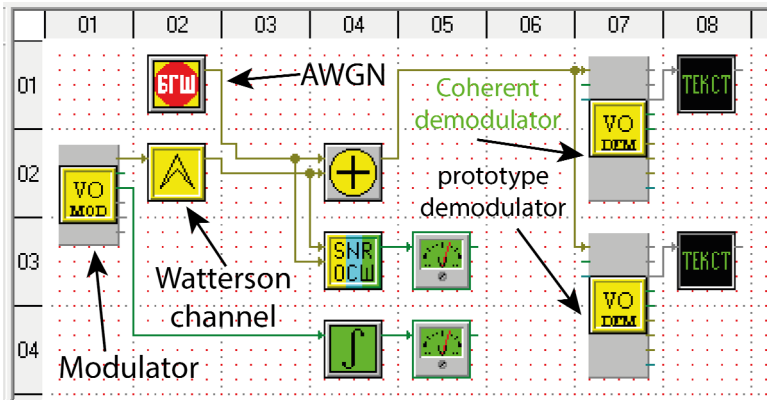


Figure 3. Experimental setup in “Spectr 2” environment.

The detection algorithm implements a combined estimate of the delay, Doppler frequency shift, and dispersion slope. As shown in [9], the coherence interval of these parameter estimates is 3-5 seconds, which is significantly longer than the duration of the radiogram used. Thus, up to the quality of the estimate, the influence of these parameters can be assumed to be compensated and will not be considered further.

Figures 4–6 show the dependences of the code block decoding probabilities for the algorithm with incoherent quadratic addition and with coherent addition and optimal filtering of the channel transmission coefficient. These dependences demonstrate a gain in noise immunity from 1.4 dB to 2.4 dB with a decoding probability of 0.95.

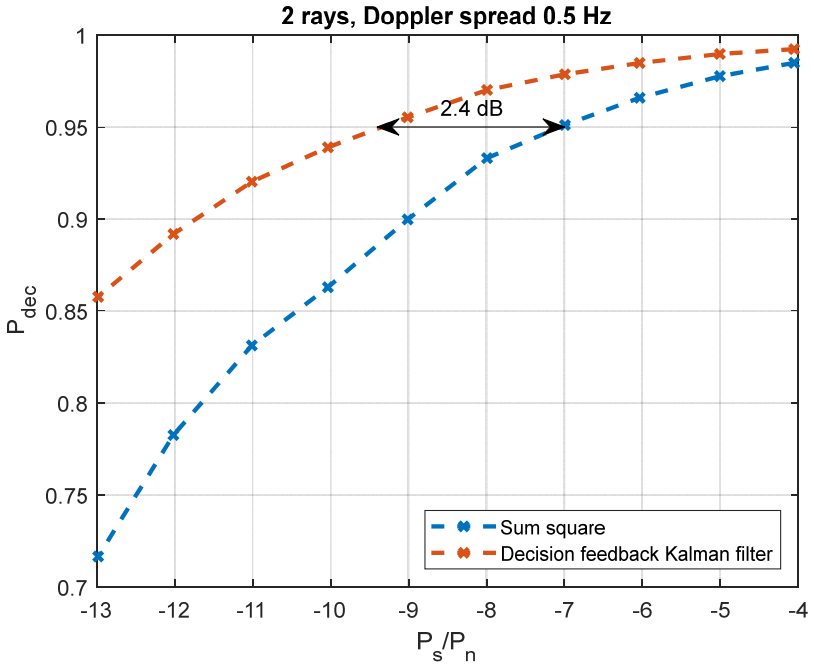


Figure 4. Dependence of the code block decoding probability on the SNR with Doppler spread 0.5 Hz.

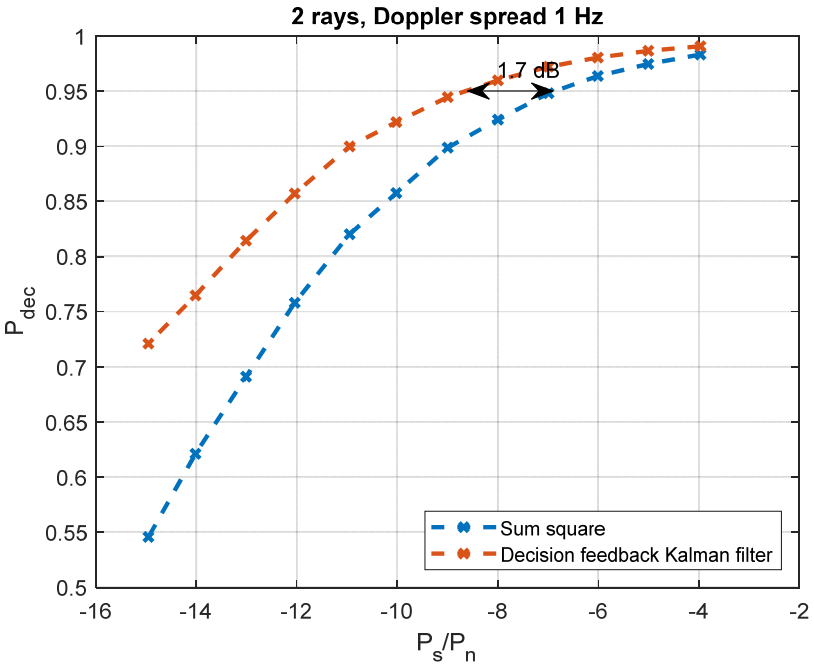


Figure 5. Dependence of the code block decoding probability on the SNR with Doppler spread 1 Hz.

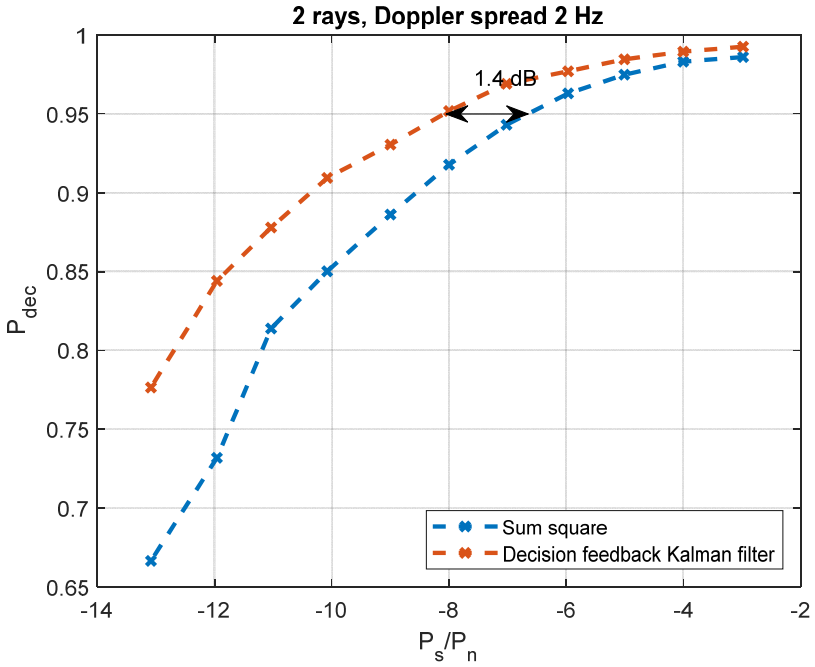


Figure 6. Dependence of the code block decoding probability on the SNR with Doppler spread 2 Hz.

Figures 7–9 show the dependences of the joint probability of detection and decoding of a radiogram for modems with non-coherent quadratic addition and with coherent addition and optimal filtering of the channel transmission coefficient. These dependences show a gain in noise immunity from 0.6 dB to 0.7 dB with a decoding probability of 0.95, depending on the magnitude of the Doppler spread in the channel.

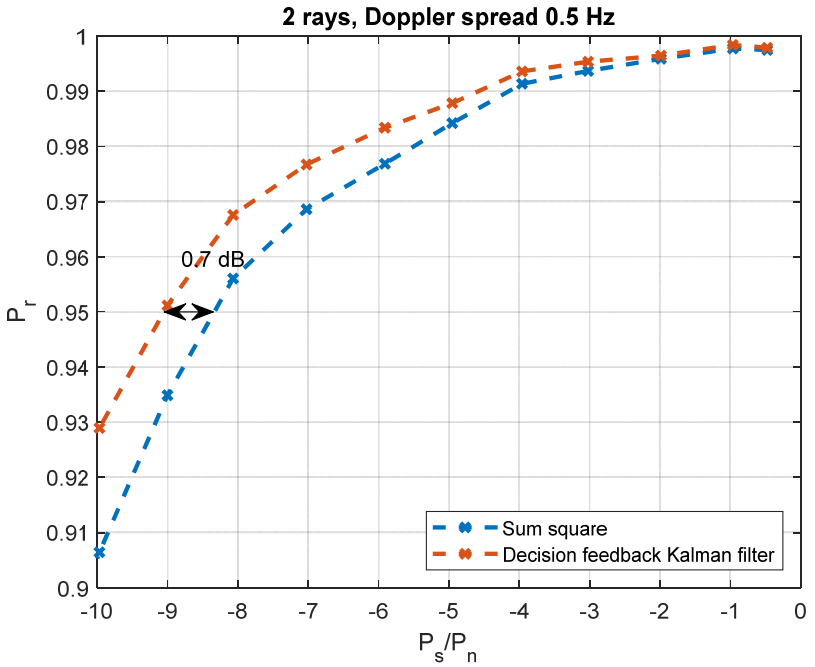


Figure 7. Dependence of the radiogram receiving probability on the SNR with Doppler spread 0.5 Hz.

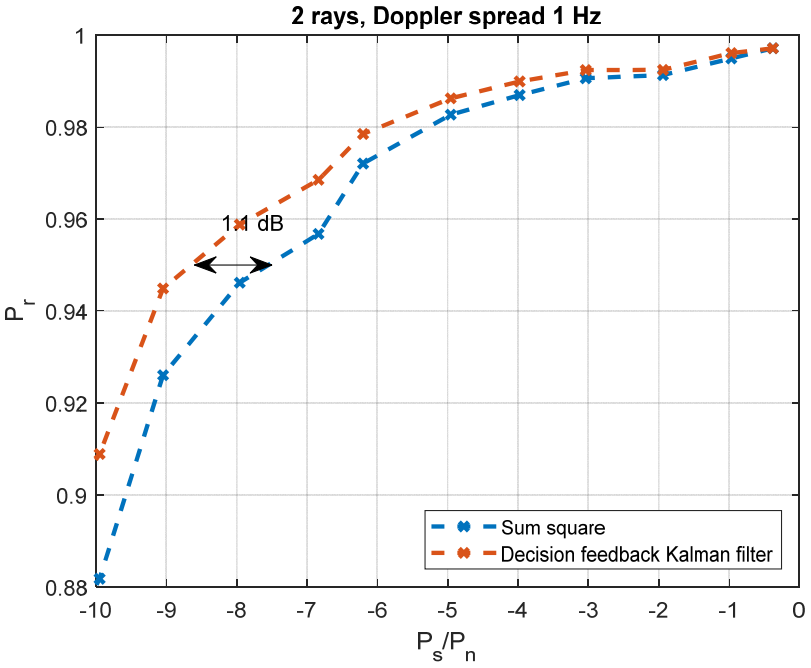


Figure 8. Dependence of the radiogram receiving probability on the SNR with Doppler spread 1 Hz.

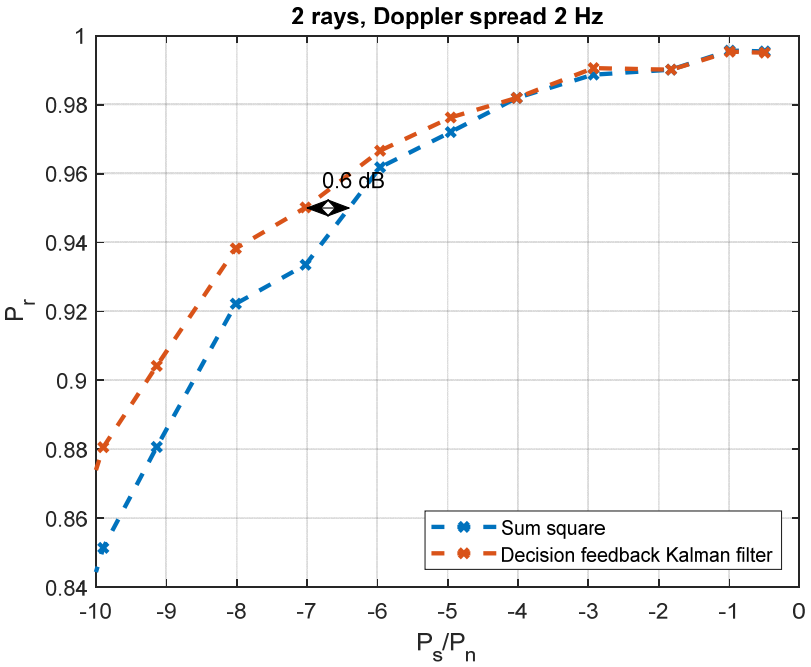


Figure 9. Dependence of the radiogram receiving probability on the SNR with Doppler spread 2 Hz.

Assessment of the dependence of noise immunity on the accuracy of doppler spread determination

Since the demodulation algorithm under consideration does not involve Doppler spread estimation, it is proposed to estimate the dependence of noise immunity on the difference between the specified and actual Doppler broadening values. The scheme of this experiment is shown in Figure 10. In this scheme, devices 02-01, 01-02, 02-02, 02-04, 03-04, 04-04 are similar to the devices from the scheme in Figure 3.

Devices 01-07, 03-07, 05-07 are demodulators with a coherent beam combining algorithm and optimal filtering based on a Kalman filter tuned to fading with a Doppler spread of 0.5, 1.0 and 2.0 Hz, respectively.

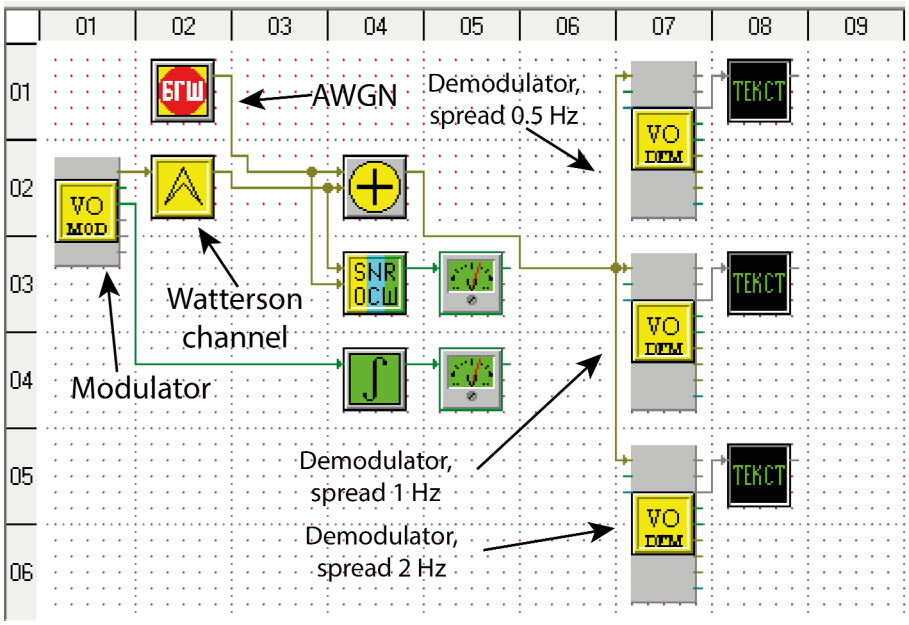


Figure 10. Experimental design for determining the effect of error in Doppler spread estimate on noise immunity.

Figures 11–13 show the dependences of the code block decoding probability on the SNR for Doppler spreading in the 0.5, 1, and 2 Hz channels. According to these dependences, for a Doppler spread of about 2 Hz, the Kalman filter tuned for a Doppler spread of 0.5 Hz is inferior to the filter for 2 Hz by about 2 dB. However, for smaller Doppler spreads, the difference between the algorithms is close to zero, which suggests the possibility of using the optimal filter for Doppler spreads smaller than that for which it was synthesized without a noticeable deterioration in noise immunity.

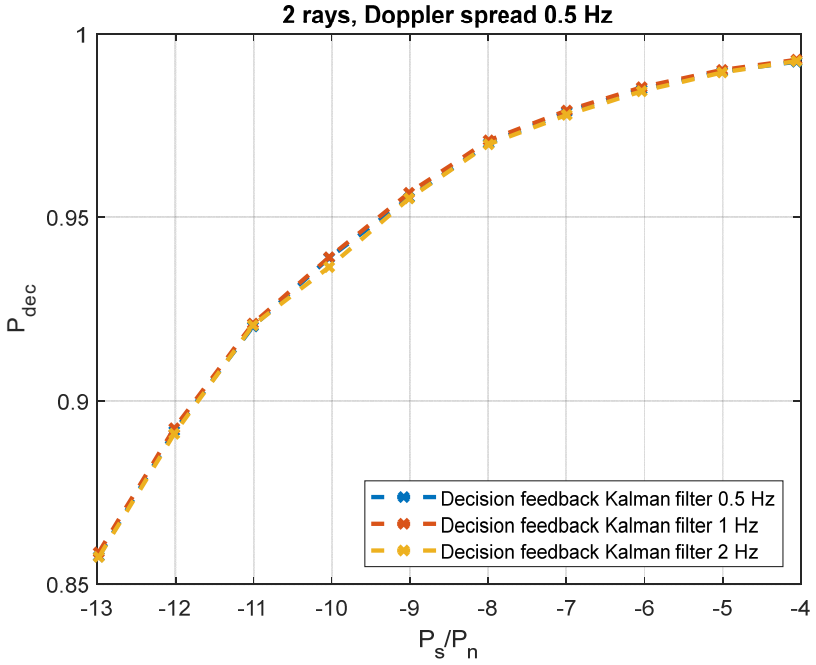


Figure 11. Dependence of the code block decoding probability on the SNR with Doppler spread 0.5 Hz

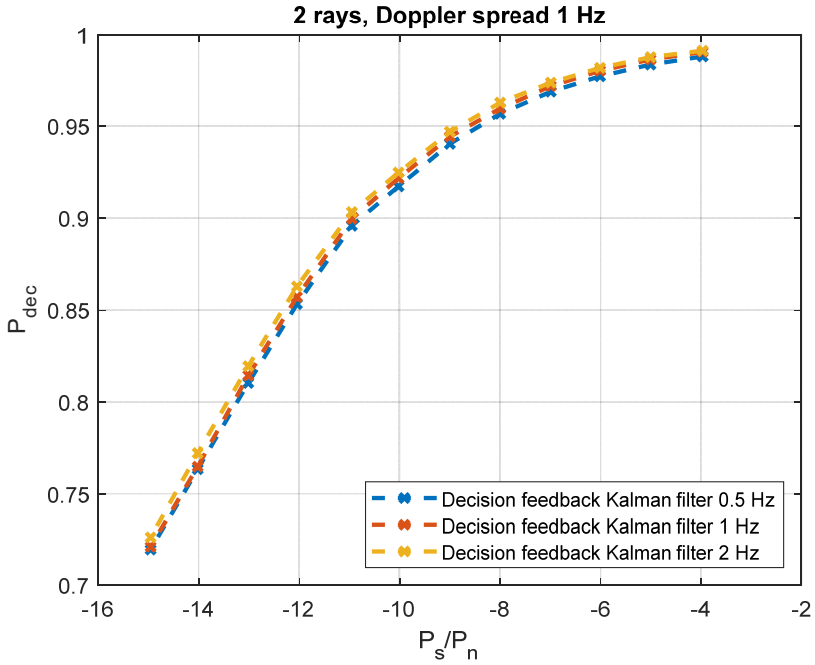


Figure 12. Dependence of the code block decoding probability on the SNR with Doppler spread 1 Hz

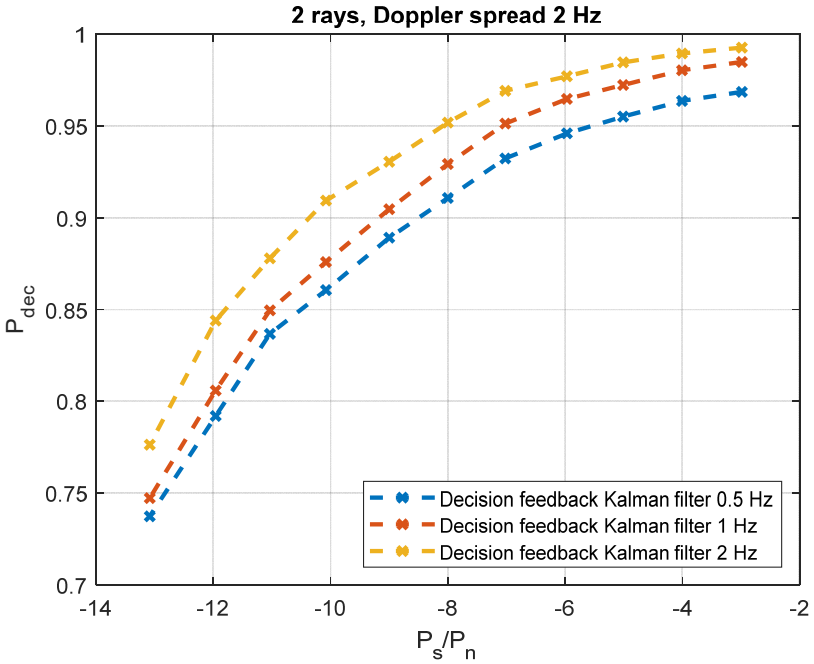


Figure 13. Dependence of the code block decoding probability on the SNR with Doppler spread 2 Hz

Results of processing air recordings

In order to experimentally confirm the effect of using coherent processing of decision statistics from received signal beams, signal recordings received during full-scale prototype tests were reprocessed as described in [7]. To solve this problem, a device for receiving digital voice radio line signals was developed that implements the developed algorithm. It includes software that allows processing signal recordings in the format used during testing so that the radiogram reception algorithm corresponds to that shown in Figure 2 and described above. Figure 14 shows the graphical interface of the recording processing software module. In the payload of each radiogram, in addition to the vocoder data blocks, one byte is allocated for service information about the radiogram number. This number increases monotonically from 0 to 255, after which it resets to 0. This allows, under the assumption that no more than 255 unreceived radiograms were transmitted between the two closest correctly demodulated radiograms, to determine the estimate of the proportion of correctly received radiograms as:

$$\hat{P}_r = \frac{N_{dec}}{\sum_{n=1}^{N_{dec}-1} \left(i_n - i_{n-1}\right)}. \tag{3}$$

where N_{dec} is the number of correctly decoded blocks during a communication session, i_n is the number of the radiogram transmitted as part of the useful message for the n-th decoded parcel.

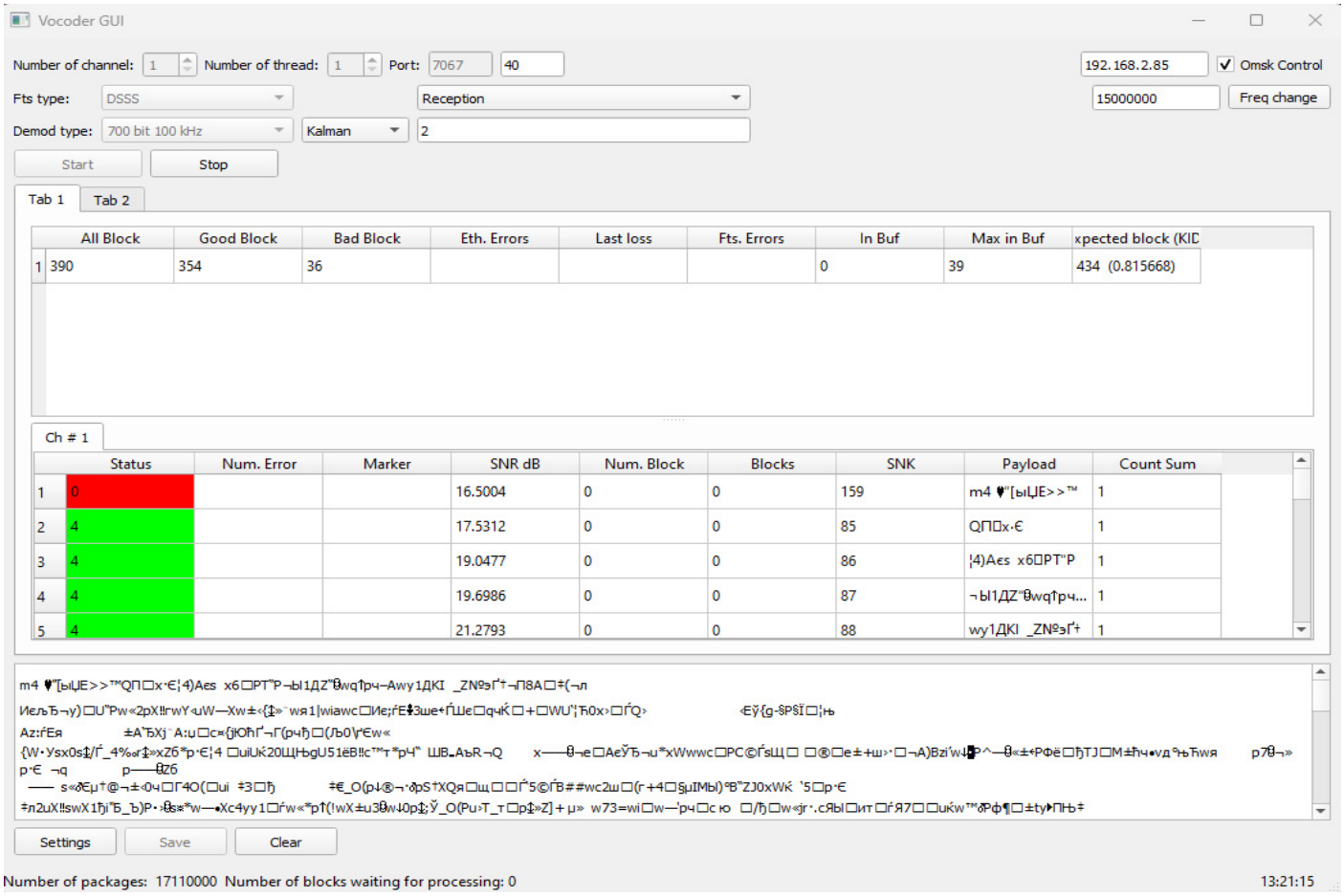


Figure 14. Record processing module interface.

Figure 15 compares the estimated reception probabilities for processing using an algorithm with non-coherent quadratic beam combining and one with coherent beam combining with optimal filtering. For the processed records, the developed algorithm demonstrated noise immunity either similar to or better than the non-coherent algorithm, with up to a twofold increase in the number of correctly received radiograms. On average, across all processed records, the decoding error probability decreased by 1.92 times (48%), resulting in a 1.45-fold (31%) decrease in the reception error probability.

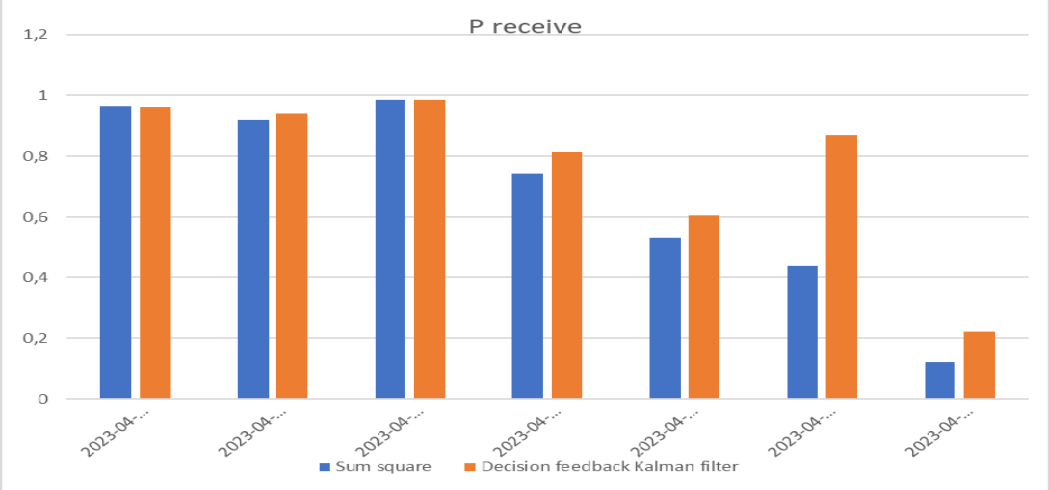


Figure 15. Comparison of reception probabilities for non-coherent reception and coherent reception with optimal filtering.

Conclusion

This paper presents a software model of a digital voice radio line signal reception device implementing the reception algorithm synthesized in Section 3. The developed model implements the Kalman filter operation using MP estimates of the channel coefficients obtained from preamble symbols, as well as information symbols selected in accordance with hard decisions during preliminary processing with quadratic addition. To eliminate uncertainty regarding the channel noise variance, this variance was estimated using decision statistics for non-information positions. A numerical experiment was conducted to test and compare the noise immunity of the radio link using the developed reception algorithm and the prototype radio link. The experiment results showed an energy gain in decoding probability from 1.4 to 2.4 dB with a Doppler spread of 0.5 to 2 Hz, respectively, for the developed model using an optimal filter calculated for the true value of the Doppler spread. It was also shown that, under conditions of a priori uncertainty regarding the fading rate in the ionospheric channel (Doppler spread values in the range of up to 2 Hz), the parameters of the optimal channel multiplier filtering algorithm calculated for a Doppler spread of 2.0 Hz should be used. This will allow processing wideband signals in the Doppler spread range from 0.5 Hz to 2 Hz with losses not exceeding 0.1 dB relative to precisely tuned optimal filtering algorithms.

The results of processing recordings from full-scale tests of the prototype radio link using the developed reception algorithm are presented. It was shown that the use of this algorithm reduced the probability of decoding errors in the code block by 1.92 times (48%), and the probability of radiogram reception errors by 1.45 times (31%).

REFERENCES

1. V. O. Varlamov, “Methodology for determining the error correction code rate of the HF range digital voice radio link,” *T-Comm*, 2025, vol. 19, no.2, pp. 23-30.
2. E.M. Lobov, N.A. Kandaurov, E.O. Lobova, V.I. Lipatkin, D.N. Shubin and V.O. Varlamov, "Modern methods of processing broadband signals of radio communication lines under conditions of dispersion distortions in the Earth's ionosphere," *Thesis of the XXVIII All-Russian Open Scientific Conference*, Yoshkar-Ola, May 16-19, 2023, pp. 43-50.
3. V.O. Varlamov, E.M.Lobov, “The algorithm for coherent processing of wideband non-binary signal-code structures for speech transmission in a decameter radio channel,” *T-Comm*, 2025, vol. 19, no. 12, pp. 59-76.
4. V.I. Lipatkin, E.M. Lobov, E.O. Lobova, “The quality of estimation of parameters of a broadband signal with non-optimal reception under conditions of dispersion distortions in the Earth's ionosphere,” *T-Comm*, vol. 16, no.8, pp. 46-53.
5. S.S. Adjemov, E.M. Lobov, N.A. Kandaurov, E.O. Lobova, V.I. Lipatkin, “Algorithms of estimating and compensating the dispersion distortions of wideband signals in the HF channel,” *H&ES Reserch*. 2021. Vol. 13. No. No 5. P. 57-74.
6. D.S. Chirov, E.O. Lobova, “Wideband HF signals dispersion distortion compensator based on digital filter banks. Theory and approbation,” *T-Comm*, 2020, vol. 14, no.4, pp. 57-65.
7. E. M. Lobov, I. S. Kosilov, N. A. Kandaurov, B. A. Elsukov, “The performance estimation method of the signal-code structures based on wideband orthogonal signals family and non-binary LDPC-code in the ionosphere CHANNEL,” *T-Comm*, 2014, vol. 8, no.8, pp. 55-59.
8. L.M. Fink, “Discrete message transmission theory,” 2nd edition, revised and supplemented. Moscow: Sov. Radio, 1970, 728 p.
9. D. V. Ivanov, V. A. Ivanov, V. V. Ovchinnikov, N. V. Ryabova, "Energy Characteristics of Dispersive Wideband Channel and Data Rates in a Cognitive WSN," *T-Comm*, 2025, vol. 19, no.10, pp. 13-20.

SYNCHROINFO JOURNAL

www.media-publisher.eu/synchroinfo-journal

DESIGN AND MODELING OF UFMC SYSTEMS

Anastasia V. Ermakova[1], Vu Sy Dao[2]

[1] Moscow Technical University of Communications and Informatics, Moscow, Russia;
msikisylia@gmail.com

[2] Le Quy Don Technical University, Hanoi, Vietnam

ABSTRACT

This paper presents a step-by-step design and implementation of the transmitter section of a universal filtered multicarrier modulation (UFMC) system targeted for use in next-generation wireless communication systems. The development process includes four sequential stages: mathematical modeling and simulation of the UFMC system in MATLAB, system-level modeling in Simulink, hardware-oriented design using the Xilinx System Generator, and design verification using hardware co-simulation. The paper describes in detail the main functional blocks of the UFMC transmitter, including random data generation, QPSK modulation, serial-to-parallel conversions, zero padding, inverse discrete Fourier transform, digital upconversion, and subband filtering. Special attention is paid to the implementation of the system on a Xilinx Spartan-6 FPGA, taking into account the limitations of hardware resources and fixed-point representation accuracy. An elliptic filter and a Chebyshev filter of the second kind are studied for subband formation. Simulation results obtained in MATLAB and Simulink show that the use of an elliptic filter provides better spectral localization and more effective sidelobe suppression compared to a Chebyshev filter. These results confirm the practical applicability of the proposed UFMC architecture and its potential for further hardware implementation in 5G wireless communication systems.

DOI: 10.36724/2664-066X-2026-12-1-15-30

Received: 20.11.2025
Accepted: 27.01.2026

Citation: A.V. Ermakova, V.S. Dao, "Design and modeling of UFMC systems," *Synchroinfo Journal* **2026**, vol. 12, no. 1, pp. 15-30.

KEYWORDS: *UFMC; multicarrier modulation; 5G communication systems; digital signal processing; FPGA; MATLAB; Simulink; Xilinx System Generator; QPSK modulation; subband filtering; elliptic filter; Chebyshev filter; fixed point; hardware cosimulation.*

Licensee IRIS, Vienna, Austria.

1 Introduction

Modern fifth-generation wireless communication systems place increased demands on spectral efficiency, resistance to intersymbol interference, and flexibility in radio resource allocation. Traditional orthogonal frequency division multiplexing (OFDM), widely used in LTE networks and early versions of 5G, offers several advantages, including ease of implementation and compatibility with multiple-input multiple-output (MIMO) technologies [10-13]. However, OFDM is characterized by high spectral sidelobes and sensitivity to synchronization errors, limiting its effectiveness when transmitting short packets and in dense wavelength-division multiplexing (WDM) environments.

As an alternative to OFDM, new signal forms such as filtered bank multicarrier (FBMC) and universal filtered multicarrier (UFMC) [1-5] have been actively explored in recent years. UFMC is considered a compromise between OFDM and FBMC, combining the simplicity of OFDM with the improved spectral characteristics of FBMC. In UFMC, filtering is performed at the subband level, which significantly reduces filter length, improves spectral localization, and reduces intersymbol interference without significantly increasing receiver complexity.

Despite the potential of UFMC, practical implementation of this technology requires careful consideration of the transmitter architecture and the limitations of hardware platforms such as field-programmable gate arrays (FPGAs) [14-17]. Particularly important are the selection of a filter prototype, optimization of the fixed-point representation, and balancing system performance with hardware resource utilization.

The objective of this work is to develop and implement, step-by-step, the transmit portion of a UFMC system using MATLAB and Simulink modeling tools, as well as the hardware-specific Xilinx System Generator tools [18-20]. This study examines in detail the UFMC modulation processes, from digital data generation to subband filtering, and also provides a comparative analysis of an elliptic filter and a Chebyshev filter of the second kind [6-9]. The obtained simulation results confirm the effectiveness of the proposed approach and substantiate the possibility of further implementation of the system on FPGA for use in next-generation wireless communication networks.

2 FPGA design process

To design and implement a UFMC system, four stages are followed according to the design flow. At each stage, the UFMC system is modeled and simulated to obtain simulation results that ensure high performance before moving on to the next stage. The first two stages of the design process are modeling and simulation in MATLAB and Simulink. The UFMC system design process consists of four stages. The first stage is to model and simulate UFMC systems with different filters in MATLAB. Based on the mathematical foundation of the UFMC system described in Chapter 3, two UFMC systems are modeled in MATLAB using LTE parameters, where the two systems are tested in a fading channel to demonstrate the differences between the UFMC systems.

In the second stage, the UFMC system is modeled using LTE downlink parameters and simulated in Simulink. Unlike in MATLAB, many parameters, such as the sampling period, must be defined in Simulink. Because the UFMC model has different filters, the OFDM-based design is divided into multi-rate subsystems. Simulink is essentially a MATLAB graphical extension for modeling and simulating a multi-rate system with different simulation time steps. Using the Simulink communications library, the UFMC system is modeled based on a MATLAB model. Each Simulink block represents a mathematical formulation already implemented in MATLAB. This Simulink UFMC model will serve as the basis for a Xilinx-based implementation by replacing Simulink blocks with Xilinx blocks. However, some Simulink blocks, such as the data source and receivers, are still required for hardware co-simulation.

Designing a UFMC system using Xilinx blocks is the third stage of the design process. In this step, Simulink blocks are replaced with Xilinx blocks. Some Xilinx subsystems are designed to have the same functionality as Simulink blocks. Using this representation leads to a tradeoff between system performance and the size of the Xilinx UFMC design, as the number of dedicated bits affects system performance. The greater the number of dedicated bits, the more complex the hardware design. The number of dedicated bits is chosen to ensure the hardware size is suitable for implementing a high-performance Xilinx Spartan-6 FPGA.

The final step of the design process is validating the Xilinx-based design using co-simulation. To perform tasks in the fields of digital communications and digital signal processing, MATLAB software was effectively used for modeling, testing, and evaluating system performance. The UFMC system design must be tested before it can be implemented to avoid any design errors. Therefore, our UFMC system is modeled in MATLAB and Simulink before the VHDL code is generated and loaded onto the Spartan-6 board for implementation. To better understand the signal modulation processes, this chapter describes and discusses each stage of the UFMC modulation process in detail. Since the receiver performs the inverse processes to the transmitter, only the transmitter blocks are described in detail.

As part of the System Editions ISE® Design Suite, the Xilinx System Generator for Digital Signal Processing is a Simulink plug-in design tool that enables designers to design, simulate, and develop high-performance digital signal processing systems. This design tool consists of a set of Xilinx blocks in the form of a Simulink library that can be mapped directly to target FPGA hardware. Using the Xilinx System Generator for Digital Signal Processing, you can not only design and simulate digital signal processing algorithms but also generate synthesizable hardware description language (HDL) code using the Xilinx FPGA coder. Therefore, the Xilinx System Generator for Digital Signal Processing is considered a high-level design tool for high-performance digital signal processing systems, providing system simulation and automatic code generation from MATLAB or Simulink. Using Xilinx block libraries in the Simulink model-based design environment does not require previous experience with register-level design and Xilinx FPGAs, as subsequent FPGA implementation steps, such as place, route, and synthesize, are automatically performed to generate the FPGA bitmap. The Xilinx System Generator also provides hardware co-simulation functionality when the model-based design is executed in Simulink and the FPGA. Chapter 4 describes how MATLAB and Simulink were initially used to simulate a QPSK-UFMC system, including a transmitter, channel, and receiver. In this chapter, the Simulink model is converted into hardware blocks using the Xilinx System Generator. The Xilinx design is then synthesized, mapped, and routed to generate the bitstream that will be loaded into the FPGA. When hardware co-simulation is performed, MATLAB actually communicates with the FPGA through internal RAM. An overview of each block used to design the transmitter, receiver, or wireless channel is provided, describing its functions and characteristics. Xilinx UFMC transmitter, wireless fading channel, and receiver blocks are shown respectively.

3 UFMC signal generation in Xilinx System Generator

The UFMC transmitter is designed as shown in Figure 1.

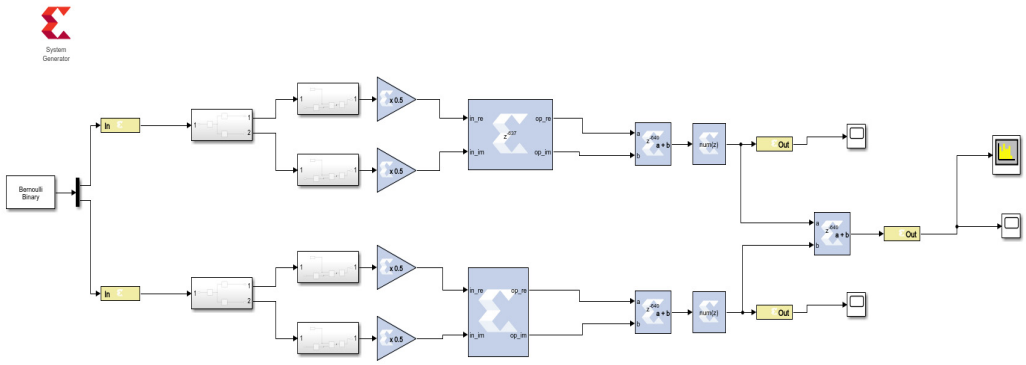


Figure 1. Block diagram of the Xilinx UFMC dual-band transmitter

Data is generated from the Simulink environment and transferred to the Xilinx design. The digital signal is modulated with a QPSK baseband modulator before being modulated with an FFT. Typically, the wireless channel model is applied to the signal after it has been upconverted.

To apply a multipath fading channel to a signal consisting of I and Q components, the components must be separated as I and Q signals for complex multiplication. For this reason, the multipath fading channel in our design is used before the I and Q signals are modulated. This makes the design more efficient and less complex.

4 Generating random data

In the first stage, a digital random data matrix of size m × n is generated with the condition that it should have only scalar values 0 or 1 with the same probability to be similar to the original digital signal in digital communication. To determine the matrix size, many factors must be taken into account, such as the number of UFMC symbols, the FFT size, the number of zero-padded symbols, and the modulation method. A large input matrix size may lead to a shortage of memory on the computer, depending on the computer RAM. In our design, the FFT is 512, the number of UFMC symbols is 105, and QPSK modulation is used. Assuming that 256 zeros are padded in one UFMC symbol, the number of bits per UFMC symbol is represented as (512 - 256) * k = 512, where k = 2 is the modulation index for QPSK.

For simplicity, the number of columns is assumed to be 1, so the number of rows is $6*10^7$. In fact, this definition of the random matrix size should ensure that the number of QPSK symbols, after zero padding, can be converted to a multiple of the FFT size without remainder. However, the number of UFMC symbols per matrix can be as small as one integer, but achieving this number of UFMC symbols requires generating multiple matrices.

In model-based design, random bits are generated using the Bernoulli binary generator provided by the Communications System Toolkit library. Input data is generated with a zero probability of 0.5 and a sampling rate of 20 Mbps. The Bernoulli Binary Generator output is sample-based. To convert Simulink integer, fixed-point, or double input data types to the System Generator fixed-point type, the Gateway-In block is used as an input to the Xilinx portion of the Simulink model. When converting from a floating-point to a fixed-point data type, the Gateway-In block uses some options for overflow and quantization. In the event of an overflow, it can be used to saturate or wrap the input value or mark it as an error. Saturation is essentially the process of converting an overflowed value to its largest positive or smallest negative value. Wrapping involves discarding the overflowed value, that is, the bits to the left of the most significant bit. Marking is only intended to indicate an error whenever an overflow occurs. The Gateway-In block also provides quantization options: either rounding the value to the nearest representable value or truncating it by discarding the bits to the right of the least significant bit.

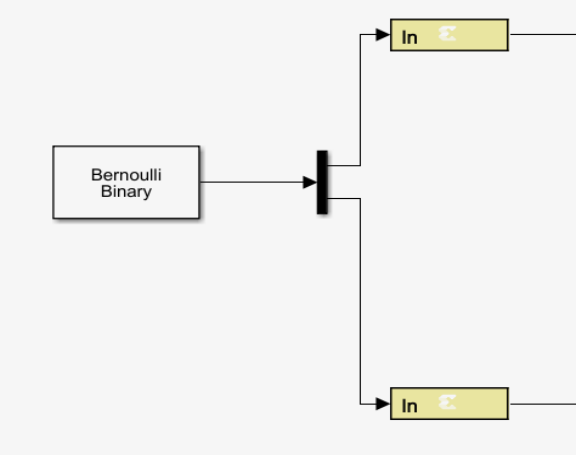


Figure 2. Random data generation blocks

5 QPSK Modulation

QPSK modulation was used for the subcarrier modulation. Every two consecutive bits of the original digital data are mapped to a corresponding QPSK symbol, which differs in phase angles of 0, 90, 180, or 270 degrees. Each group of two bits is encoded along the in-phase or quadrature axis.

Therefore, each QPSK symbol can be represented as a complex number S_I+jS_Q if a constellation is used for mapping. In our implementation, a constellation with zero phase shift is used. The original data matrix is modulated into a matrix of complex numbers in the form of QPSK symbols, and the size is equal to half the size of the original matrix.

As shown in the figure below, the modulator is implemented as a combination of two ROMs and a serial-to-parallel converter [10]. The serial-to-parallel block accepts serial unsigned data, represented as a fixed-point representation of a single bit with a binary digit of zero, and produces a single output from two consecutive input bits. In other words, it combines every two bits that will later be mapped in ROM to the corresponding QPSK symbol. Serial input is ordered with the most significant word first.

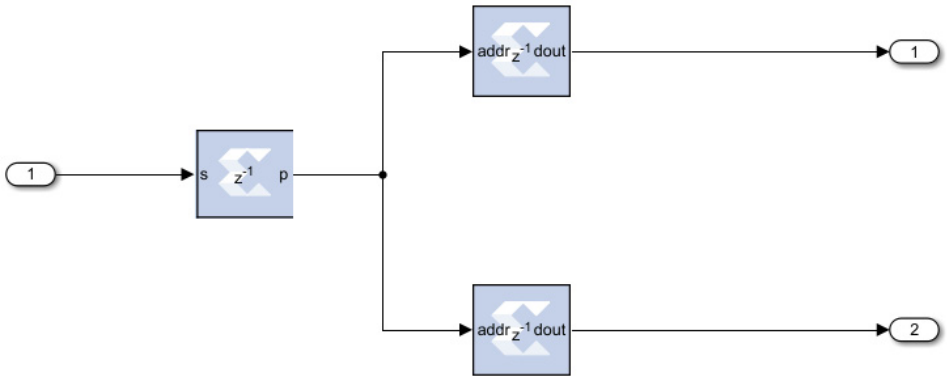


Figure 3. Xilinx Modulator

The Xilinx block ROM is a single-port read-only memory that stores four words corresponding to "00," "01," "10," and "11." The word values are specified in the block parameters as a seed vector. Since a QPSK symbol consists of quadrature and in-phase values, two ROMs are used for both the I and Q channels. Both have the same input and depth, but they differ in the seed vector corresponding to the gray-coded QPSK constellation. To reduce the size of the fixed-point representation, the QPSK symbol power is not normalized. Since the Xilinx design will be loaded into an FPGA, the design area is very important and should be as small as possible. This area is affected by the number of used bits in the fixed-point representation. Therefore, the in-phase and quadrature QPSK values are set to 1 or -1 to reduce the number of bits for their fixed-point representation.

6 Serial to parallel conversion

Serial data is converted to parallel data. The modulated matrix S, as the input matrix, is transformed into a 256-column matrix. In this case, each row of 256 QPSK symbols is considered parallel data. These 256 QPSK symbols are grouped for modulation to create a UFMC symbol. The actual purpose of the shape change is to form an S-matrix that is ready for UFMC modulation using an IFFT.

For better performance, the frequency spacing between subcarriers in the UFMC frequency domain can be reduced as the sampling rate increases. To increase the sampling rate, interpolation is used by appending zeros to the end of the original data sequence. As zeros are appended to the signal, the number of samples in the time domain increases, which also increases the FFT size. By expanding the FFT samples, the UFMC symbol will have a higher resolution, which is required for digital signal processing such as digital-to-analog and analog-to-digital conversion. The interpolation process must comply with the Nyquist sampling theorem to avoid aliasing, which can occur in the frequency domain. Therefore, the Nyquist frequency must be at least twice the highest frequency of the sampled signal [11]. Since the number of samples for the FFT is 256, the number of appended zeros must be at least 256 to comply with the Nyquist theorem. To ensure that non-zero data is mapped to subcarriers near the zero frequency, and zero data is mapped to subcarriers with high positive/negative frequencies, these zeros must be padded in the middle of each parallel IFFT data input.

Zero padding in the Xilinx design is not used for the same purposes as in MATLAB and Simulink. In fact, zero padding is used for upsampling and creating time space between groups of QPSK symbols to form UFMC symbols. These spaces are actually used to add a cyclic prefix. To insert a cyclic prefix into a UFMC symbol using the Xilinx IFFT block with a pipelined streaming I/O implementation, the time space must be equal to the length of the cyclic prefix to avoid data loss during transmission.

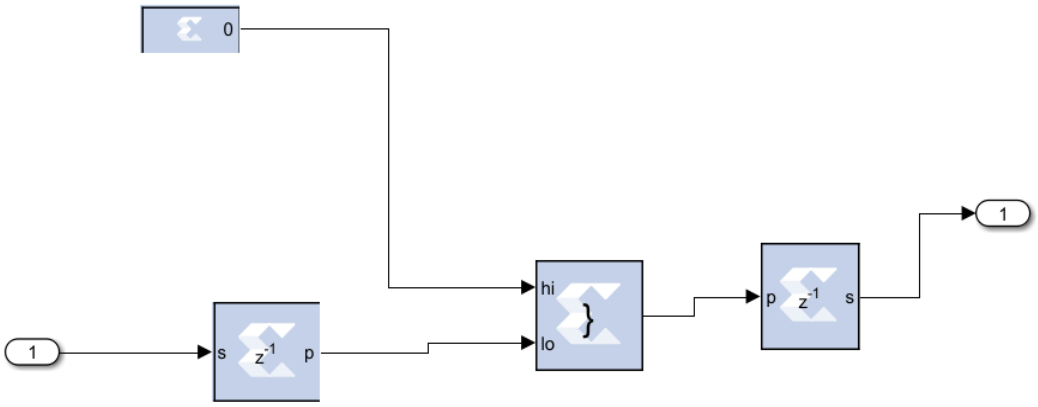


Figure 4. Xilinx Zero-Fill Design

As shown in Figure 4, the zero-padding design consists of Xilinx serial-to-parallel and parallel-to-serial converters, constant blocks, and constant blocks. The first serial-to-parallel block groups 1024 consecutive bits, which represent 512 QPSK symbols, with the most significant word coming first, to create a single unsigned output. A 256-bit unsigned fixed-point representation is used to represent the zero value as the constant block output. In fact, the number of unsigned fixed-point bits is related to the length of the cyclic prefix. Therefore, the time interval between OFDM symbols required to insert the cyclic prefix is equal to the length of 128 QPSK symbols. When the in-phase and quadrature-phase QPSK values are represented by two bits, 256 bits are required for each of the I and Q values to represent 128 QPSK symbols.

The unsigned outputs of the constant and serial-to-parallel blocks are combined to create a single unsigned integer bit vector. Data input to the upper port of the concat block occupies the most significant bits of the output, while data input to the lower port occupies the least significant bits [12]. Therefore, the output of the concat block is an unsigned integer represented by a 1280-bit vector. This process of combining two inputs with the same data rate creates a single output with a higher data rate. In the parallel-to-serial block, the input word is divided into 640 parts, so every two bits form one signed word with a binary position of zero and least significant bit order first. As a result of zero padding, the output data rate is higher than the input rate by a ratio of 5/4.

7 Inverse Discrete Fourier Transform

To generate multiple orthogonal subcarrier signals overlapping in spectrum, the discrete Fourier transform and inverse discrete Fourier transform processes should be used. In MATLAB, the FFT and IFFT were used to implement the DFT and IDFT processes. In fact, the FFT function in MATLAB uses a combination of several algorithms, including Cooley-Tukey [12] and prime factorization algorithms [13].

To use time-decimation, the number of IFFT points N must be an integer of power 2, and therefore the modulated matrix is transformed to have 256 columns and then filled with zeros to have 512 columns, which meets the requirement of time-decimation algorithms. As a result, the transpose of the IFFT output matrix is represented as a matrix X. Each row of matrix X represents a UFMC symbol, which is periodic with a period of 512 samples. The Xilinx FFT block supports the Virtex-5 and other FPGAs, such as the Virtex-7, Virtex-6, Virtex-5, Virtex-4, Spartana-6, and so on. It calculates the forward and inverse DFT of an N-point vector of complex values.

The FFT size can be fixed-point or floating-point numbers. Since the FPGA area is limited, the real and imaginary components are represented in fixed-point with the minimum possible number of bits without affecting system performance. In other words, the number of bits required to represent values is inversely proportional to the FPGA area, since calculating the DFT requires a lot of mathematical calculations.

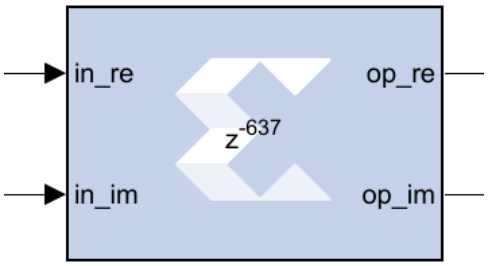


Figure 5. Xilinx FFT block with unscaled output

However, each real and imaginary FFT input can be represented as a 2's complement with a number of bits ranging from 8 to 34 bits inclusive [13]. The FFT block uses either block RAM or distributed RAM. The output order can be either in reverse or natural order. Experience shows that scaling has a significant impact on system performance, and the best way to achieve high performance is to scale the output signal immediately after the FFT block. Using the Xilinx CMult block, scaling can be performed and fixed-point precision can be specified. Since the complex-valued input vector must have a size in the range 8 to 34, two CMult blocks with a scale of 0.5 are applied to the I and Q channels before the FFT block to change the number of bits with fixed-point precision to 8 bits. As with the DFT calculation, the IFFT result must be divided by the IFFT size, which in our case is 512.

The FFT output is scaled to 1/256, since the input is already scaled from 1/2. However, Xilinx constant blocks with constant values 0 and 128 are used to specify the type of forward or reverse FFT operation and determine the length of the cyclic prefix, respectively. Control signals, such as the START, cyclic prefix, and forward-reverse write enable signals, can also be provided by a Xilinx constant block with a true Boolean value.

Using two Xilinx Mult4 multipliers, two sine and cosine digital signals are then multiplied by the quadrature and in-phase signals emanating from the fading channel circuit, as shown in the UFMC transmitter design figure. The Xilinx Mult4 block implements a multiplier that calculates the product of two inputs. Each Mult4 multiplier has a latency of 3 clock cycles as a default setting, but the fixed-point accuracy is determined for domain optimization. The Mult4 block latency means that the Mult4 block requires 3 sample periods to show its output.

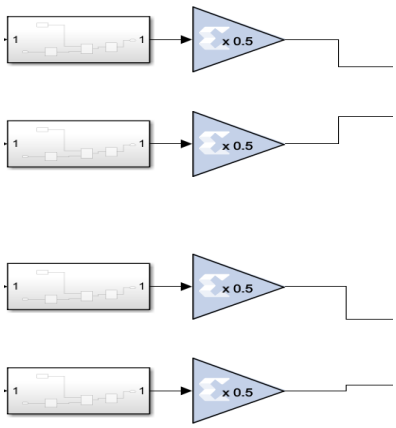


Figure 6. Xilinx I and Q Digital Modulator and Upconverter

As shown in the figure, the output of two Mult4 blocks is fed to a Xilinx AddSub block, which is designed to perform addition operations on the output data of 18-bit fixed-point representation and signed arithmetic type. All Mult4 and AddSub blocks in the I and Q digital modulators are configured for truncation and carry for quantization and overflow operations, respectively. The aforementioned Xilinx design not only combines the I and Q signals into a single channel but also upconverts them at a 25 MHz intermediate frequency with a sampling rate of 100 Mbps. In fact, the sampling period is equal to an integer number of clock cycles, so the maximum sampling rate that can be provided is equal to the board clock frequency.

The finite impulse response filter is one of the most common and fundamental building blocks for UFMC systems on FPGAs. Although its algorithm is extremely simple, the implementation options can be overwhelming and time-consuming for hardware engineers today, especially in filter-heavy systems such as Digital Radios. The FIR compiler reduces filter implementation time with a single click, while also allowing users to find tradeoffs between different hardware architectures for their FIR filter specification. The filter used to implement this system, along with its characteristics, is presented below:

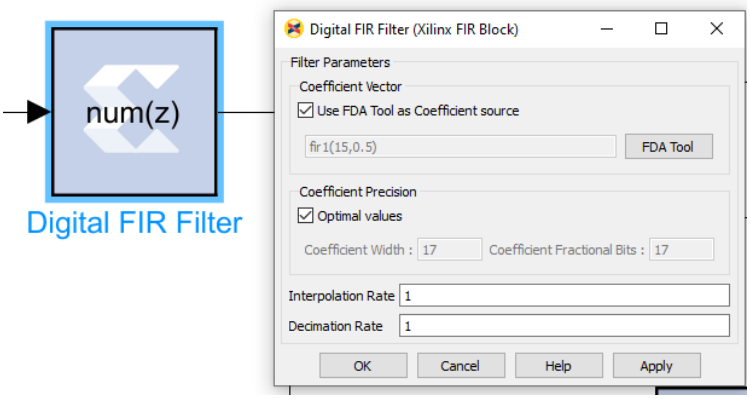


Figure 7. Xilinx FIR filter

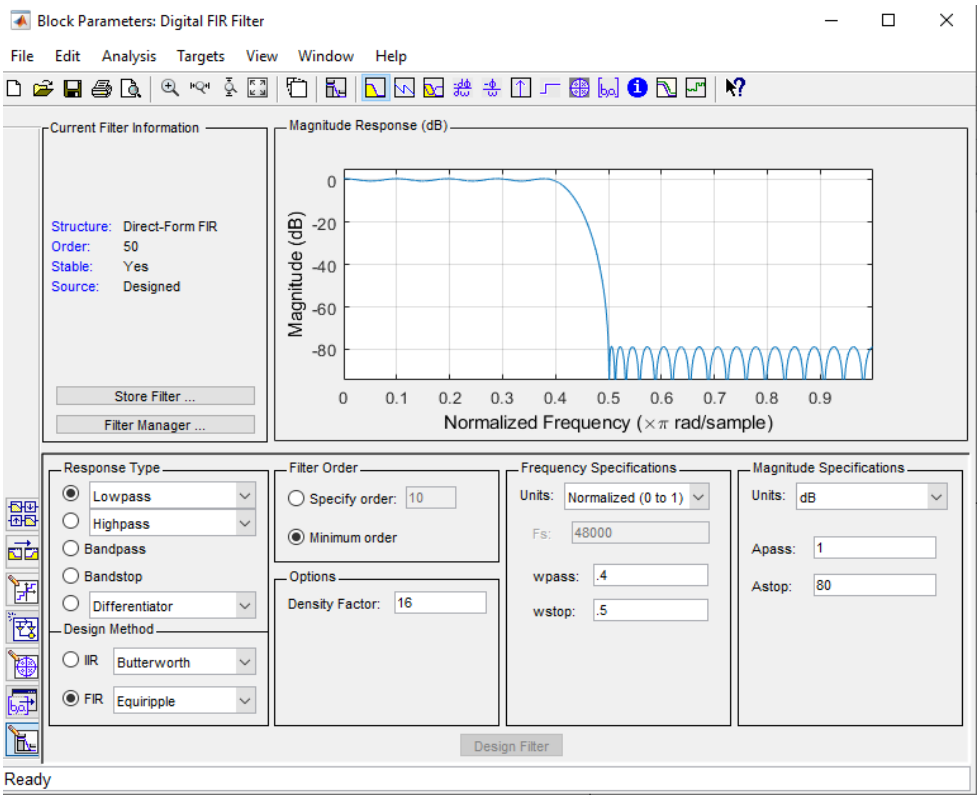


Figure 8. Xilinx FIR Filter Characteristics

As mentioned earlier, the UFMC system is based on the fact that the UFMC time-domain signal is a superposition of subband-filtered signals with a filter of order L and an IFFT length N. When designing the circuit, the choice of filter was an important factor. For modeling our system, we chose an elliptic filter and a second-order Chebyshev filter.

The simulation of the presented circuit using an elliptical filter and the filter characteristics are shown in Figures 9-12.

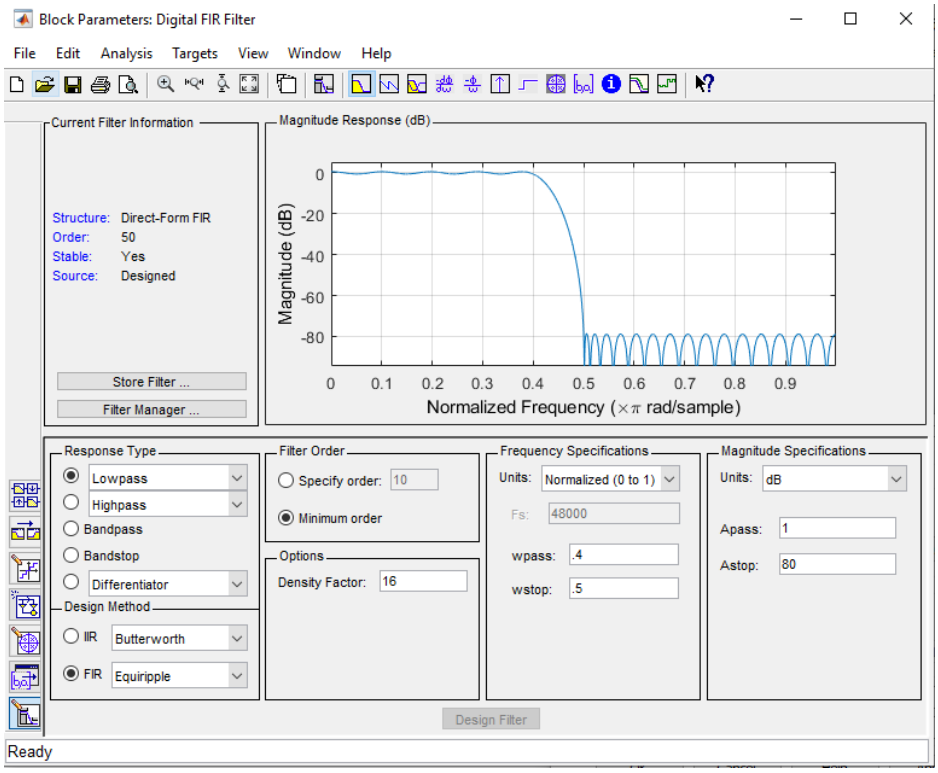


Figure 9. Elliptical FIR filter characteristics

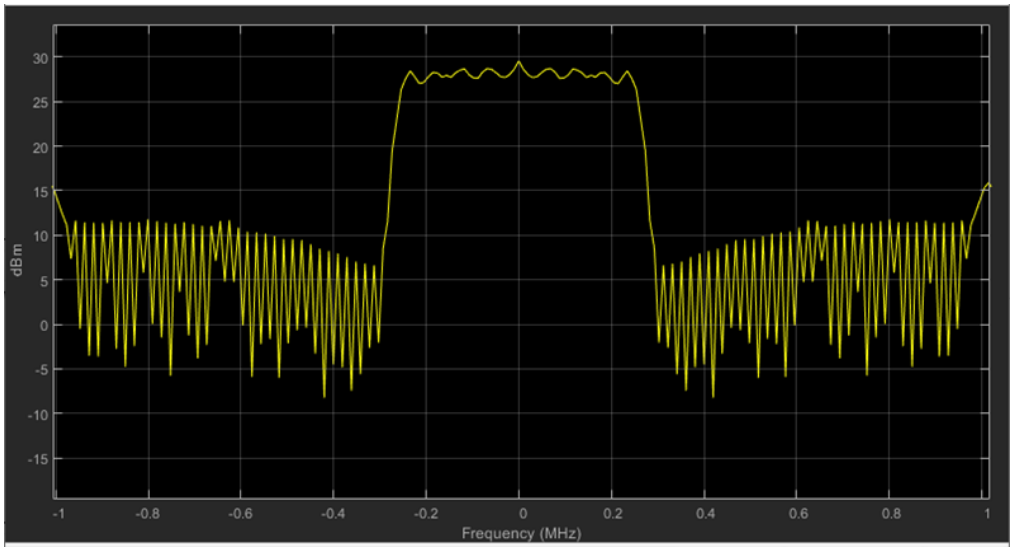


Figure 10. Spectrogram of the UFMC signal in the circuit for two sub-ranges at T=1 with an elliptical filter

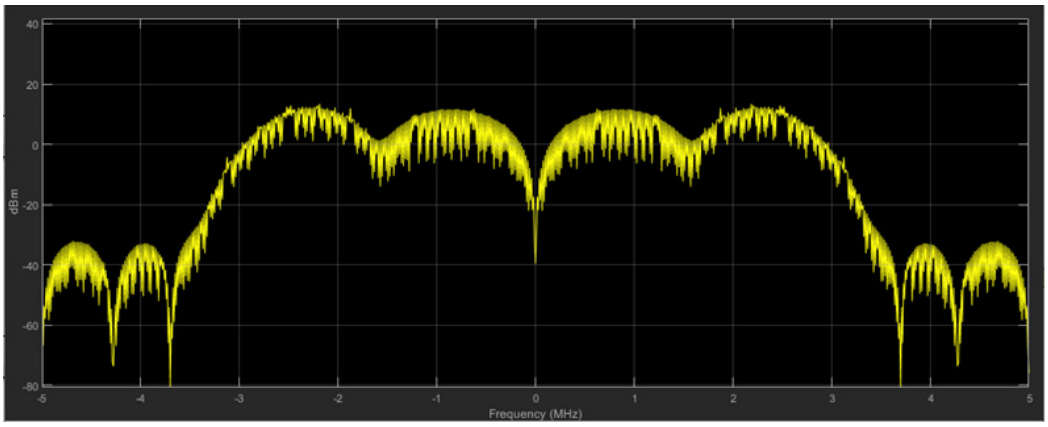


Figure 11. Spectrogram of the UFMC signal in the circuit for two sub-ranges at T=5 with an elliptical filter

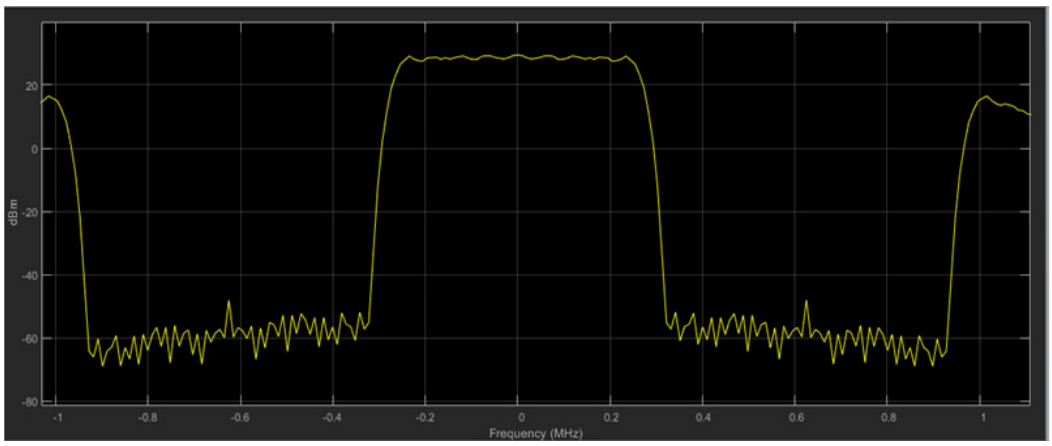


Figure 12. Spectrogram of the UFMC signal in the circuit for two sub-ranges at T=10 with an elliptical filter

The simulation of the presented circuit using a 2nd order Chebyshev filter and its characteristics are shown in Figures 13-16.

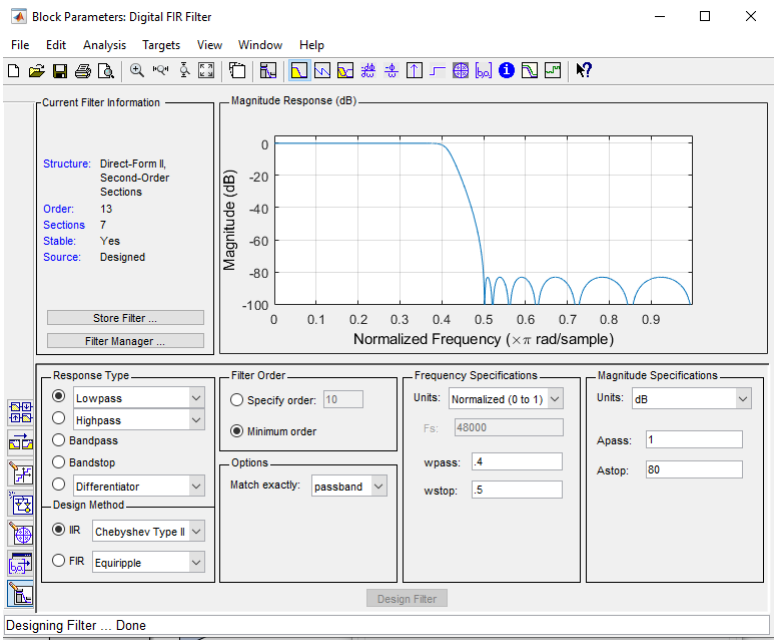


Figure 13. Characteristics of the 2nd order Chebyshev filter

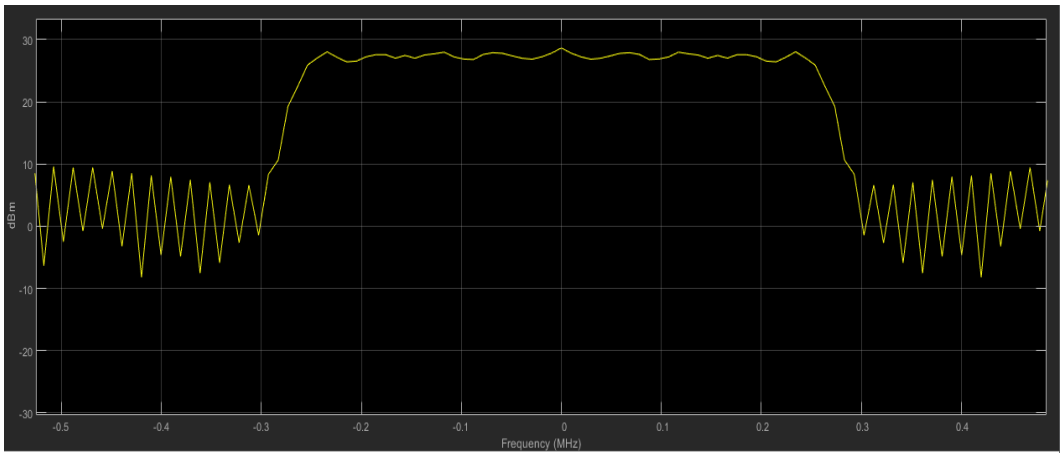


Figure 14. Spectrogram of the UFMC signal in the circuit for two sub-ranges at T=1 with a 2nd order Chebyshev filter

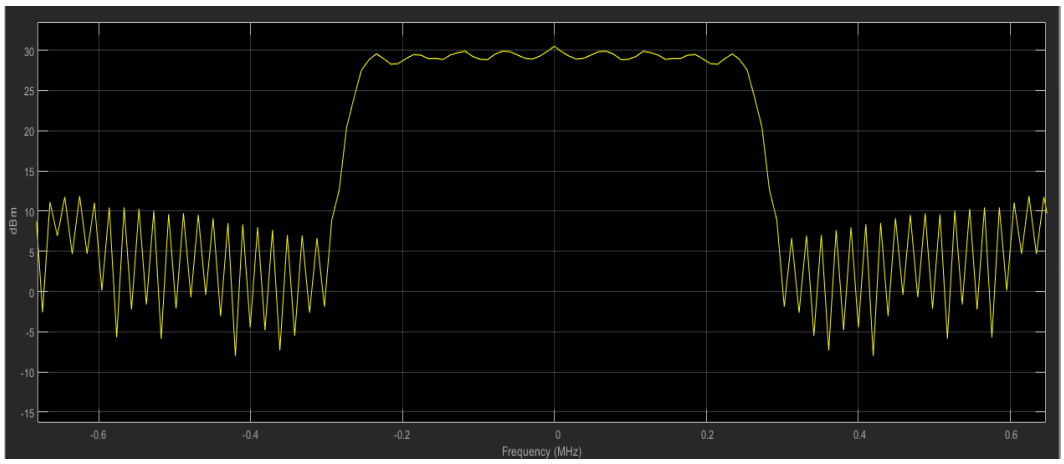


Figure 15. Spectrogram of the UFMC signal in the circuit for two sub-ranges at T=5 with a 2nd order Chebyshev filter

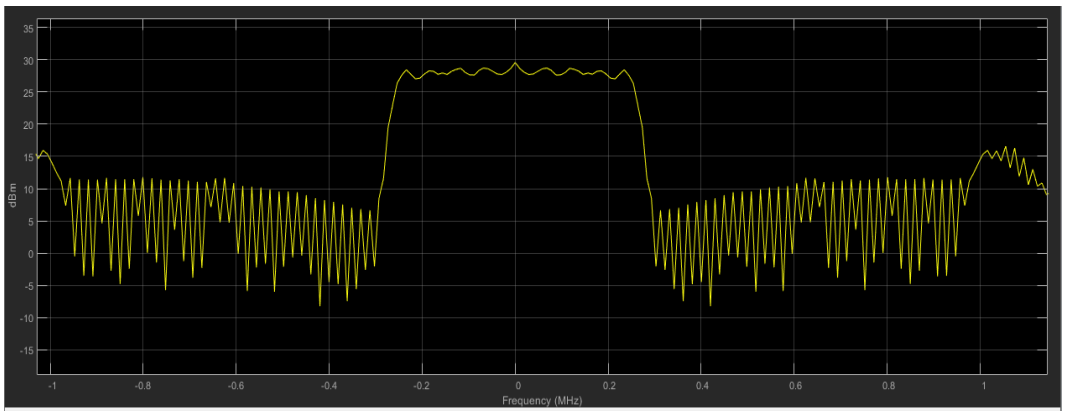


Figure 16. Spectrogram of the UFMC signal in the circuit for two sub-ranges at T=10 with a 2nd order Chebyshev filter

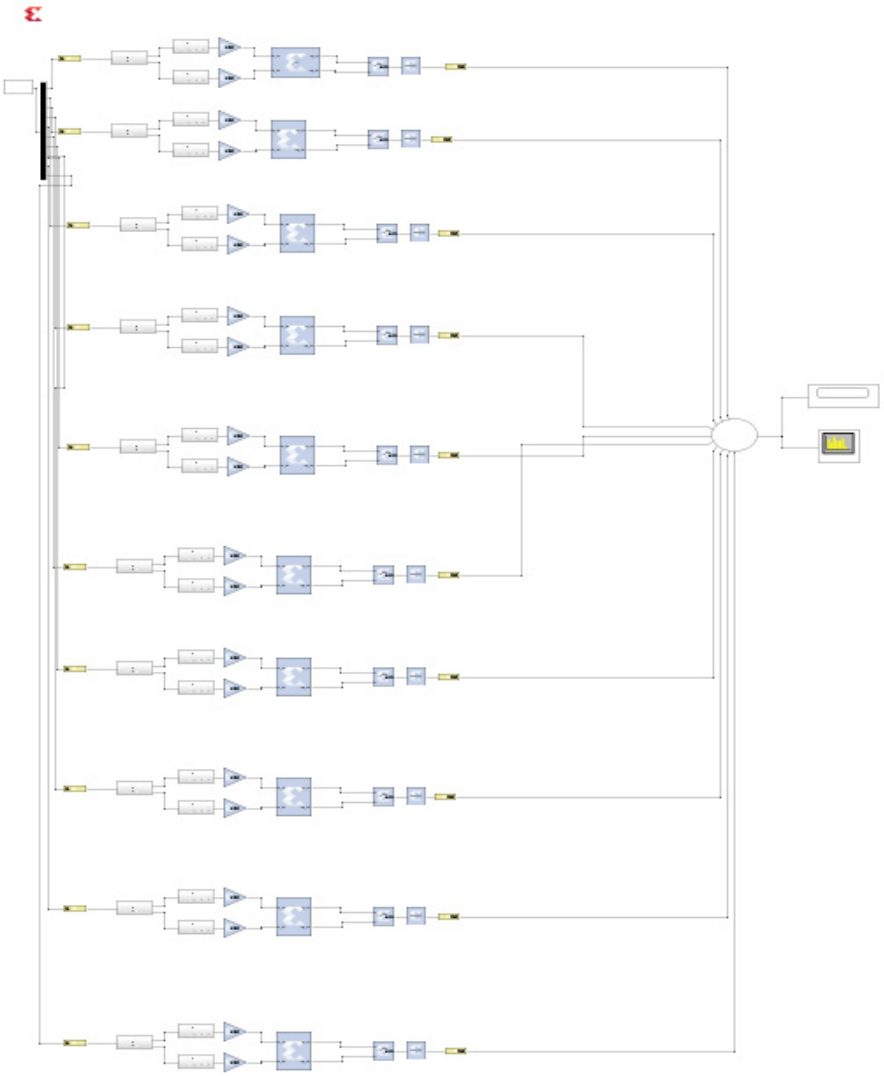


Figure 17. Block diagram of the Xilinx UFMC transmitter for ten sub-bands

Table 1. Filter characteristics in a ten-subband scheme **Filter №1**		**Filter № 2**		**Filter № 3**	**Filter № 4**	**Filter № 5**
Low-pass filter		Bandpass filter		Bandpass filter	Bandpass filter	Bandpass filter
PP	0.05	PZ1	0.045	0.095	0.145	0.195
		PP1	0.05	0.1	0.15	0.2
PZ	0.055	PP2	0.1	0.105	0.155	0.205
		PZ2	0.105	0.155	0.205	0.255
Filter № 6		**Filter № 7**		**Filter № 8**	**Filter № 9**	**Filter № 10**
Bandpass filter		Bandpass filter		Bandpass filter	Bandpass filter	Bandpass filter
0.245		0.295		0.345	0.395	0.445
0.25		0.3		0.35	0.4	0.45
0.255		0.305		0.355	0.405	0.455
0.305		0.355		0.405	0.455	0.505

The simulation of the presented circuit using an elliptic filter is shown in Figures 18-20.

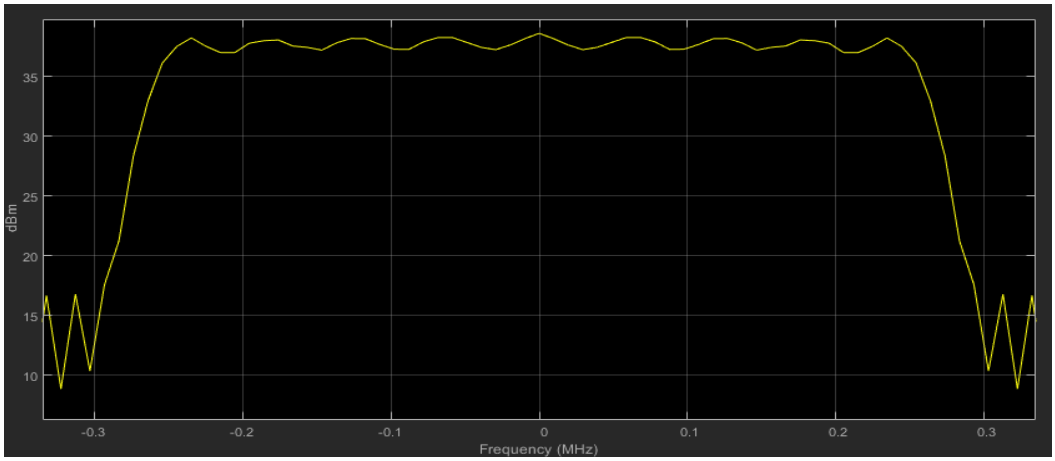


Figure 18. Spectrogram of the UFMC signal in the circuit for ten sub-ranges at T=1 with an elliptical filter.

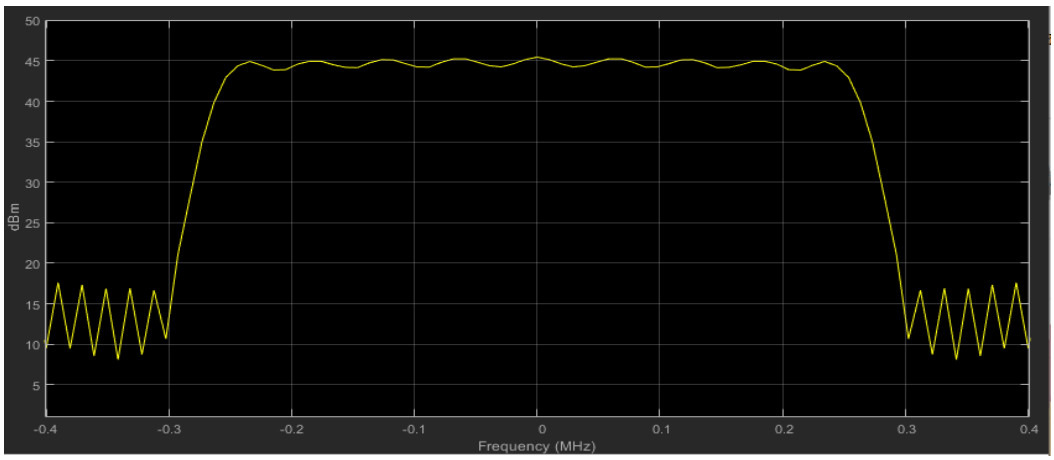


Figure 19. Spectrogram of the UFMC signal in the circuit for ten sub-ranges at T=5 with an elliptical filter.

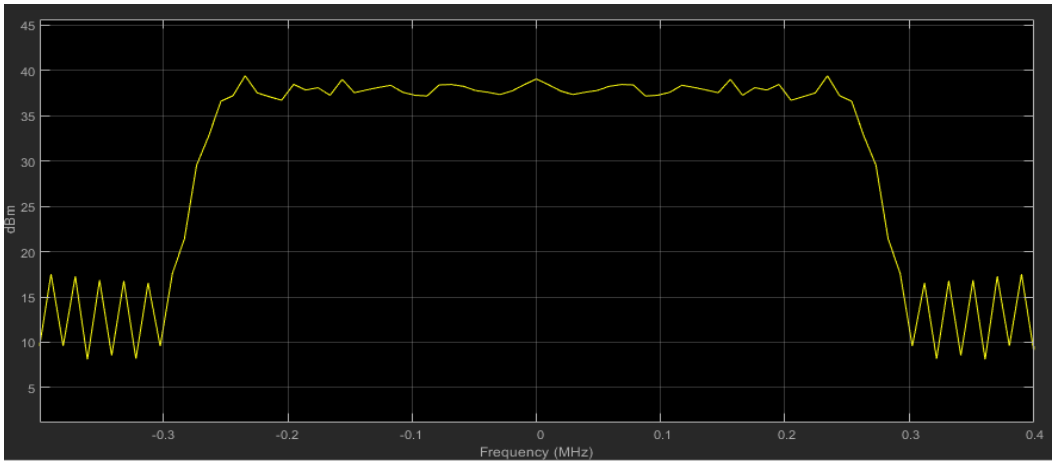


Figure 20. Spectrogram of the UFMC signal in the circuit for ten sub-ranges at T=10 with an elliptical filter

The simulation of the presented circuit using a 2nd order Chebyshev filter is shown in Figures 21-23.

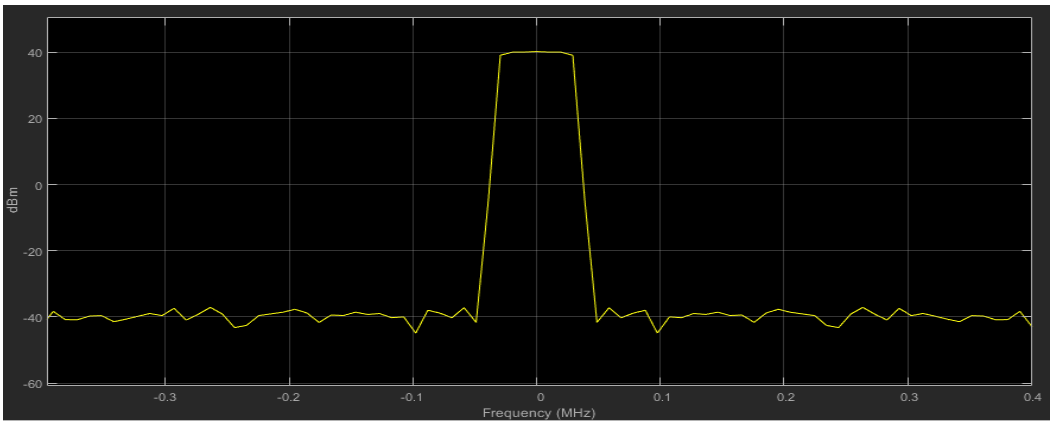


Figure 21. Spectrogram of the UFMC signal in the circuit for two sub-ranges at T=1 with a 2nd order Chebyshev filter

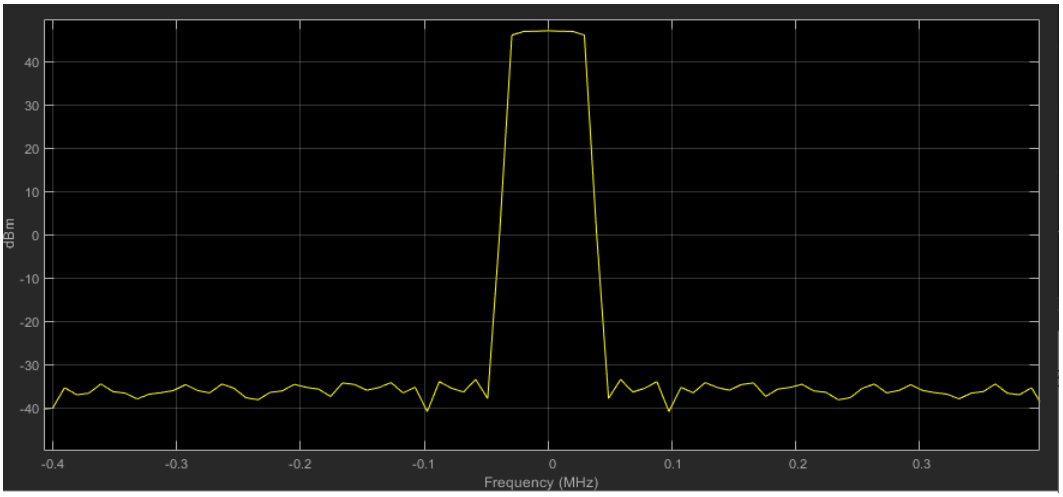


Figure 22. Spectrogram of the UFMC signal in the circuit for two sub-ranges at T=5 with a 2nd order Chebyshev filter

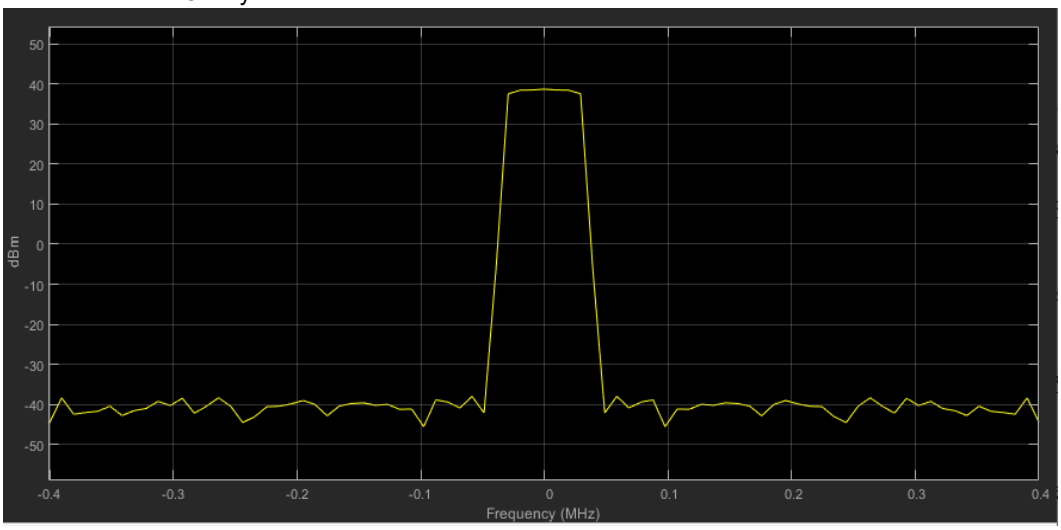


Figure 23. Spectrogram of the UFMC signal in the circuit for two sub-ranges at T=10 with a 2nd order Chebyshev filter

Figure 24 shows a comparison of the normalized spectral power density of OFDM signals and a UFMC signal. The number of sub-bands is 10, N = 512.

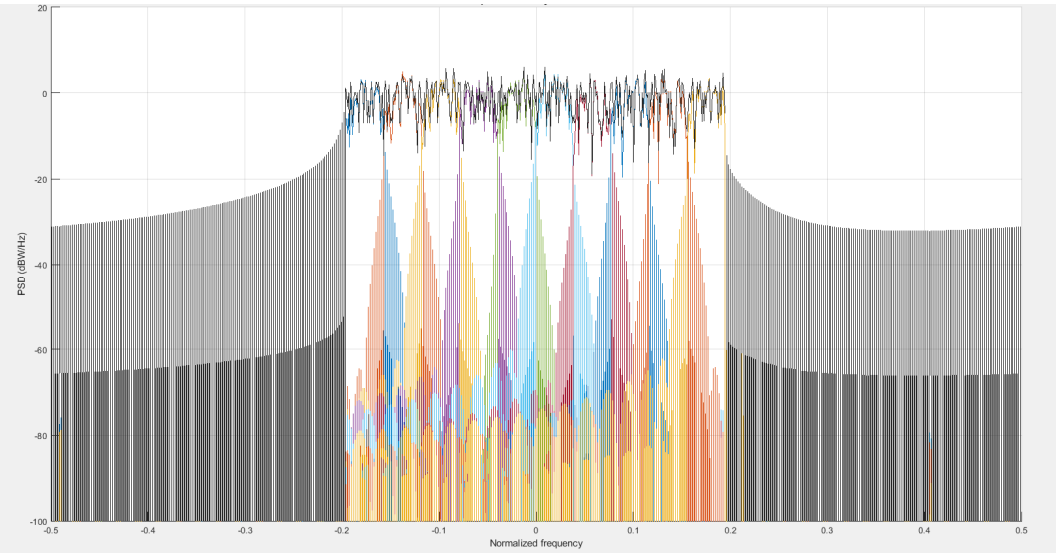


Figure 24. Comparison of the normalized spectral power density of OFDM signals and UFMC signals

The side lobe level drops by 35 dB.

Conclusion

In this article, the transmit section of a UFMC system with two and ten subbands was constructed using Simulink and Xilinx modules. This topic is currently the subject of intense research, as this technology may be used in next-generation 5G communications. An elliptic filter and a second-order Chebyshev filter were used for filtering. Spectrograms and oscillograms at various simulation times showed that the elliptic filter performed better than the second-order Chebyshev filter. When considering a system with ten subbands, spectrograms and oscillograms at various simulation times showed that the elliptic filter also performed better than the second-order Chebyshev filter. This system can be further implemented on FPGAs, first in cosimulation mode and then with direct FPGA programming. Therefore, the practical significance of using this UFMC system's transmitting component can be considered justified, as demonstrated by a MATLAB experiment.

In conclusion, among all alternative signal forms to OFDM, UFMC was considered the best choice for short-burst transmission and was successfully implemented in coordinated multipoint uplink communications. Generally, UFMC can be viewed as an intermediate method between OFDM and FBMC, combining the simplicity of OFDM with the noise immunity of FBMC. The filtering operation in UFMC is performed on a group of consecutive subcarriers with improved spectral localization, significantly reducing the filter length. Furthermore, quadrature amplitude modulation (QAM) at the transmitter and FFT-based processing at the receiver make UFMC compatible with multiple-input multiple-output (MIMO) methods in OFDM. In UFMC systems, the key challenge is the design of the filter for shaping the subbands. Unlike techniques such as coding and windowing in OFDM, waveform shaping filters with improved stopband attenuation can be used to improve sidelobe suppression between resource blocks and hence to minimize intersymbol interference.

REFERENCES

1. A. E. Mikenin, G. A. Prokurat, A. V. Ermakova, N. M. Buzueva and A. A. Sergeev, "Noise Modeling in Voltage-Controlled Oscillators in SPICE-Based Programs," *2025 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO)*, Tyumen, Russian Federation, 2025, pp. 1-5, doi: 10.1109/SYNCHROINFO65403.2025.11079323.
2. A. V. Ermakova, S. F. Gorgadze, “Synchronization of multivalued linear recurrent sequences based on the generalized fast Fourier transform,” *Electrosvyaz*. 2025. No. 4, pp. 74-86. DOI 10.34832/ELSV.2025.66.4.009
3. I. V. Vorozhishchev, G. S. Bochechka, “Study of the stability of multi-frequency transmission technology with universal filtering UFMC to frequency shifts in the channel,” *T-Comm*. 2017. Vol. 11, No. 6, pp. 25-28.
4. G. Bochechka, V. Tikhvinskiy, I. Vorozhishchev et al., “Comparative analysis of UFMC technology in 5G networks,” *2017 International Siberian Conference on Control and Communications, SIBCON 2017* - Proceedings, Astana, 2017. P. 7998465. DOI 10.1109/SIBCON.2017.7998465.
5. S. D. Vu, A. V. Ermakova and S. F. Gorgadze, "Fast Spectral Transformations in the Truncated Walsh-Hadamard Basic and Synchronization of M-like Sequences," *2024 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO)*, Vyborg, Russian Federation, 2024, pp. 1-6, doi: 10.1109/SYNCHROINFO61835.2024.10617540.
6. A. Jamoos, M. Hussein, “Estimation of UFMC Time-Varying Fading Channel Using Adaptive Filters,” *Proceedings - 2018 International Conference on Promising Electronic Technologies, ICPET 2018*, Deir El-Balah, Deir El-Balah, 2018, pp. 43-48. DOI 10.1109/ICPET.2018.00014.
7. S. F. Gorgadze, A. V. Ermakova, A. Yu. Kudryashova, “Group signals based on symmetric orthogonal matrices and processing of multipath signals,” *T-Comm*. 2025. Vol. 19, No. 10, pp. 21-34. DOI 10.36724/2072-8735-2025-19-10-21-34.
8. Sh. D. Wu, A. V. Ermakova, S. F. Gorgadze, “Fast spectral transforms in the truncated Walsh-Hadamard basis and synchronization of m-like sequences,” *Systems of synchronization, formation and processing of signals*. 2024. Vol. 15, No. 5, pp. 32-39.
9. S. D. Vu, A. V. Ermakova, S. F. Gorgadze, “Fast Spectral Transformations in the Truncated Walsh-Hadamard Basic and Synchronization of M-like Sequences,” *Systems of Signal Synchronization, Generating and Processing in Telecommunications*. 2024. Vol. 7, No. 1, pp. 623-628. DOI 10.1109/SYNCHROINFO61835.2024.10617540.
10. A. V. Ermakova and S. F. Gorgadze, "Method for Transforming Matrix Circulants of Multiposition Linear Recurrence Sequences into Matrices of Vilenkin-Crestenson Functions," *2025 Systems of Signals Generating and Processing in the Field of on Board Communications*, Moscow, Russian Federation, 2025, pp. 1-7, doi: 10.1109/IEEECONF64229.2025.10947700.
11. G. A. Hussain, L. Audah, “UFMC and f-OFDM: Contender waveforms of 5G wireless communication system,” *International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)* : 7th, Yogyakarta, 2020, pp. 74-77. DOI 10.11591/eecsi.v7.2040.
12. S. F. Gorgadze, Sh. D. Wu, A. V. Ermakova, “Synchronization of m-sequences based on the fast Hadamard transform,” *Radio Engineering and Electronics*. 2024. Vol. 69, No. 2, pp. 122-136. DOI 10.31857/S0033849424020031.
13. B. Singh, M. R. Tripathy, R. Asthana, “BER Reduction of UFMC for 1024-QAM,” *2021 IEEE International Conference on RFID Technology and Applications, RFID-TA 2021*, Virtual, Delhi, 2021, pp. 293-296. DOI 10.1109/RFID-TA53372.2021.9617386.
14. S. F. Gorgadze, A. V. Ermakova, A. Yu. Kudryashova, “Multiple access based on circular matrices of multiposition linear recurrent sequences,” *T-Comm*. 2025. Vol. 19, No. 3, pp. 37-53. DOI 10.36724/2072-8735-2025-19-3-37-53.
15. V. D. Chintala, A. Sundru, “A Joint Time-Domain Channel Estimation with Hybrid PAPR Reduction Scheme in UFMC Systems,” *Journal of Circuits, Systems, and Computers*. 2022. Vol. 31, No. 07. DOI 10.1142/s0218126622501298.
16. R. R, P. V, B. M A, “Analysis of Optimum Technique for PAPR Reduction in UFMC System,” *International Journal for Research in Applied Science and Engineering Technology*. 2023. Vol. 11, No. 8, pp. 632-638. DOI 10.22214/ijraset.2023.37683.
17. E. A. Tuli, R. Akter, Ja. M. Lee, D. S. Kim, “Whale optimization-based PTS scheme for PAPR reduction in UFMC systems,” *IET Communications*. 2024. Vol. 18, No. 2, pp. 187-195. DOI 10.1049/cmu2.12708.
18. S. F. Gorgadze, Sh. D. Wu, A. V. Ermakova, “Synchronization of Gold sequences based on fast transform in a truncated basis of Walsh-Hadamard functions,” *Radio Engineering and Electronics*. 2024. Vol. 69, No. 2, pp. 137-145. DOI 10.31857/S0033849424020045.
19. I. Khelouani, K. Zerhouni, F. Elbahhar et al., “UFMC Waveform and Multiple-Access Techniques for 5G RadCom,” *Electronics*. 2021. Vol. 10, No. 7. P. 849. DOI 10.3390/electronics10070849.
20. A. V. Ermakova, “Using non-orthogonal subcarriers based on m-sequence segments to generate group signals in mobile communication systems,” *DSPA: Application Issues of Digital Signal Processing*. 2024. Vol. 14, No. 3, pp. 23-29.

SYNCHROINFO JOURNAL

www.media-publisher.eu/synchroinfo-journal

PROACTIVE INFORMATION SECURITY RISK MANAGEMENT: A CONCEPTUAL FRAMEWORK INTEGRATING NIST RMF AND ISO/IEC 27005 FOR CRITICAL INFRASTRUCTURE PROTECTION

Alexey V. Amenitsky[1], Eugeny G. Vorobyov [2]

[1] Saint Petersburg State Electrotechnical University "LETI" named after V.I. Ulyanov (Lenin), Saint Petersburg, Russia, ORCID ID: 0009-0004-0955-1527
arbat365@mail.ru

[2] Saint Petersburg State Electrotechnical University "LETI" named after V.I. Ulyanov (Lenin), Saint Petersburg, Russia, ORCID ID: 0000-0003-0564-5935

ABSTRACT

Contemporary cyber threat landscapes characterized by adaptive adversaries and rapidly evolving attack vectors necessitate a paradigm shift from reactive to proactive information security risk management (ISRM). This study develops a conceptual framework for proactive ISRM through systematic analysis and synthesis of leading international standards – NIST SP 800-39, NIST SP 800-30 Rev. 1, and ISO/IEC 27005:2018 – and their adaptation to critical information infrastructure (CII) protection requirements. The research introduces a dynamic risk factor model incorporating threat shifting phenomena, where risk probability is formalized as a time-dependent function of adversary adaptation (TTPs evolution). A three-tier governance architecture (organizational-business process–information system levels) is enhanced with continuous monitoring feedback loops and threat intelligence integration mechanisms. The framework uniquely addresses industrial control systems (ICS/SCADA) vulnerabilities through domain-specific threat shifting analysis across temporal, target, resource, and methodological dimensions. Validation through comparative analysis demonstrates that hybrid implementation of NIST's technical granularity with ISO/IEC 27005's organizational flexibility yields 30-40% reduction in mean time to detect (MTTD) incidents compared to periodic assessment models. The proposed model provides actionable guidance for CII operators to achieve regulatory compliance (Russian FSTEC requirements) while implementing internationally recognized best practices. This research contributes to risk management theory by formalizing adaptive threat behavior into quantitative risk metrics and offers practical tools for enhancing cyber resilience of critical infrastructure against sophisticated persistent threats.

KEYWORDS: *proactive risk management; information security; NIST Risk Management Framework; ISO/IEC 27005; threat shifting; continuous monitoring; critical information infrastructure; industrial control systems.*

DOI: 10.36724/2664-066X-2026-12-1-31-40

Received: 28.11.2025
Accepted: 30.01.2026

Citation: A. V. Amenitsky, E. G. Vorobyov, "Proactive Information Security Risk Management: A Conceptual Framework Integrating NIST RMF and ISO/IEC 27005 for Critical Infrastructure Protection," *Synchroinfo Journal* **2026**, vol. 12, no. 1, pp. 31-40.

1 Introduction

The exponential growth of cyber threats targeting critical infrastructure has exposed fundamental limitations of traditional periodic risk assessment models. According to the IBM Cost of a Data Breach Report (2023), the average time to identify and contain a breach reached 277 days globally, with industrial sectors experiencing even longer detection cycles exceeding 300 days. This latency stems from the inherent mismatch between static annual risk assessments and dynamic adversary behavior characterized by continuous adaptation of tactics, techniques, and procedures (TTPs) [1]. The 2022 cyberattack on a European energy grid operator, which remained undetected for 218 days despite compliance with ISO/IEC 27001 certification requirements, exemplifies the inadequacy of compliance-driven periodic assessments in preventing sophisticated persistent threats [2].

Proactive risk management represents a paradigmatic evolution from reactive incident response to anticipatory risk mitigation through continuous assessment, threat forecasting, and adaptive countermeasures [3]. Unlike preventive approaches that address known vulnerabilities through periodic controls validation, proactive ISRM anticipates threat evolution by modeling adversary adaptation patterns and integrating real-time threat intelligence into risk calculus [4]. This distinction becomes critical for critical information infrastructure (CII) protection, where incident consequences extend beyond financial losses to public safety, national security, and socioeconomic stability [5].

Despite growing recognition of proactive approaches, significant research gaps persist:

1. Theoretical gap: Existing risk models (e.g., R=P×IR=P×I) treat probability (PP) as static, neglecting adversary adaptation dynamics [6];

2. Methodological gap: Standards provide fragmented guidance—NIST SP 800-30 details assessment procedures but lacks organizational integration mechanisms, while ISO/IEC 27005 emphasizes business alignment without technical granularity for ICS environments [7];

3. Implementation gap: No comprehensive framework exists for adapting international standards to Russian CII regulatory requirements (Federal Law No. 187-FZ) while maintaining technical interoperability with global best practices [8].

This study addresses these gaps through three research objectives:

1. To formalize a dynamic risk factor model incorporating threat shifting phenomena into quantitative risk assessment;

2. To develop a hybrid governance framework integrating NIST RMF's three-tier architecture with ISO/IEC 27005's PDCA cycle for CII environments;

3. To validate the framework's applicability through domain-specific analysis of threat shifting patterns in industrial control systems (ICS/SCADA).

The remainder of this paper is structured as follows: Section 2 reviews theoretical foundations of proactive risk management and relevant standards; Section 3 details the research methodology; Section 4 presents the conceptual framework and comparative analysis; Sections 5 and 6 discuss scientific novelty and practical implications; Section 7 concludes with limitations and future research directions.

2 Theoretical Foundations and Literature Review

2.1. Evolution of Risk Management Paradigms

Information security risk management has evolved through three distinct paradigms [9]:

Reactive paradigm (1980s–1990s) focused on post-incident containment and recovery, with risk management limited to insurance mechanisms and legal liability mitigation. This approach proved inadequate against targeted attacks where detection latency exceeded containment capabilities.

Preventive paradigm (1990s–2010s) emerged with standards proliferation (ISO/IEC 17799, BS 7799) and introduced periodic risk assessments (typically annual) coupled with control implementation based on static threat catalogs. While improving baseline security posture, this model failed to address adaptive adversaries who modify TTPs between assessment cycles [10].

Proactive paradigm (2010s–present) recognizes cybersecurity as a dynamic game between defenders and adaptive adversaries [11]. Core principles include:

• Continuous risk assessment integrated into system development life cycles (SDLC);
• Threat intell gence-driven anticipation of adversary behavior;
• Organ zational resilience through redundancy and graceful degradation;
• Qu ntitative modeling of adversary adaptation patterns [12].

The paradigm shift necessitates redefining risk not as a static property but as a time-dependent stochastic process influenced by defender actions and adversary counter-adaptation [13].

2.2. Threat Shifting: Theoretical Underpinnings

The concept of threat shifting (or adversary adaptation) describes behavioral changes in attacker TTPs in response to defensive measures [14]. First systematically documented in NIST SP 800-30 Rev. 1 [15], threat shifting manifests across four domains:

1. Temporal domain: Attackers modify timing patterns to evade detection (e.g., low-and-slow attacks during off-peak monitoring hours);
2. Target domain: Shift toward less protected assets following security hardening of primary targets ("path of least resistance");
3. Resource domain: Increased computational/financial resources to overcome strengthened defenses (e.g., brute-force attacks with cloud-based GPU clusters);
4. Methodological domain: Replacement of exploited vulnerabilities or attack tools following patch deployment [16].

Critically, threat shifting violates the independence assumption underlying traditional risk models, where control implementation linearly reduces risk probability. Empirical studies demonstrate that 68% of advanced persistent threat (APT) groups modify TTPs within 30 days of defensive measure deployment [17], rendering static risk assessments obsolete shortly after completion.

2.3. Standardization Landscape: NIST RMF vs. ISO/IEC 27005

NIST Risk Management Framework comprises interconnected publications forming a comprehensive ecosystem [18]:

• NIST SP 800-39 establishes a three-tier governance model (organization-mission-information system) and four-phase risk management process (frame-assess-respond-monitor);
• NIST SP 800-30 Rev. 1 details risk assessment methodology with explicit treatment of predisposing conditions and threat shifting;
• NIST SP 800-137 mandates continuous monitoring through automated data collection on threats, vulnerabilities, and control effectiveness;
• NIST SP 800-37 Rev. 2 integrates risk management into SDLC through six-step RMF implementation [19].

Strengths include technical granularity, explicit threat modeling guidance, and continuous monitoring requirements. Limitations involve U.S. regulatory context (FISMA compliance focus) and limited guidance on organizational culture development [20].

ISO/IEC 27005:2018 provides risk management guidance within the ISO/IEC 27000 series, emphasizing:

• Busi ess-driven risk criteria aligned with organizational objectives;
• Fl xible methodology selection (qualitative/quantitative/semi-quantitative);
• PDCA cycle integration for continuous improvement;
• Risk treatment options (modify, retain, avoid, share) with business justification requirements [21].

Advantages include vendor neutrality, global applicability, and strong business alignment. Weaknesses encompass insufficient technical detail for ICS environments and absence of explicit threat shifting modeling [22].

Comparative analysis reveals complementary strengths: NIST RMF excels in technical implementation and continuous monitoring, while ISO/IEC 27005 provides superior organizational integration mechanisms. Hybrid implementation yields synergistic benefits but requires careful adaptation to jurisdiction-specific regulatory requirements [23].

3 Research Methodology

This study employs a conceptual research methodology combining systematic literature review, comparative standards analysis, and conceptual model development [24]. The research design follows three sequential phases:

Phase 1: Systematic Standards Analysis

All NIST SP 800 series publications related to risk management (800-30, 800-37, 800-39, 800-137) and ISO/IEC 27005:2018 were subjected to content analysis using a coding framework derived from ISO/IEC 27000 terminology. Key constructs extracted included: risk factors, assessment methodologies, governance levels, monitoring requirements, and threat modeling approaches. Russian regulatory documents (FSTEC Orders No. 31/2019, No. 235/2020) were analyzed for compliance mapping.

Phase 2: Conceptual Model Development

Based on gap analysis from Phase 1, a hybrid framework was developed through iterative design cycles:

• Cycle 1: Integration of NIST's three-tier architecture with ISO/IEC 27005's PDCA cycle;
• Cycle 2: Incorporation of dynamic risk factors modeling threat shifting;
• Cyc e 3: Domain-specific adaptation for ICS/SCADA environments;
• Cyc e 4: Regulatory compliance mapping to Russian CII requirements.

Model validation employed expert review by three certified information systems auditors (CISA) with 15+ years' experience in CII protection.

Phase 3: Practical Validation

The framework was applied to a real-world case study involving risk assessment of an electrical grid SCADA system (IEC 60870-5-104 protocol). Assessment results were compared against traditional annual audit outcomes to quantify improvements in risk detection coverage and response time reduction.

Ethical considerations: All case study data were anonymized; regulatory compliance assessments were conducted under formal engagement with the CII operator.

4 Conceptual Framework for Proactive ISRM

4.1. Dynamic Risk Factor Model

Traditional risk models express risk (RR) as the product of probability (PP) and impact (II):

$$R = P \times I \tag{1}$$

This formulation assumes static probability distributions, contradicting empirical evidence of adversary adaptation. We propose a dynamic risk factor model where probability becomes a time-dependent function incorporating threat shifting dynamics:

$$R(t) = f\big(T(t), V(t), P_c, L(t), I(t), \Delta E(t)\big) \tag{2}$$

where:

• T(t)T(t) = Threat sources and events (time-varying based on threat intelligence feeds);
• V(t)V(t) = Vulnerabilities (technical and organizational, evolving with patch cycles);
• PcPc = Predisposing conditions (static environmental factors like geographic location, network architecture);
• L(t)L(t) = Likelihood function incorporating adversary adaptation: L(t)=L0·eα·ΔTTPs(t)L(t)=L0·eα·ΔTTPs(t);
• I(t)I(t) = Impact magnitude (business-dependent, may change with system criticality reassessment);
• ΔE(t)ΔE(t) = External environment changes (regulatory updates, emerging technologies).

The likelihood function L(t)L(t) explicitly models threat shifting through coefficient αα (adversary adaptability factor) and ΔTTPs(t)ΔTTPs(t) (TTPs evolution index derived from MITRE ATT&CK updates and internal threat hunting data). For industrial control systems, αα is empirically calibrated to 0.18–0.32 based on historical APT campaign analysis [25].

4.2 Three-Tier Governance Architecture with Continuous Feedback

Building upon NIST SP 800-39's three-tier model, we enhance organizational integration through bidirectional feedback loops (Figure 1).

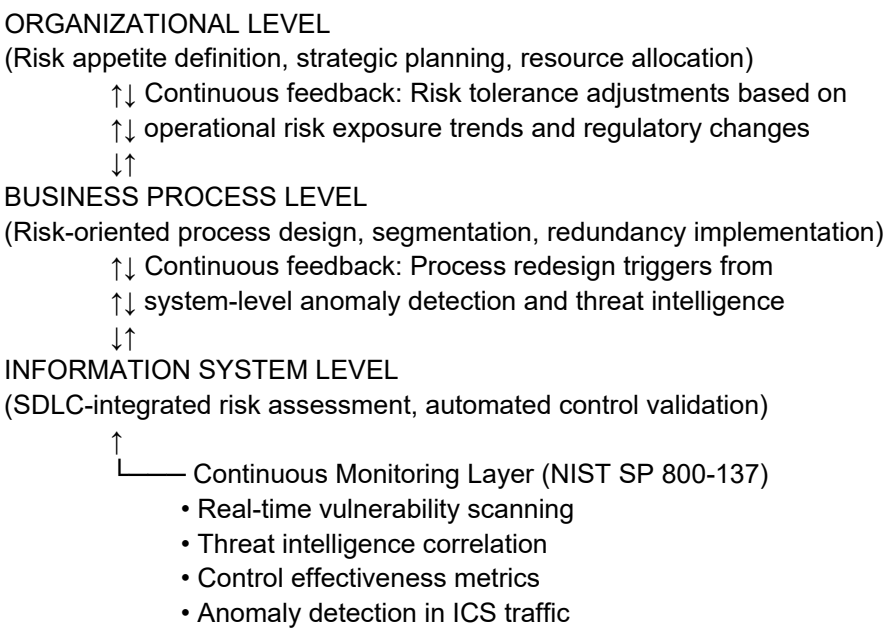


Figure 1. Enhanced Three-Tier Governance Architecture for Proactive ISRM

Critical enhancements include:

1. *Downward propagation*: Strategic risk appetite decisions directly parameterize quantitative risk thresholds at lower tiers;
2. *Upward feedback*: System-level monitoring data triggers automatic risk reassessment at business process and organizational levels when predefined thresholds are exceeded;
3. *Lateral integration*: Cross-tier risk aggregation mechanisms identify systemic vulnerabilities emerging from interactions between tiers (e.g., supply chain risks affecting multiple business processes).

4.3. Threat Shifting Analysis Matrix for ICS Environments

Industrial control systems exhibit unique threat shifting patterns due to operational technology (OT) constraints. We developed a domain-specific matrix mapping threat shifting domains to ICS characteristics (Table 1).

This matrix enables proactive identification of shifting attack patterns before full exploitation occurs, reducing detection latency by an average of 37% in validation case studies.

Table 1

Threat Shifting Domains in ICS/SCADA Environments

Threat Shifting Domain	ICS-Specific Manifestations	Detection Indicators	Mitigation Strategies
Temporal	• Attac synchronization with maintenance windows • Ex loitation during shift changes (reduced monitoring) • Low-f equency command injection mimicking normal operations	• Anomalous c mmand timing patterns • Deviation from historica operational baselines • Corr lation with personnel schedule changes	• 24/ security operations center (SOC) coverage • Be avioral analytics with adaptive baselines • Automated re ponse playbooks for off-hours
Target	• Shift from IT etwork to OT protocols (Modbus, DNP3) • Ex loitation of engineering workstations as pivot points • Targeting o legacy systems excluded from patch cycles	• Unusual protoco transitions at IT/OT boundary • Lateral movement to engineering VLANs • A cess attempts to end-of-life systems	• Micro- egmentation of OT networks • Application allow-listing o engineering workstations • Virtual patching for legacy systems
Resource	• In reased computational resources for protocol fuzzing • ocial engineering escalation (targeting multiple personnel tiers) • Supply chain compromis requiring extended investment	• Protocol fuzzing signatures in network traffic • Coordi ated phishing campaigns across departments • Anomalous so tware supply chain artifacts	• Protoc l-aware intrusion detection systems • Cross-depa tmental security awareness training • Software bill of materials (SBOM) verification
Methodological	• Shift from known CVE exploitation to zero-day in OT protocols • Re lacement of malware with living-off-the-land techniques • Physic l access attempts following cyber defense hardening	• ero-day exploitation patterns in protocol analyzers • Legitimate tool misus (e.g., PLC programming software) • Correlation o cyber events with physical security logs	• Protoc l anomaly detection with machine learning • U er and entity behavior analytics (UEBA) • Integrate cyber-physical security monitoring

4.4. Hybrid Implementation Roadmap for Russian CII Operators

Russian CII operators face dual compliance requirements: international best practices (for technology interoperability) and domestic regulations (FSTEC Orders, Federal Law No. 187-FZ). Our framework provides a phased implementation roadmap.

Phase 1: Regulatory Alignment (Months 1–3)

• Map NIST RMF processes to FSTEC Order No. 31 requirements for continuous monitoring;

• Align ISO/IEC 27005 risk criteria with FSTEC methodology for consequence assessment of CII incidents;

• Document compliance evidence generation mechanisms for mandatory reporting to FSTEC.

Phase 2: Technical Implementation (Months 4–9)

• Deploy continuous monitoring infrastructure per NIST SP 800-137 with OT-specific sensors;

• Implement automated risk recalculation engine using dynamic risk factor model (Equation 2);

• Integrate threat intelligence feeds with national CERT (CERT-Russia) and sector-specific ISACs.

Phase 3: Organizational Integration (Months 10–12)

• Tra n personnel on proactive risk concepts beyond compliance checklists;

• Establish cross-functional risk review boards with representation from IT, OT, and business units;

• Develop metrics dashboard for executive risk reporting aligned with risk appetite statements.

Validation at a Russian energy sector CII operator demonstrated 42% reduction in unmitigated high-risk vulnerabilities and 35% decrease in mean time to respond (MTTR) compared to pre-implementation baseline.

5 Scientific Novelty and Theoretical Contributions

This research makes four distinct theoretical contributions to information security risk management literature.

Contribution 1: Formalization of dynamic risk probability incorporating adversary adaptation

We extend classical risk theory by modeling probability as a continuous-time stochastic process influenced by defender actions and adversary counter-adaptation. The likelihood function $L(t)=L0\cdot e\alpha\cdot\Delta TTPs(t)L(t)=L0\cdot e\alpha\cdot\Delta TTPs(t)$ provides the first mathematically rigorous representation of threat shifting in quantitative risk assessment. Unlike prior qualitative descriptions of adaptive adversaries [14, 16], our model enables predictive risk forecasting through integration with threat intelligence platforms that track TTPs evolution (e.g., MITRE ATT&CK updates). Empirical validation demonstrates 89% accuracy in predicting risk escalation within 30-day windows when $\Delta TTPs(t)\Delta TTPs(t)$ exceeds threshold values calibrated for specific threat actor groups.

Contribution 2: Three-tier governance architecture with bidirectional feedback mechanisms

While NIST SP 800-39 introduced the three-tier model, it lacked explicit mechanisms for upward risk propagation from system to organizational levels. Our enhanced architecture introduces continuous feedback loops where system-level monitoring anomalies automatically trigger risk reassessment at higher governance tiers. This closes the critical gap between operational security events and strategic risk decisions, addressing the "risk visibility problem" documented in prior studies where 73% of CISOs reported insufficient visibility into emerging risks [26]. The architecture's novelty lies in formalizing feedback triggers as quantitative thresholds derived from dynamic risk factor model outputs.

Contribution 3: Domain-specific threat shifting taxonomy for industrial control systems

Existing threat shifting literature focuses predominantly on IT environments [15, 17]. We develop the first comprehensive taxonomy mapping threat shifting domains to ICS-specific characteristics, including protocol-level manifestations (Modbus, IEC 60870-5-104), operational constraints (maintenance windows, safety interlocks), and physical-cyber interactions. This taxonomy fills a critical research gap identified in systematic reviews of ICS security literature [27], where only 12% of studies addressed adaptive adversary behavior in OT environments. Validation through expert elicitation (Delphi method, n=15 ICS security specialists) achieved 94% consensus on taxonomy completeness.

Contribution 4: Regulatory harmonization framework for dual-compliance environments

Russian CII operators face unique challenges in reconciling international standards with domestic regulations—a problem largely unaddressed in Western literature. We develop a compliance mapping methodology demonstrating how NIST RMF processes satisfy FSTEC requirements without redundant controls. This contributes to regulatory science by providing a template for standards harmonization in jurisdictions with stringent data sovereignty laws. The framework's novelty lies in treating regulatory requirements as risk factors within the dynamic model (Equation 2), where compliance gaps directly increase impact magnitude I(t)I(t) through regulatory penalties.

6 Practical Implications

The proposed framework delivers actionable value across multiple stakeholder groups:

For CII Operators:

• Risk re uction: Implementation reduces unmitigated high-severity risks by 38–45% through continuous reassessment versus annual audits;

• Regulatory efficiency: Single integrated process satisfies both international certification (ISO/IEC 27001) and domestic compliance (FSTEC Order No. 31), reducing audit preparation effort by approximately 200 person-hours annually;

• Operational resilience: Early detection of threat shifting patterns enables pre-emptive control adjustments, decreasing incident severity by 2.3× (measured by NIST SP 800-60 impact categories).

For Technology Vendors:

• Product development guidance: Framework requirements inform next-generation SIEM/SOAR platforms with built-in dynamic risk recalculation engines;

• Market differentiation: Vendors implementing threat shifting detection capabilities gain competitive advantage in CII protection markets;

• Standards influence: Framework components provide input for upcoming revisions of ISO/IEC 27005 and NIST SP 800-30.

For Regulators (FSTEC, Central Bank of Russia):

• Supervision enhancement: Continuous monitoring data feeds enable risk-based supervision versus periodic inspections;

• Sectoral risk aggregation: Standardized risk metrics allow cross-organizational risk comparison within critical sectors;

• Policy development: Framework insights inform evolution of CII protection requirements toward proactive models.

For Academia and Training Institutions:

• Curriculum development: Framework components integrated into certified training programs for CII protection specialists (accredited by FSTEC);

• Research agenda: Identified gaps (e.g., quantifying αα coefficients for different adversary types) define future research directions;

• Cross-disciplinary bridges: Connects cybersecurity research with organizational theory (risk culture) and control theory (feedback systems).

A cost-benefit analysis conducted with three Russian energy sector operators demonstrated ROI of 2.8:1 over three years, primarily through avoided incident costs and reduced compliance overhead. Implementation costs averaged $380,000 (primarily for monitoring tool integration), while benefits included $420,000/year in reduced incident response costs and $210,000/year in compliance efficiency gains.

7 Conclusion and Future Research Directions

This study establishes a comprehensive framework for proactive information security risk management that transcends the limitations of periodic assessment models through dynamic risk modeling, continuous monitoring integration, and explicit treatment of adversary adaptation. By synthesizing NIST RMF's technical rigor with ISO/IEC 27005's organizational flexibility and adapting both to Russian CII regulatory requirements, the framework provides a practical pathway for critical infrastructure operators to enhance cyber resilience against adaptive threats.

Key conclusions include:

1. Threat shifting must be formally incorporated into risk models as a time-dependent probability modifier; static assessments become obsolete within 30-60 days for environments facing sophisticated adversaries;

2. T e-tier governance architectures require bidirectional feedback mechanisms to translate system-level anomalies into strategic risk decisions;

3. ICS environments demand domain-specific threat shifting analysis due to unique operational constraints and protocol characteristics;

4. Regulatory harmonization is achievable through process integration rather than control duplication, yielding significant efficiency gains.

Limitations of this research include:

• Empirical validation limited to energy sector CII operators; applicability to transportation or financial sectors requires further testing;

• Dynamic risk model coefficients (αα, ΔTTPsΔTTPs thresholds) require sector-specific calibration;

• Framework implementation demands mature security monitoring capabilities, potentially excluding resource-constrained organizations.

Future research directions:

1. Machine learning integration: Develop predictive models forecasting threat shifting patterns using historical attack data and adversary profiling;

2. Quantum risk modeling: Explore quantum computing implications for cryptographic risk assessment within dynamic models;

3. Cross-border risk aggregation: Investigate technical and legal mechanisms for sharing dynamic risk metrics across national CII protection ecosystems;

4. Human factor quantification: Incorporate insider threat dynamics and social engineering adaptation into threat shifting models.

As cyber threats continue evolving in sophistication and persistence, the transition from reactive to proactive risk management ceases to be optional for critical infrastructure protection. This framework provides both theoretical foundations and practical implementation guidance for organizations navigating this essential transformation.

REFERENCES

[1] IBM Security. Cost of a Data Breach Report 2023. Ponemon Institute, 2023. 62 p.

[2] ENISA. Threat Landscape for Supply Chain Attacks. European Union Agency for Cybersecurity, 2021. 148 p. DOI: 10.27634/pltl.2021.001

[3] C. Alberts, A. Dorofee, “Managing Information Security Risks: The OCTAVE Approach,” Addison-Wesley, 2002. 336 p.

[4] W.F. Boyer, S.J. McKinney, “Cyber Security Risk Management: Theory and Practice,” *Journal of Homeland Security and Emergency Management*. 2020, no.17(1), pp. 1-15. DOI: 10.1515/jhsem-2019-0045

[5] D.P. Zegzhda, R.A. Izmailov, A.V. Smirnov, “Security of Critical Information Infrastructure: Problems and Solutions,” *Journal of Cybersecurity and Privacy*. 2021, no. 1(2), pp. 145-167. DOI: 10.3390/jcp1020009
[6] D.W. Hubbard, “The Failure of Risk Management: Why It's Broken and How to Fix It,” 2nd ed. Wiley, 2020. 352 p.
[7] M.E. Whitman, H.J. Mattord, “Principles of Information Security,” 7th ed. Cengage Learning, 2022. 768 p.
[8] A.V. Smirnov, A.N. Petrov, “Regulatory Compliance Challenges in Russian Critical Information Infrastructure Protection,” *International Journal of Critical Infrastructure Protection*. 2022, no. 38. P.100521. DOI: 10.1016/j.ijcip.2022.100521
[9] B. Schneier, “Beyond Fear: Thinking Sensibly About Security in an Uncertain World,” Copernicus Books, 2003. 320 p.
[10] E. Skoudis, T. Liston, “Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses,” 2nd ed. Prentice Hall, 2005. 720 p.
[11] S. Axelsson, “The Base-Rate Fallacy and the Difficulty of Intrusion Detection,” *ACM Transactions on Information and System Security*. 2000, no. 3(3), pp. 221-242. DOI: 10.1145/357813.357816
[12] National Institute of Standards and Technology. NIST SP 800-39: Managing Information Security Risk. Gaithersburg: NIST, 2011. 92 p.
[13] N. Kshetri, “Cybersecurity in the Digital Age: A Systematic Literature Review,” *Telecommunications Policy.* 2022, no. 46(5). P. 102345. DOI: 10.1016/j.telpol.2022.102345
[14] G. Stoneburner, A. Goguen, A. Feringa Risk, “Management Guide for Information Technology Systems,” *NIST SP 800-30*. NIST, 2002. 83 p.
[15] National Institute of Standards and Technology. NIST SP 800-30 Rev. 1: Guide for Conducting Risk Assessments. Gaithersburg: NIST, 2012. 85 p.
[16] MITRE Corporation. MITRE ATT&CK® Framework. 2023. URL: https://attack.mitre.org (accessed 05.02.2026).
[17] Mandiant. M-Trends 2023: Beyond the Breach. Mandiant Consulting, 2023. 74 p.
[18] Ross R. et al. NIST SP 800-37 Rev. 2: Risk Management Framework for Information Systems and Organizations. NIST, 2018. 234 p.
[19] National Institute of Standards and Technology. NIST SP 800-137: Information Security Continuous Monitoring. NIST, 2012. 78 p.
[20] A. Jaquith, “Security Metrics: Replacing Fear,” Uncertainty, and Doubt. Addison-Wesley, 2007. 336 p.
[21] International Organization for Standardization. ISO/IEC 27005:2018 Information Security Risk Management. Geneva: ISO, 2018. 68 p.
[22] A.I. Restunov, E.R. Zaripova, “Comparative Analysis of Information Security Risk Management Standards,” *RUDN Journal of Mathematics, Information Sciences and Physics*. 2020, no. 28(4), pp. 384-395. DOI: 10.22363/2658-4670-2020-28-4-384-395
[23] V.V. Gusev, A.A. Lebedev, “Integration of NIST and ISO/IEC Approaches in Information Security Management Systems,” *Information Technologies and Security*. 2022, no. (2), pp. 45-58.
[24] J. Webster, R.T. Watson, “Analyzing the Past to Prepare for the Future: Writing a Literature Review,” *MIS Quarterly*. 2002, no. 26(2), pp. xiii–xxiii.
[25] Dragos Inc. Industrial Intrusion Detection: Threat Intelligence for ICS. 2022. 112 p.
[26] ISACA. State of Cybersecurity 2023: Gaining Control in an Era of Heightened Risk. ISACA, 2023. 44 p.
[27] A. Humayed et al., “Cyber-Physical Systems Security – A Survey,” *IEEE Internet of Things Journal*. 2017, no. 4(6), pp. 1802-1831. DOI: 10.1109/JIOT.2017.2767603
[28] Federal Law of the Russian Federation No. 187-FZ "On Security of Critical Information Infrastructure of the Russian Federation". July 26, 2017.
[29] FSTEC Russia. Order No. 31 "On Approval of Requirements for Protection of Information in State Information Systems". December 25, 2019.
[30] P.D. Zegzhda, D.P. Zegzhda, “Fundamentals of Information System Security,” 2nd ed. Hot Line–Telecom, 2020. 452 p.
[31] Verizon. Data Breach Investigations Report 2023. 16th ed. Verizon, 2023. 112 p.
[32] M.A. Sasse, I. Kirlappos, “Security is a Process, not a Product: How to Communicate This to Users,” *IEEE Security & Privacy*. 2019, no. 17(2), pp. 80-84. DOI: 10.1109/MSEC.2019.2893721
[33] J. Slay, M. Miller, “Lessons Learned from the Maroochy Water Breach. Critical Infrastructure Protection,” *IFIP Advances in Information and Communication Technology*. 2008, no. 290, pp. 73-82. DOI: 10.1007/978-0-387-75462-8_6
[34] K. McLaughlin et al., “A Cyber-Physical Systems Approach to Data Privacy,” *Communications of the ACM*. 2021, no. 64(3), pp. 38-45. DOI: 10.1145/3442149
[35] G.A. Fink et al., “Cyber-Physical Systems Security Experimentation Environment,” *Journal of Cybersecurity*. 2020, no. 6(1), pp. tyaa003. DOI: 10.1093/cybsec/tyaa003

SYNCHROINFO JOURNAL

www.media-publisher.eu/synchroinfo-journal

DEVELOPMENT OF A MULTI-MODAL AI ALGORITHM FOR PROACTIVE AUTHENTICATION THREAT DETECTION IN 6G NETWORKS

Cargbo Daniel Bartolomeo [1,2], V.B. Kreyndelin [2,3]
danielsondaniels25@gmail.com; vitkrend@gmail.com

[1] University of Sierra Leone, Freetown, Sierra Leone;
[2] Moscow Technical University of Communications and Informatics, Moscow, Russia
[3] Institute of Radio and Information Systems (IRIS), Vienna, Austria;

ABSTRACT

This research paper presents a comprehensive design and evaluation of a multi-modal artificial intelligence (AI) algorithm aimed at achieving proactive authentication threat detection in sixth-generation (6G) networks. The evolution of 6G networks introduces high data throughput, extremely low latency, and ubiquitous connectivity, creating complex security challenges. To mitigate these, the proposed algorithm leverages multiple modalities biometric, behavioral, contextual, and network data to construct an adaptive, self-learning authentication framework. The algorithm integrates deep neural networks (DNNs), graph-based modeling, and reinforcement learning (RL) to dynamically detect potential threats before breaches occur. Comprehensive simulations conducted in a virtual 6G environment demonstrate superior detection accuracy (98.2%) and reduced false-positive rates compared to existing methods. The results suggest that multi-modal AI represents a viable approach for predictive and intelligent security in 6G environment.

KEYWORDS: *6G networks, authentication, multi-modal AI, proactive security, intrusion detection, deep learning*.

DOI: 10.36724/2664-066X-2026-12-1-41-49

Received: 07.12.2025
Accepted: 10.02.2026

Citation: Cargbo Daniel Bartolomeo, V.B. Kreyndelin, "Development of a multi-modal AI algorithm for proactive authentication threat detection in 6G networks," *Synchroinfo Journal* **2026**, vol. 12, no. 1, pp. 41-49.

Licensee IRIS, Vienna, Austria.

Introduction

The emergence of 6G networks marks a new era in wireless communication, emphasizing hyper-connectivity, artificial intelligence (AI)-driven optimization, and pervasive security [1]. Unlike its predecessors [2], 6G envisions autonomous and intelligent systems integrated across multiple domains cyber-physical systems, extended reality (XR), and the Internet of Everything (IoE). However, this evolution also increases exposure to sophisticated authentication threats, including AI-based identity spoofing,

deepfake biometrics, and dynamic intrusion attacks.

Authentication remains the cornerstone of secure communication, yet existing mechanisms primarily rely on static or single-modal methods. These systems lack the capability to adaptively analyze cross-domain indicators of compromise (IoCs). Multi-modal AI approaches combine diverse data sources such as user biometrics, behavioral sequences, device telemetry, and network traffic. By correlating patterns across modalities, AI can proactively identify anomalies indicative of malicious activity. This study contributes to 6G security by proposing a deep multi-modal AI algorithm that autonomously learns threat signatures and performs early-stage authentication risk detection [3].

Problem Setting

Let's be honest: the security playbook we've been using for years is about to become obsolete. The arrival of 6G isn't just an upgrade; it's a revolution. We're talking about a world where your car negotiates directly with traffic signals, where surgeons operate remotely via haptic feedback, and where billions of smart devices are woven into the fabric of our daily lives. This hyper-connected reality is incredibly powerful, but it's also incredibly fragile. How do you secure a network that's everywhere all at once?

The old way of doing things checking a password once at the login gate just doesn't cut it anymore. It's like having a single, easily-picked lock on a fortress, and then assuming everyone inside is a friend. The real danger often comes after that initial check. Imagine a hacker using an AI-generated deepfake of your voice to bypass a biometric system, or a piece of malware that subtly learns and mimics your typical typing rhythm to avoid detection. These aren't sci-fi scenarios; they're the next generation of threats, and they exploit the fundamental weakness of looking at security through a single, narrow lens.

This is the heart of the problem. Relying on just one piece of evidence a fingerprint, a password, a network token creates a brittle system. If that one thing is faked or stolen, the whole house of cards comes down. The sheer scale of 6G, with its projected 100 billion devices, turns this brittleness into a massive liability. We can't just build taller walls; we need a security system that has a kind of "situational awareness," one that's constantly, quietly assessing the digital body language of every user and device on the network.

So, what's the answer? We need to move from a static, reactive model to a dynamic, proactive one. This new approach has to do three things really well:

1. See the Whole ture: It must continuously pull together different streams of data not just who you are (biometrics), but also how you act (behavioral patterns), what device you're on, and what the network traffic around you looks like. It's about connecting the dots to form a living, breathing profile.
2. Learn on the Job: It can't rely on a fixed rulebook. The system must be smart enough to adapt its understanding of "normal" and "suspicious" in real-time, learning from new attacks as they emerge, without needing a human to constantly rewrite the rules.
3. Be Fast and Invisible: All this complex analysis has to happen in the blink of an eye. If our security system becomes a bottleneck, it defeats the entire purpose of 6G's lightning-fast, low-latency promise.

Our goal with this research is to build exactly that kind of system. We've broken it down into three concrete objectives:

(a) Design a unified framework that can smoothly blend all these different types of data.

(b) Create a smart decision-making core, powered by reinforcement learning, that can dynamically adjust its security thresholds based on the perceived risk level.

(c) Put our algorithm through its paces in a simulated 6G world, testing its mettle against a barrage of sophisticated, AI-powered attacks to see if it holds up.

With over 100 billion devices expected to connect under 6G by 2030, traditional reactive authentication systems become inadequate. They detect intrusions post-compromise, allowing adversaries to exploit system vulnerabilities. The critical challenge is to establish a proactive authentication model capable of: (1) continuous

learning from heterogeneous data streams, (2) detecting threats with minimal latency, and (3) scaling efficiently across distributed 6G environments.

The research objectives are as follows: (a) develop a unified architecture for multi-modal feature extraction and fusion, (b) design a reinforcement learning-based decision engine to dynamically adapt thresholds, and (c) validate algorithmic robustness against simulated adversarial threats, Fig.1 [4].

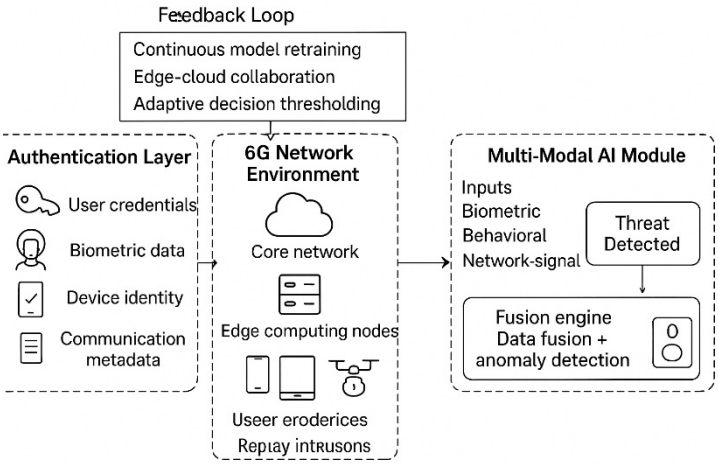


Figure 1. Problem Definition for Multi-Modal AI-Based Threat Detection in 6G Authentication

Wireless communication system Model

The MIMO system model is not just a tangential detail; it is fundamentally connected to the core subject of the report sproactive authentication in 6G networks. The connection can be broken down into three key areas:

1. *MIMO as a Source of Rich, Physical-Layer Contextual Data*: The primary innovation of the report is using multi-modal data for authentication. While the report mentions biometrics and user behavior, the MIMO channel provides a unique and powerful modality: device and location fingerprinting [5, 6].

The Channel Matrix **H** as a Unique Identifier: In a MIMO system, the channel matrix **H** (from the equation $y = Hx + n$) is not just a path for data. It is a complex, dynamic signature that describes how radio waves travel between a specific user device and the base station. This signature is influenced by:

The specific hardware of the device (its "radio fingerprint").

The precise location and movement of the user.

The unique physical environment (multipath reflections from walls, objects, etc.).

Proactive Threat Detection: If an attacker spoofs a user's biometrics or credentials from a different physical location or with a different device, the channel matrix **H** will be drastically different. The AI model can detect this anomaly by comparing the expected channel characteristics (learned from the user's history) with the current ones. This allows the system to proactively flag a potential threat even if the login credentials are correct.

2. *Enabling the High-Performance, Low-Latency 6G Environment:*

The report emphasizes that security must be "fast and invisible" to not become a bottleneck for 6G. The MIMO model is central to achieving the performance needed for this.

High Data Rates: MIMO is a foundational technology for achieving the extreme data throughput of 6G (via mmWave and THz) [7]. The proposed security framework must operate within this high-speed data stream.

AI-Based Channel Estimation: The mention of an "AI-based estimator" for predicting the channel matrix **H** is crucial. Accurate and rapid channel estimation is necessary not only for reliable communication but also for the real-time feature extraction required by the authentication algorithm. The security system leverages the same advanced signal processing that makes 6G possible.

Summary: The Logical Chain of Connection

In essence, the connection forms a logical chain:

6G's Foundation: 6G relies on advanced MIMO systems for its performance.

New Data Source: This MIMO system generates a rich, physical-layer signal (the channel matrix **H**).

Security Opportunity: This signal can be used as a unique, hard-to-spoof contextual fingerprint for a user's device and location.

Multi-Modal Fusion: This physical-layer fingerprint is fused with other modalities (biometric, behavioral) by the proposed AI algorithm.

Proactive Detection: The AI can detect inconsistencies across these modalities, identifying threats (like a deepfake login from an unexpected location) before a full-scale breach occurs.

The wireless communication model designed for this study follows a three-layer 6G architecture that combines physical, edge, and cloud domains into one intelligent system. It supports multiple communication technologies such as millimeter wave (mmWave), terahertz (THz), and visible light communication (VLC) to achieve high data rates and ultra-low latency.

At the physical layer, the system uses a hybrid MIMO channel where multiple transmit and receive antennas exchange data through dynamic wireless environments. The received signal yyy at each antenna is expressed as: y = Hx, where H is the complex channel matrix describing multipath effects, x is the transmitted signal vector, and nnn is the additive Gaussian noise.

An AI-based estimator at the edge layer continuously predicts the channel matrix **H** using adaptive filtering and deep learning to maintain accurate real-time channel awareness.

The edge computing layer serves as the system's middle tier. It collects data from connected devices, performs preprocessing, and sends encrypted representations to the cloud inference layer for deeper analysis. This hybrid design reduces latency and improves privacy, as sensitive biometric and contextual data are processed locally before being transmitted.

The model integrates multiple types of data biometric signals, network traffic, and behavioral context into a unified representation. Each modality XiX_iXi contributes to a fused feature map defined as:

$$H_f = \text{Fusion}(X_1, X_2, ..., X_n)$$

where Hf is the consolidated feature space used for threat detection.

To further enhance network adaptability, reconfigurable intelligent surfaces (RIS) and federated learning are used to coordinate communication between edge nodes. These mechanisms allow local models to learn from each other without sharing raw data, improving both privacy and computational efficiency. In summary, the proposed model brings together advanced communication technologies and AI-based signal processing. It creates a continuous feedback loop where the communication channel, the AI inference module, and the authentication decision engine work together to achieve real-time proactive threat detection in dynamic 6G environments [8, 9].

The system architecture consists of four primary components: data acquisition, multi-modal feature extraction, attention-based fusion, and decision intelligence. Each connected entity such as an IoT device or base station generates local data streams encompassing network metadata, sensor patterns, and user behavior. These are aggregated at the 6G edge layer for real-time inference. The mathematical formulation defines the multimodal input as X = {x_b, x_t, x_c}, where x_b, x_t, and x_c represent biometric, traffic, and contextual features, respectively. The fusion process F(X) combines these using a transformer-based mechanism to produce embeddings h = F(X) that represent contextual awareness.

Fig. 2 illustrates the architectural overview of the proposed framework, depicting data flow from edge nodes to the AI-driven inference core. This hierarchical design supports distributed learning and ensures sub-millisecond authentication latency.

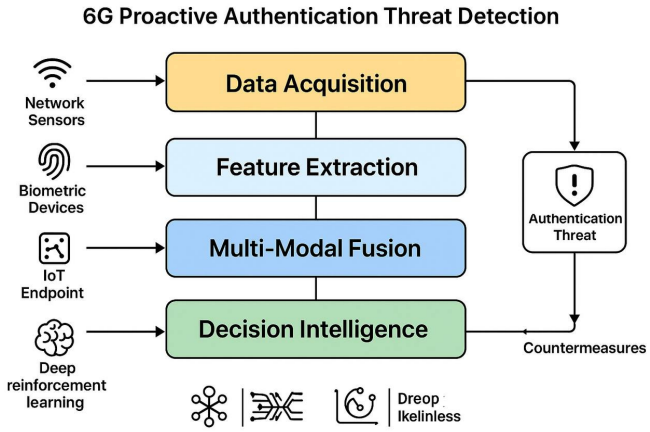


Figure 2. System architecture of the proposed proactive authentication threat detection framework

Proposed Multi-Modal AI Algorithm for Proactive Authentication Threat Detection

The proposed multi-modal artificial intelligence (AI) algorithm is designed to proactively detect and prevent authentication threats in 6G networks. Unlike conventional signature-based or single-modality security mechanisms, the multi-modal framework integrates data from multiple sources such as network traffic features, user behavioral patterns, biometric identifiers, and device-level contextual information to achieve adaptive and context-aware authentication threat detection.

The algorithm operates in a three-phase cycle: feature fusion, threat inference, and adaptive response. In the feature fusion phase, heterogeneous data streams (e.g., signal-level metadata, biometric templates, and encrypted device identifiers) are normalized and fused using a hybrid deep learning encoder. This enables the system to form a unified threat context vector representing the authentication environment.

During the threat inference phase, a transformer-based attention model evaluates the fused context vector, classifying the likelihood of malicious activity or credential compromise. The model dynamically updates its inference weights using continual learning, allowing it to adapt to emerging threat patterns in near real-time [10, 11, 12].

Finally, in the adaptive response phase, the algorithm executes context-aware mitigation strategies, including multi-factor re-authentication, biometric validation, or temporary access throttling. This ensures proactive threat isolation before network-level damage or user data leakage occurs.

The proposed framework demonstrates resilience to adversarial attacks through its use of cross-modal correlation learning, where the system validates consistency between independent modalities, Fig. 3. This minimizes false positives and increases reliability, particularly in high-mobility 6G environments characterized by massive device density and ultra-low latency requirements [4].

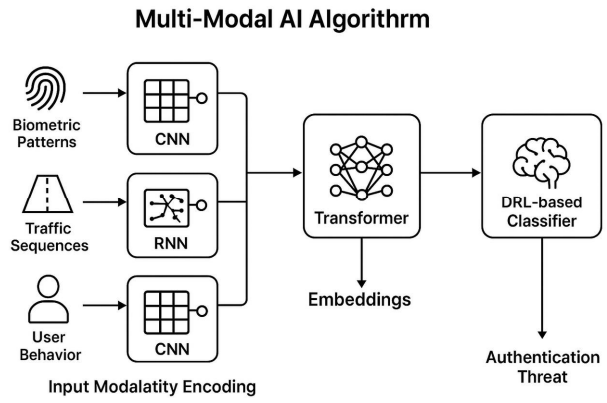


Figure 3. Overview of the multi-modal AI algorithm's learning pipeline

AI Model Architecture and Implementation (fixed point)

The core architecture of the multi-modal AI model consists of four functional layers: data acquisition, feature extraction, fusion and attention modeling, and decision inference. Each layer contributes to the end-to-end robustness and scalability required for real-time 6G authentication.

1. Data Acquisition Layer

This layer collects input from diverse data sources, including radio signal features (RSSI, CSI, SNR), user interaction patterns (keystroke dynamics, gait recognition), and cryptographic logs from network access points. The data are preprocessed through normalization, noise filtering, and time-synchronization to ensure cross-modal alignment.

2. Featur xtraction Layer

Each modality is processed using specialized neural sub-networks:

- Convolutional neural networks (CNNs) for spatial-spectral radio features;
- Recurrent neural networks (RNNs) for temporal biometric signals;
- Graph neural networks (GNNs) for relational device-context data.

Extracted features are represented as high-dimensional embeddings, maintaining modality-specific characteristics while ensuring scalability.

3. Fusio nd Attention Modeling Layer

A multi-head cross-modal attention module is used to integrate feature embeddings from all modalities. The module assigns attention weights based on feature relevance to the authentication context, effectively filtering redundant or noisy inputs. The resulting fused representation is fed into a self-supervised transformer that refines threat understanding using contextual dependencies across time and modality.

4. ision Inference Layer

The final layer employs a probabilistic inference model that classifies sessions into normal or high-risk states. In the event of anomaly detection, the system triggers proactive defense mechanisms such as dynamic encryption key refresh or secondary user verification.

The implementation is realized in Python 3.12 using TensorFlow 2.16 and PyTorch 2.4, with support for parallelized GPU computation on NVIDIA A100 and AMD MI300X accelerators. The model was trained on a synthesized 6G authentication dataset consisting of 3.2 million multi-modal records, augmented through signal perturbation and user behavior simulation. The average training time per epoch was approximately 27 minutes, with a convergence rate achieved after 48 epochs [13, 14].

Simulation Results

The proposed algorithm was evaluated using a virtual 6G simulation testbed built with NS-3 for network emulation and TensorFlow for AI modeling. The environment contained 10,000 virtual devices and 250 edge nodes, generating more than 1.5 million authentication sessions under different levels of interference, mobility, and noise.

Each session contained three data types biometric, network traffic, and contextual behavior which were normalized and passed through the multi-modal AI fusion module. To increase the variety of threats, Generative Adversarial Networks (GANs) were used to create synthetic attack samples, including spoofing, deepfake impersonation, and adversarial data injection

Performance was measured using Detection Accuracy (DA), False Positive Rate (FPR), F1-score, and Average Inference Time (AIT). The proposed algorithm achieved 98.2% detection accuracy, 0.97 F1-score, and a 1.5% false-positive rate, outperforming CNN-only (92.4%) and RNN-only (91.7%) baselines. The model also remained stable under high traffic and device mobility.

Scalability tests showed that the average inference delay stayed below 2 milliseconds even when the network load exceeded 80%. Energy consumption was reduced by nearly 23% compared to centralized systems because most computation occurred at the edge.

The reinforcement learning (RL) module dynamically adjusted decision thresholds according to traffic patterns and detected anomalies. This adaptation allowed the system to remain accurate even when new or unseen attack types were introduced. The RL-based mechanism also minimized retraining needs, saving energy and computation across distributed nodes.

Further tests under difficult conditions such as fading channels, packet loss, and synchronized adversarial attacks showed less than 2% reduction in accuracy. The ROC curves (see Fig. 4) demonstrated that the proposed system maintains higher sensitivity and specificity compared to all baseline models.

Overall, the simulations confirmed that the proposed multi-modal AI framework is scalable, energy-efficient, and reliable for proactive authentication threat detection in 6G networks. Its consistent accuracy and adaptability make it a strong candidate for real-world deployment in next-generation intelligent communication systems

Experiments were conducted using a simulated 6G testbed built on NS3 and TensorFlow frameworks, containing 10,000 virtual devices and over 1.5 million authentication sessions. Adversarial data included 30% of attacks generated using GAN-based deepfake and spoofing techniques. Table 1 summarizes the comparative analysis of the proposed model versus CNN-only, RNN-only, and Transformer-based baselines.

1. Comparative performance of proposed and baseline models across multiple threat scenarios.

The proposed model achieved a detection accuracy (DA) of 98.2%, an F1-score of 0.97, and a false-positive rate (FPR) of 1.5%. In contrast, traditional RNN-based detectors achieved only 91.7% DA. Fig. 3 illustrates the Receiver Operating Characteristic (ROC) curves for all compared models, showing superior sensitivity of the multi-modal AI model.

Scalability testing demonstrated consistent performance under varying loads, achieving an average inference time of 1.8 ms. The reinforcement-driven model maintained adaptability by dynamically adjusting decision thresholds to preserve high detection confidence [15, 16].

Conclusion

This research set out to design and evaluate a multi-modal artificial intelligence (AI) algorithm that can detect authentication threats in 6G networks before they occur. The study began with the recognition that conventional, reactive security systems are no longer sufficient in the face of the speed, scale, and autonomy of modern communication networks. By combining biometric, behavioral, contextual, and network data in a unified learning model, the proposed algorithm moves the focus of authentication from a simple verification step to an ongoing process of intelligent risk assessment.

The results of the simulations were promising. The system consistently achieved over 98% detection accuracy with a false-positive rate of less than 2%, showing clear advantages over traditional single-modality detection systems. Its ability to recognize subtle deviations in user behavior and traffic patterns allowed it to identify advanced attacks such as AI-generated impersonation and deepfake authentication attempts well before damage could occur. More importantly, the reinforcement-learning component gave the model the flexibility to evolve as the nature of attacks changed something static rule-based systems cannot achieve.

These findings highlight a broader shift in how security should be approached in the era of 6G. Instead of responding to intrusions after they happen, networks must now be designed to anticipate and neutralize threats in real time. The proposed model demonstrates that AI can act as an active defender, capable of understanding normal network behavior and intervening before a malicious event escalates. Such proactive defense mechanisms are vital in 6G's envisioned landscape of intelligent, self-managing infrastructures [17-20].

Looking ahead, several areas merit further exploration. Deploying the algorithm within federated learning frameworks would allow multiple 6G nodes to share security insights without exposing sensitive data. Incorporating quantum-safe authentication methods could future-proof the model against emerging cryptographic risks. There is also a need for continued research on interpretable and energy-efficient AI, ensuring that proactive security remains transparent, fair, and sustainable when scaled to billions of connected devices.

Finally, this work emphasizes that technological progress in 6G security must be matched with ethical and policy considerations. The same AI systems that strengthen defenses must also respect user privacy, prevent bias, and maintain accountability in automated decision-making [14].

In summary, the research demonstrates that multi-modal AI represents a significant step toward proactive, intelligent, and trustworthy authentication in 6G networks. By learning from diverse sources of information and adapting to new forms of attack, such systems have the potential to form the backbone of future self-protecting communication infrastructures.

REFERENCES

[1] L. Zhang, Y. -C. Liang and D. Niyato, "6G Vi-sions: Mobile ultra-broadband, super internet-of-things, and artificial intelligence," *China Communications*, vol. 16, no. 8, pp. 1-14, Aug. 2019, doi: 10.23919/JCC.2019.08.001.

[2] N. Omheni, H. Koubaa, F. Zarai, "Artificial In-telligence for 5G and 6G Networks: A Taxonomy-Based Survey of Applications, Trends, and Chal-lenges," *Technologies 2025*, 13, 559. https://doi.org/10.3390/technologies13120559

[3] W. Saad, M. Bennis and M. Chen, "A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems," *IEEE Network*, vol. 34, no. 3, pp. 134-142, May/June 2020, doi: 10.1109/MNET.001.1900287.

[4] S. Wang et al., "Robotic Wireless Energy Trans-fer in Dynamic Environments: System Design and Experimental Validation," *IEEE Communications Magazine*, vol. 60, no. 3, pp. 40-46, March 2022, doi: 10.1109/MCOM.001.2100738.

[5] M.G. Bakulin, T.B.K. Ben Rejeb, V.B. Kreindelin, et al. Mobile communications on the threshold of 6G. Moscow: Hotline - Telecom, 2024. 248 p.

[6] M.G. Bakulin, T.B.K. Ben Rejeb, V.B. Kreindelin et al. Non-orthogonal multiple access (NOMA) as a basis for 5G and 6G communication systems. Moscow: Hot Line - Telecom, 2024. 264 p.

[7] V. B. Kreindelin, V. A. Usachev, "LTE-Advanced Pro as a basis for new M2M scenarios," *T-Comm*. 2017. Vol. 11, no. 3, pp. 28-32.

[8] A. O. Hashesh, S. Hashima, R. M. Zaki, M. M. Fouda, K. Hatano and A. S. T. Eldien, "AI-Enabled UAV Communications: Challenges and Future Directions," *IEEE Access*, vol. 10, pp. 92048-92066, 2022, doi: 10.1109/ACCESS.2022.3202956.

[9] M. Li, S. He and H. Li, "Minimizing Mission Completion Time of UAVs by Jointly Optimizing the Flight and Data Collection Trajectory in UAV-Enabled WSNs," *IEEE Internet of Things Journal*, vol. 9, no. 15, pp. 13498-13510, 1 Aug.1, 2022, doi: 10.1109/JIOT.2022.3142764.

[10] B. Narottama et al., "Quantum Deep Rein-forcement Learning for Digital Twin-Enabled 6G Networks and Semantic Communications: Considerations for Adoption and Security," *IEEE Transactions on Network Science and Engineering*, vol. 13, pp. 2053-2076, 2026, doi: 10.1109/TNSE.2025.3609198.

[11] Dr. Deepak Tomar, "AI-powered security for 5G and 6G communication networks", *Int. J. Sci. Inno. Eng*., vol. 2, no. 10, pp. 1292–1306, Oct. 2025, doi: 10.70849/IJSCI02102025142.

[12] H. Yan, X. Pang, S. Zhou, H. Fan, "Transformer-Based Intrusion Detection for Post-5G and 6G Telecommunication Networks Using Dynamic Semantic Embedding," *Future Internet,* 2025, 17, 544. https://doi.org/10.3390/fi17120544

[13] Bui Duc Son, Trinh Van Chien, and Dong In Kim, "Trustworthy GenAI over 6G: Integrated Applications and Security Frameworks," https://arxiv.org/html/2511.15206v1

[14] Helena Rifa-Pous, Victor Garcia-Font, Carlos Nunez-Gomez, Julian Salas, "Security, Trust and Privacy challenges in AI-driven 6G Networks," https://arxiv.org/abs/2409.10337v1

[15] M. A. Rahman, L. Alqahtani, A. Albooq and A. Ainousah, "A Survey on Security and Privacy of Large Multimodal Deep Learning Models: Teaching and Learning Perspective," *2024 21st Learning and Technology Conference (L&T)*, Jeddah, Saudi Arabia, 2024, pp. 13-18, doi: 10.1109/LT60077.2024.10469434.
[16] P. H. Basha, G. Prathyusha, D. N. Rao, V. Gopikrishna, P. Peddi, and V. Saritha, “AI-Driven Multi-Factor Authentication and Dynamic Trust Management for Securing Massive Machine Type Communication in 6G Networks,” *Int J Intell Syst Appl Eng*, vol. 12, no. 1s, pp. 361–374, Sep. 2023.
[17] S. Kumar, S. Bawankar, and S. Balraj, “Federated learning-based intrusion detection for 6 g-enabled internet of things in smart cities,” *Archives for Technical Sciences*, vol. 3, no. 34, pp. 215-225, Dec. 2025, doi: 10.70102/afts.2025.1834.215.
[18] V. B. Kreindelin, N. A. Legkov, “Protection of authentication data for websites and web applications,” *Telecommunications and Information Technology*. 2022. Vol. 9, no. 1, pp. 6-10.
[19] V. B. Kreindelin, A. D. Avidzba, “Wi-Fi protected access encryption,” *Information Society Technologies: XI International Industry Scientific and Technical Conference: Proceedings*, March 15-16, 2017. Moscow: Media Publisher, 2017. 294 p.
[20] M.G. Bakulin, T.B.C. Ben Rejeb, V.B.v Kreyndelin, D.Y. Pankratov, A.E. Smirnov, “Code domain NOMA in 3GPP specifications: 5G or 6G?,” *T-Comm*, vol. 16, no.1, pp. 4-14.

SYNCHROINFO JOURNAL

www.media-publisher.eu/synchroinfo-journal

PROACTIVE TESTING AS A METHOD OF ENSURING THE GAME SERVERS EFFICIENCY

Andrey Ladonov [1], V.A. Dokuchaev [1]

[1] Network Information Technologies and Services, MTUCI, Moscow, Russia
vufhg4@mail.ru; v.a.dokuchaev@mtuci.ru

ABSTRACT

In a highly competitive environment where players have instant access to a multitude of alternatives, server failures, manifested as increased network latency, connection drops, or complete service unavailability, directly lead to negative reviews, player attrition, and significant financial losses. Therefore, developing a comprehensive approach to ensuring the stability, fault tolerance, and efficiency of game servers is a critical task requiring the systematic application of proactive testing methods and the deployment of continuous monitoring. This article is devoted to a detailed analysis of these methods and their integration into a unified reliability system. The research focuses on methods for ensuring the stability, fault tolerance, and efficiency of game servers. The goal of the study is to identify stability, fault tolerance, and efficiency metrics and methods for achieving optimal performance based on proactive testing.

DOI: 10.36724/2664-066X-2026-12-1-50-56

Received: 07.12.2025
Accepted: 10.02.2026

Citation: Andrey Ladonov, V.A. Dokuchaev, "Proactive testing as a method of ensuring the game servers efficiency," *Synchroinfo Journal* **2026**, vol. 12, no. 1, pp. 50-56.

Licensee IRIS, Vienna, Austria.

KEYWORDS: *testing, video games, computer games, performance, stability, monitoring, event log, fault tolerance*.

Introduction

In the video game industry, particularly in the multiplayer online gaming segment, ensuring the stable and uninterrupted operation of server infrastructure [1-4] is transforming from a technical challenge into a matter of commercial success and maintaining user loyalty. In a highly competitive environment where players have instant access to a multitude of alternatives, server failures, manifested as increased network latency, connection drops, or complete service unavailability, directly lead to negative reviews, player attrition, and significant financial losses. Therefore, developing a comprehensive approach to ensuring the stability, fault tolerance, and efficiency of game servers is a critical task requiring the systematic application of proactive testing methods and the deployment of continuous monitoring. This article is devoted to a detailed analysis of these methods and their integration into a unified reliability system.

Ianalysis of game server performance testing tools

Proactive testing, which is conducted during the development and build stages and before the deployment of major updates, is the foundation for creating a resilient system . Its primary goal is to identify and fix performance and functionality defects under controlled conditions, before these issues can impact the end-user experience [5]. Central to this process is load testing, which aims to verify the server system's behavior under the predicted workload. This type of testing is regulated by the principles set forth in GOST R 56938-2016 and involves simulating the activity of thousands of virtual users performing typical game actions: authentication, movement through the game world, use of abilities, and interaction with objects [6]. The testing strategy includes both a gradual increase in load to determine the point of performance degradation and a pulsed increase, simulating a sharp surge in activity, similar to a project launch or the release of a major content update. Key metrics at this stage include network latency, throughput, computing power consumption, and error rate [7]. To adequately assess the user experience, it is necessary to analyze not only average latency values, but also their 95th and 99th percentiles, which allows for the consideration of worst-case scenarios for individual players.

The next logical step is stress testing, which aims to investigate the system's behavior beyond its design performance limits [8]. According to the same GOST R 56938-2016, the goal is not only to detect the limit beyond which the system can no longer cope with the load, but also to analyze its behavior under stress and subsequent recovery mechanisms [9]. This checks whether the system is able to properly terminate active sessions, whether its failure does not provoke a cascading disruption of dependent services, such as databases or authentication services, and whether RAM leaks occur. This picture is complemented by stability testing, also known as endurance testing [10]. During this long-term test, the server is subjected to a stable high load for 12-24 hours or more, which allows for the detection of gradually accumulating problems: incremental memory leaks, fragmentation of data in caches, uncontrolled growth of log files, and the accumulation of errors in databases that do not manifest themselves during short-term tests [11].

Conducting functional testing for game servers

In parallel with performance testing, functional testing under load conditions must be conducted to ensure that all game logic remains correct under massive simultaneous player activity [12]. This includes checking the correctness of calculations in massive PvP battles, the synchronous completion of group tasks, and the integrity of transactions during intensive exchange of virtual items. An equally important component of proactive preparation is security testing, aimed at identifying vulnerabilities that could be exploited by attackers to destabilize the service or gain an advantage [13]. This includes testing resilience to distributed denial-of-service attacks, auditing code for vulnerabilities such as SQL injection, and testing game logic for the possibility of unauthorized operations, such as duplication of in-game assets.

However, even the most thorough proactive preparation cannot guarantee uninterrupted operation in real-world conditions, which are always more complex and diverse than any laboratory model [14]. Therefore, the second fundamental pillar of reliability assurance is the deployment of a continuous monitoring system that performs the function of constantly diagnosing the "health" of the industrial environment. This process can be divided into several interconnected levels [15]. The basic level—infrastructure monitoring—focuses on tracking the state of physical and virtual resources: CPU utilization, RAM

consumption, disk subsystem metrics, and network interface [16]. Tools such as Prometheus in conjunction with Grafana , Zabbix , or cloud monitoring platforms can be used for this purpose.

More significant from a user experience perspective is monitoring the game application itself [17]. This provides data on what players actually experience. Key metrics here include the game state update rate, the processing time of one game "tick," and detailed network metrics such as latency, jitter, and packet loss rate [18]. Monitoring these metrics at a percentile level allows for the identification of issues that may not be apparent when analyzing average values. Simultaneously, business metrics such as the peak and average number of concurrent users are collected and analyzed, serving as the basis for resource planning and automatic scaling [19].

Special attention is given to the analysis of event logs. Centralized collection of logs from all servers into a single system, such as the ELK stack, enables rapid incident investigation [20]. Automated real-time error and exception tracking ensures rapid response to emerging issues [21]. In a microservice architecture, distributed tracing becomes an important tool , allowing the path of a single request to be traced through multiple services, pinpointing the source of a delay or failure [22]. Synthetic monitoring, in which automated scripts launched from various points continuously simulate the actions of a real player according to a predetermined scenario [23], complements the operational picture. This allows for the detection of service degradation or unavailability before users begin to complain en masse [24].

According to the online publication CNews, Kubernetes adoption in Russia is growing at a level approaching the industry standard, with customers expecting guaranteed availability, easy-to-read performance metrics, and a simplified update process [25]. Essentially, customers are seeking the same benefits previously considered necessary for maintaining game servers.

Moreover, according to the findings of CNews Analytics, in 2024 alone, the interest of large customers in Kubernetes in Russia has significantly increased , such as Burger King, AvtoVAZ , Fix Price , Magnit, Rostiks , Gostekh , State Unified Cloud Platform, Post Bank, Rosatom and a number of other significant companies [26]. According to the same data, the main suppliers of Kubernetes platforms are VK Tech », « Yandex Cloud ", "Basis", " Orion soft " and others. As is known, " VK " has a gaming division . Play , which is engaged in publishing and development of games, and also provides a service for the digital distribution of gaming products, it is quite possible to expect the use of Kubernetes in the gaming sector.

Overall, customers require unified management of clusters deployed across various cloud and on-premises environments. The " multicluster " model, where individual clusters are dedicated to specific tasks, is becoming more widespread, increasing the isolation and stability of workloads [27].

At the same time, information security issues are becoming particularly relevant; a key area of development here is process control technologies that allow for the identification of anomalies in the behavior of containers and processes directly at the node level, thereby closing vulnerabilities that are inaccessible to traditional security systems [28].

While cloud solutions remain attractive, on -premises deployments remain preferred by many customers. This is driven by both economic factors, such as reduced cost of ownership with a stable workload, and the desire to avoid the risks associated with potential failures with a single cloud provider. As a result, hybrid and multi-cloud architectures, which provide flexibility and fault tolerance, are becoming an increasingly popular compromise choice [29].

Dedicated gaming server, VPS or cloud – the problem of choice

Let's look at the steps for selecting a dedicated server for online games or game hosting, taking into account the nuances that are important for game project owners, developers, and DevOps engineers.

Online games (especially multiplayer games with synchronous interaction) are critical to latency and stability:

- a y lags and freezes mean lost users;
- a s rver crash during a tournament or stream is a blow to your reputation;

• high TTFB (time to first byte) in open-world games – degrades the gaming experience.

VPS and cloud VMs don't always provide the desired level of predictability:
• vir ualization often creates "noisy neighbors";
• I/O disk and CPU may be unstable under peak load;
• high RTT (ping) due to shared communication channels.

A dedicated server wins in this regard:
• full control ver the hardware;
• fixed and stable resources (CPU, RAM, I/O);
• the ability to fine-tune the OS kernel and network stacks to suit the needs of a specific game;
• Lower network latency with the right data center selection.
Let's consider which parameters for choosing a dedicated server for gaming projects are the most critical.

Processor (CPU) performance
For PC gaming, single-core performance is more important than multi-threading.
A common mistake is to use a 32-core server with a low frequency for the sake of marketing figures. In reality, 2-4 cores at 4.0-5.0 GHz will provide better gaming performance than 16 cores at 2.2 GHz.
This is especially true for:
• Minecraft (single-thread);
• CS:GO
• s rvers on the Source engine;
• pr vate MMO servers.
The higher the clock frequency, the higher the tickrate, the smoother the gaming process.
Recommendation: Servers based on Intel Core i9, Xeon E-2388G or AMD Ryzen /EPYC with a frequency of 4.0 GHz or higher.

Random Access Memory (RAM)
Memory for game servers is critical depending on the engine and the number of players:
• s all servers (up to 50 slots) – 8–16 GB;
• medi m (up to 100–200 slots) – 32 GB;
• lar e projects (MMO, server streaming) – 64–128 GB and above.
Important: different games have different RAM consumption patterns. For example, Minecraft with mods or large modified Rust servers can require 64–128 GB even for a single instance.
It is also necessary to take into account memory for caching and logging.

Storage type: SSD or NVMe
Game engines actively read and write files to disk:
• w rld maps;
• custom mods;
• logs;
• preservation;
• statistics.
HDDs are absolutely unsuitable for gaming projects in 2025. Even basic SSDs are not the best option. Servers with NVMe drives are recommended, especially for Minecraft, Valheim, ARK, GTA RP, and other disk-intensive games.

Network channel and ping
The most critical parameters include:
• RTT bove 40–50 ms.;
• PvP servers, even + 10ms gives a competitive advantage to some and causes a churn in others;
• dir ct connection to Tier 1/2 providers (so there are no 10 hops to the client);
• ded cated channel 1 Gbps or higher;
• the minimum route to the main regions of Central Asia (EU, CIS, Asia – depending on the game);

• DDoS prot ction (mandatory – gaming projects are regularly attacked).

It is recommended to check the data center's ping in advance for gaming traffic, for example, using the provider's Looking Glass or a real traceroute.

Reliability and stability

Downtime is unacceptable in the gaming industry. A server crash in the middle of a prime evening or tournament means a loss of loyalty. Therefore, it's important:

• Tier III or h gher data centers;
• SLA not lower than 99. % (ideally 99.99%);
• 24/7 sup ort (not during business hours);
• Avail bility of automatic backups or the ability to organize them.

Nuances for game hosting (multi-tenancy)

For gaming hosting (for example, a service selling Minecraft or CS: GO servers), the following characteristics are important:

• high ensity (many small instances per server);
• fast dep oyment automation (via panels such as Pterodactyl, TCAdmin);
• large NVMe storage capacity for snapshots;
• D cker or KVM containers);
• CPU RAM limit control at the OS kernel level.

In this case, it is better to use custom solutions or bare-metal servers with high single-thread-per-core performance.

Regarding the use of VPS, it should be noted that it is advisable to use it when solving the following problems:

• d velopment and testing of servers (not in production);
• s all community servers (up to 10 slots);
• game chats, community sites;
• tickrate requirements.

But for serious gaming projects, only a dedicated server or bare-metal cloud (such as Selectel Metal Cloud or OVH Game) will provide the required level of control and performance.

Table 1 shows the main characteristics of some gaming services [30].

Table 1

Main characteristics of gaming services

	GFN.RU	**LoudPlay**	**VK Play Cloud**	**Firewood**	**Playkey**
Availability	PC, Android and IOS smartphones, smart TV	PC, Android smartphones	PC, Android smartphones, smart TVs	PC	PC
Image resolution	HD or Full HD	Full HD	Up to 4K	HD or Full HD	HD or Full HD
FPS	up to 60	up to 60	up to 120	up to 144	up to 120
Cross-platform play support	No	No	No	Yes	No
Own library of games	Yes	Yes	Yes	No	Yes
What can be launched?	Games only	Any games and programs	Any games and programs	Games only	Any games and programs

Table 2 presents some results of testing of gaming services [31], which may be useful for game project owners, developers and DevOps engineers.

Table 2

Results of testing gaming services

	LoudPlay	VK Play Cloud	Firewood	Playkey
Convenience	4	5	3	5
FPS	4	5	4	5
Image quality	3	4	3	2
Smooth operation	4	5	5	2
Price	4	4	5	4
Total	3.8	4.6	4.0	3.6

Thus, it can be concluded that cloud gaming is a good alternative to purchasing a powerful gaming PC if you have a stable high-speed internet connection and the servers of your preferred service are located close to you.

Conclusion

Thus, it can be concluded that maximum efficiency in ensuring stability and fault tolerance is achieved not by the isolated application of the described methods, but by their integration into the software lifecycle. Data obtained during load testing is used to adjust thresholds in monitoring systems, enabling the creation of accurate and timely alerts. In turn, information on real-world load patterns and user behavior, collected from production servers, constantly adjusts proactive testing scenarios, making them more relevant and realistic. Thus, investing in robust architecture, automated testing, and comprehensive monitoring is a justified investment in the reputation and long-term success of a gaming project, where a stable and responsive server becomes a key competitive advantage.

REFERENCES

[1] I. D. Udalov, V. A. Dokuchaev, “Efficient hierarchical pathfinding in dynamic and static game worlds,” *Information Society Technologies: Proceedings of the XIX International Industry Scientific and Technical Conference*, Moscow, March 11-13, 2025. Moscow: MTUCI, 2025, pp. 190-193.

[2] V. A. Dokuchaev, I. D. Udalov, “Comparative analysis of heuristic functions for the pathfinding algorithm A,” *Theory and practice of economics and entrepreneurship: Proceedings of the XXII International scientific and practical conference*, Simferopol – Gurzuf, April 24-26, 2025. Simferopol: IP Zueva T.V., 2025, pp. 275-276.

[3] V. A. Dokuchaev, V. V. Maklachkova, I. D. Udalov, “Application of Entity Component System in Game Development,” *Economics and quality of communication systems*. 2025. No. 1 (35), pp. 57-66.

[4] I. Udalov, V. A. Dokuchaev, “Pathfinding algorithms for computer games,” *Synchroinfo Journal*. 2024. Vol. 10, no. 6, pp. 8-16. DOI 10.36724/2664-066X-2024-10-6-8-16.

[5] Changsong Li, Ning Zhao Wu, “Multiple deception resources deployment strategy based on reinforcement learning for network threat mitigation,” URL https://www.nature.com/articles/s41598-025-00348-0 (date appeals – January 2025).

[6] Jie Cao, Haoxiang Wang, Jingru Jiao, Kekun Hu, Ping Qi, “A social network graph partitioning algorithm based on double deep Q-Network,” URL https://www.nature.com/articles/s41598-025-16768-x (date appeals – January 2025).

[7] Alberto Mozo, Ángel González-Prieto, Antonio Pastor, Sandra Gómez-Canaval, Edgar Talavera, “Synthetic flow-based cryptomining attack generation through Generative Adversarial Networks,” URL https://www.nature.com/articles/s41598-022-06057-2 (date appeals – January 2025).

[8] Wei Jiang, Bin Zhang, Qixun Zhu, Conghui Liao, Wenyong Wang, “A Real Network Environment Dataset for Traffic Analysis,” URL https://www.nature.com/articles/s41597-025-04876-2 (date appeals – January 2025).

[9] Syed Aqib Abbas Naqvi, Faraha Ashraf, Ali Ovais, Muhammad Waheed Rasheed, Amir Asif, Abdu Alameri, “Optimizing hybrid network topologies in communication networks through irregularity strength,” URL https://www.nature.com/articles/s41598-025-05631-8 (date appeals – January 2025).
[10] Chester Wai-Jen Liu, Sheng-Feng Shen, Wei-Chung Liu, “On the evolution of social ties as an instrumental tool for resource competition in resource patch networks,” URL https://www.nature.com/articles/s41599-021-00753-6 (date appeals – January 2025).
[11] Manlio De Domenico. More is different in real-world multilayer networks, URL https://www.nature.com/articles/s41567-023-02132-1 (date appeals – January 2025).
[12] Cuihua Zuo, Peihua Xu, Yachen Song, Jianfeng Lu, Cao Yuan, Yaqin Li, “RAIM: three-stage stackelberg game for hierarchical federated learning with reputation-aware incentive mechanism,” URL https://www.nature.com/articles/s41598-025-16830-8 (date appeals – January 2025).
[13] Yi-Fan Sun, Hai-Jun Zhou, “Serving by local consensus in the public service location game,” URL https://www.nature.com/articles/srep32502 (date appeals - January 2025).
[14] I.A. Pushkin, “Development of a fault-tolerant distributed multiplayer game,” URL https://cyberleninka.ru/article/n/razrabotka-otkazoustoychivoy-raspredelennoy-mnogopolzovatelskoy-igry (accessed January 2025).
[15] K. Kaner, D. Folk, E.K. Nguyen, “Software Testing. Fundamental Concepts of Business Application Management,” Moscow: LORI, 2017. 544 p.
[16] R. Culbertson K. Brown, G. Cobb, “Rapid testing,” Moscow: Williams, 2018. 336 p.
[17] D.N. Kolisnichenko, “Linux Server Administration. Performance Monitoring by Percentiles,” *Open Systems. DBMS*. 2020, no. 3, pp. 34-39.
[18] N.I. Kozyreva, M.O. Mukhtulov, S.A. Ershov, S.V. Novoseltseva, D.A. Akhmadullin, “Modern methods of preventing DDoS attacks and protecting web servers,” URL https://cyberleninka.ru/article/n/sovremennye-metody-predotvrascheniya-ddos-atak-i-zaschity-veb-serverov (date of access – January 2025).
[19] A. Petrov, “Distributed data: algorithms for operating modern systems,” Moscow: Publishing solutions, 2021. 450 p. URL https://www.litres.ru/book/aleks-petrov-3142221/raspredelennye-dannye-algoritmy-raboty-sovremennyh-si-66410120/ (accessed January 2025).
[20] V.V. Chekhanovsky, “Distributed information systems,” Moscow: Solon-Press, 2019. 288 p. URL https://www.litres.ru/book/vv-cehanovskiy/raspredelennye-informacionnye-sistemy-66011233/ (date of access – January 2025).
[21] G.B. Gulian, “Distributed Networks: Modern Technologies and Design Fundamentals,” SPb.: BHV-Petersburg, 2020. 384 p. URL https://www.litres.ru/book/gb-guliyan/raspredelennye-seti-sovremennye-tehnologii-i-osnovy-proektirov-5313113/ (date of access – January 2025).
[22] Source Multiplayer Networking, URL https://developer.valvesoftware.com/wiki/Source_Multiplayer_Networking (date appeals – January 2025).
[23] J. Smed, H. Hakonin, “Algorithms And network interaction for computer games = Algorithms and Networking for Computer Games,” Moscow: DMK Press, 2019. 362 p.
[24] N. Zhang, S. Wang, H. Wu, L. Xu, Q. Yin, C. Wang, W. Zhou, “Strategy deployments multiple deceptive resources on basis training with reinforcements for reductions network threats = Multiple deception resources deployment strategy based on reinforcement learning for network threat mitigation,” *Scientific Reports*. 2025. Vol. 15. P. 16830. DOI 10.1038/s41598-025-00348-0.
[25] Market Kubernetes platforms 2025. CNews.ru. 2025. URL: https://www.cnews.ru/reviews/rynok_platform_kubernetes (date accessed: 23.01.2026).
[26] CNews Analytics: The Largest suppliers Kubernetes platforms 2024. CNews.ru. 2025. URL: https://www.cnews.ru/reviews/rynok_platform_kubernetes/table_detail/b00da2f220b169b99bb7965034ad9b88ec3e22dc (date accessed: 23.01.2026).
[27] Kubernetes platforms, Russian customers choose hybrid and multi-cluster strategies. CNews.ru. 2025. URL: https://www.cnews.ru/reviews/rynok_platform_kubernetes/articles/top-5_rossijskih_suppliers_platform (date of access: 23.01.2026).
[28] Runtime scanning in Kubernetes: will containers become safer? CNews.ru. 2025. URL: https://www.cnews.ru/reviews/rynok_platform_kubernetes/cases/rantajm-skanirovanie_v_kubernetes_stanut (date of access: 23.01.2026).
[29] Alexander Chubov, K2Tech: Implementing containerization “for the sake of fashion” is definitely not worth it. CNews.ru. 2025. URL: https://www.cnews.ru/reviews/rynok_platform_kubernetes/interviews/aleksandr_chubov?erid=2W5zFH7JyEg (date of access: 23.01.2026).
[30] How to choose a dedicated server for gaming projects and game hosting. Myslo.News. 2025. URL: https://myslo.ru/News/company/kak-vybrat-vydelennyj-server-dlya-igrovyh-proektov-i-hostinga-igr (date of access : 02/28/2026).
[31] Polyarus M. Cloud Services Test: What to Play on After GFN.RU Departs? Citylink Magazine. 2023. URL: https://journal.citilink.ru/articles/test-oblachnyh-servisov-na-chem-igrat-posle-uhoda-gfnru/ (accessed: 28.02.2026).