https://doi.org/10.33271/nvngu/2026-2/141

V. V. Hnatushenko*,
orcid.org/0000-0003-3140-3788,
I. S. Laktionov,
orcid.org/0000-0001-7857-6382,
I. M. Udovyk,
orcid.org/0000-0002-5190-841X

Dnipro University of Technology, Dnipro, Ukraine
* Corresponding author e-mail: Hnatushenko.V.V@nmu.one

SOFTWARE-BASED EVALUATION OF PSEUDORANDOM FREQUENCY-HOPPING FOR WIRELESS INFOCOMMUNICATION CYBERSECURITY

Purpose. Improving the efficiency of mobile and satellite system design by developing and validating a computer model that allows objective comparison of different approaches to implementing frequency-hopping spread spectrum (FHSS).

Methodology. Computer-experiment methods in Python were used to generate a complex I/Q signal with oversampling and phase fluctuations. Three data transmission modes were implemented in the software: without FHSS, random FHSS, and FHSS based on a linear feedback shift register (LFSR). Selective narrowband jamming and ML-based interception attacks were simulated. The effectiveness of the algorithms was evaluated using the following metrics: BER, EVM, and SNR_{out}. Graphical interpretations included time and spectral dependencies, constellation diagrams, and a confusion matrix.

Findings. A computer model was implemented to evaluate the effectiveness and suitability of FHSS algorithms for cyber protection of mobile and satellite communications. It was established that the LFSR FHSS provided the best indicators for the set of metrics. In FHSS modes, energy dispersion in frequency and time is observed, which reduces the probability of affected spectral regions and increases the noise immunity of data transmission. The output signal-to-noise ratio for these modes under selective jamming conditions is satisfactory. The need for further research into the development of adaptive FHSS approaches and spectral-feature masking mechanisms has been substantiated.

Originality. The patterns of influence of FHSS algorithms on indicators of interference immunity and data interception at the physical level of wireless systems were determined. Approaches to a comprehensive comparative assessment of the effectiveness of FHSS algorithms under additive noise, jamming, and intelligent interception were developed.

Practical value. The developed computer model is suitable for comparative analysis of FHSS algorithms in wireless systems under conditions of noise, jamming and interception. The proposed model can be used to select rational FHSS schemes during the design of cyber-secure mobile and satellite systems.

Keywords: *frequency hopping, algorithm, jamming, interception, infocommunication system, computer model*

Introduction. Modern infocommunication systems, particularly those based on mobile and satellite technologies, play a crucial role in ensuring the exchange of data and information for both civilian and special purposes. The wide variety of their applications is accompanied by an increase in threats to the operation of wireless communication channels in conditions of active electronic warfare. Unlike wired networks, wireless channels are inherently open, making them significantly vulnerable to interference.

Up-to-date statistics from open sources and analytical reports from specialised international organisations in the fields of infocommunications and cybersecurity indicate a rapid increase in incidents aimed at destabilising wireless communication systems [1, 2]. Based on the summarised information, it can be concluded that a significant part of satellite and mobile communication channel failures in critical operating scenarios are caused by targeted physical interference [3, 4]. The most common cyber threats that lead to negative consequences include jamming attacks aimed at blocking or significantly degrading communication quality, passive interception of signals to obtain confidential information, and detection and direction finding of signal sources.

© Hnatushenko V. V., Laktionov I. S., Udovyk I. M., 2026

At the same time, there is a tendency towards increasing algorithmic complexity and the adaptability and variability of radio-electronic influence means. This allows for quick adjustment of attack parameters to the characteristics of the communication channel. Such an effect reduces the effectiveness of classical cyber defence approaches based on fixed frequency ranges and static transmission modes. Therefore, there is an urgent need to develop methods and means for cyber protection of wireless channels, focused on dynamically changing signal parameters and increasing their secrecy [5].

In this context, the physical layer of wireless information and communication systems draws particular attention as one of the most critical layers in wireless technologies [6, 7]. At this level, the time, amplitude, spectral and energy characteristics of the signal are formed. They determine its interference immunity, visibility, and ability to counter electronic warfare measures. Thus, effective protection of wireless channels is impossible without the use of specialised mechanisms designed to complicate the detection, interception and jamming of signals at the physical layer.

Considering the current trends in protecting the physical layer of mobile and satellite communications, the following can be noted. One of the most effective approaches to improving the resistance of wireless communications to interference and attacks is the use of frequency-hop-

ping spread spectrum (FHSS) algorithms [8, 9]. This is due to FHSS logic, which is physically implemented in the corresponding devices and dynamically changes the signal transmission frequency according to a specific pseudo-random sequence known only to legitimate communication participants. FHSS occurs at a fixed or variable rate and can cover a wide frequency range.

Therefore, given the increasing intensity, adaptability and complexity of radio-electronic interference with wireless systems, there is a need to rethink the role of the physical layer in the overall architecture of information security. The use of cryptographic mechanisms alone to protect the content of transmitted data does not provide sufficient resilience. This is due to conditions where the fact of signal transmission can be detected, suppressed, or used for further attacks. In this context, research on the development and implementation of FHSS algorithms is a promising approach to improving the cybersecurity of wireless channels. That is why the development, modelling, and comparative analysis of FHSS are important scientific and applied tasks aimed at creating a multilevel protection system for mobile and satellite systems capable of functioning under multi-factor threats.

Literature review. Modern scientific and practical activities have proven that FHSS is a highly effective approach that significantly complicates the implementation of jamming attacks [10, 11]. In general, this is possible because the adversary is forced to either use high-energy interference or quickly track the frequency-hopping sequence, both of which are practically impossible or more complicated without knowledge of the algorithm's parameters. In addition, FHSS reduces the probability of effective signal interception and spectral analysis, since the signal does not remain at a single frequency for long [12]. Compared to static frequency modes, FHSS systems are characterised by their ability to adapt to changing conditions in the radio-electronic environment. This makes them especially effective when used in mobile and satellite infocommunication systems operating in conditions of active information warfare.

The high efficiency of applying FHSS algorithms in both general and specialised practice is evidenced by numerous research results. Based on a priori analysis of FHSS, it has been established that, in general, known algorithmic implementations can be classified into slow- and fast-hopping [13, 14]. In slow FHSS, the frequency changes at intervals that are significantly longer than the duration of a single symbol or data packet. This approach reduces the need for high synchronisation but, at the same time, makes the system more vulnerable to adaptive attacks. In fast FHSS, the frequency changes at the level of individual or several symbols, which increases interference immunity. At the same time, this approach imposes more stringent requirements for synchronisation between the transmitter and receiver. Fast FHSS algorithms also require powerful computing resources and precise synchronisation circuits, which create technical challenges in mobile and resource-constrained devices.

Analysis of scientific sources [5, 11, 15] has established that modern attack models for FHSS systems encompass a wide range of techniques aimed at disrupting wireless communication or obtaining information. One of the classic techniques is jamming. For example, in the broadband implementation, the adversary emits a noise or pseudo-stochastic signal over a wide frequency range, reducing the signal-to-noise ratio at all frequencies simultaneously. This approach can partially or completely disable signal reception, especially when a limited spectrum is used for transmission. Another type is adaptive jamming, in which the adversary analyses current frequency transitions and attempts to predict subsequent frequencies for instantaneous impact. In such scenarios, signals from previous frequency hops can be used to predict future transitions. This significantly increases the effectiveness of attacks compared to static broadband jamming [16].

In addition, recent studies show the feasibility of implementing more complex attacks, such as interception and spectrum analysis. In such attacks, the adversary does not simply jam but attempts to reconstruct the pseudo-random frequency-hopping sequence through spectral and correlation analysis and machine learning [17, 18]. Such methods can potentially breach the complex protection of systems, decode transmitted data, or predict future frequency transitions.

At the same time, FHSS research and practical developments demonstrate that this approach can be effectively applied at the hardware level of infocommunication systems. In [11], an approach has been proposed that uses intelligent jamming in wireless communication devices rather than simply avoiding it. The authors have demonstrated that their proposed method not only enhances the ability to counter high-speed reactive interference but also better leverages reactive interference to improve communication performance under difficult operating conditions.

The authors of the scientific article [19] proposed and investigated an approach that implements a pseudo-random frequency jump generator on FPGA hardware. During implementation, the technique of chaotic mappings was used, achieving a high carrier frequency-jumping speed on real equipment.

In the scientific article [20], the authors demonstrated the feasibility and effectiveness of using FHSS in UAVs. The study uses quantum random number generators to produce truly random hopping sequences. This significantly increases resistance to interception and adaptive jamming by improving the unpredictability of sequences. Simulation results confirmed significantly improved uniformity of the frequency distribution and the absence of noticeable correlation patterns.

The authors of the manuscript [21] conducted research using a software-defined radio system to detect frequency-hopping signals. The article demonstrates that real-time FHSS generation and detection can be implemented with hopping frequencies of up to several hundred per second.

Today, there is also a significant number of scientific works devoted to the effectiveness of implementing FHSS through computer modelling and objective simulation methods. For example, in [22], the authors implemented a method to evaluate the effectiveness of FHSS in practical wireless network scenarios in MATLAB.

In [23], the authors implemented numerical modelling approaches to detect and evaluate the frequency spectrum of FHSS signals using signal processing algorithms.

The authors of [24] implemented a simulation-based approach to detecting FHSS signals, using an adaptive deep learning algorithm. As a result of their research, the authors demonstrated how software modelling of FHSS can be integrated with modern data processing methods and approaches.

Thus, the analysis of existing research on improving the cybersecurity of wireless infocommunication systems has demonstrated the significant effectiveness of FHSS approaches in countering cyberattacks on mobile and satellite communications. Given the considerable depth and scope of the research literature in this field, it is worth highlighting the following limitations that warrant further development. Most existing approaches are characterised by insufficient adaptability to dynamic radio-electronic environments. This is due, in particular, to the fact that most systems rely on fixed pseudo-random sequences that do not account for changes in the spectrum or the nature of attacks. This makes such systems vulnerable to adaptive and reactive jamming. A significant limitation is the complexity of reproducible testing of known models, as most of them rely on simplified simulation models, which complicates the objective comparison of FHSS algorithms. The limited availability of open models and detailed experimental environments also hinders the replication of results and the development of more effective and adaptive solutions.

In view of the above, the scientific and applied task of developing simulation models for an objective, reproducible comparison of different FHSS approaches is becoming increasingly relevant. This will allow for a systematic and comprehensive assessment of their interference immunity and overall effectiveness. As a result, such development will increase the efficiency of the design and practical application of cyber protection measures for wireless mobile and satellite communications.

The main aim and objectives of the study. Based on an analysis of known solutions for developing FHSS methods and means for wireless infocommunication systems, along with their main limitations, the main aim of this article was formulated. It is to improve the efficiency of mobile and satellite communication system design by developing and validating a simulation model that enables an objective comparison of different algorithmic approaches to FHSS implementation. Based on the decomposition of the main aim, the following set of the research tasks were formulated for this article:

1. To develop and test a computer model of a wireless communication channel with FHSS. This model should reproduce the processes of transmission, synchronisation, and frequency hopping, ensuring the controllability and reproducibility of the study of FHSS mechanisms.

2. To implement and integrate a set of FHSS algorithms into the model, which will allow for their objective comparison based on the main technical and functional indicators.

3. To objectively simulate the most common attack scenarios at the physical level (jamming and signal interception), which will make it possible to assess the impact of various types of threats on the performance of systems with FHSS.

4. To conduct a quantitative comparative assessment of the effectiveness of FHSS algorithms based on a set of communication quality metrics, which will allow for formulating practical recommendations for the selection and configuration of FHSS algorithms for the cyber protection of wireless systems.

Therefore, achieving the main aim and completing the set tasks will increase the efficiency of designing physical-level cyber protection measures for wireless infocommunication systems in the presence of signal jamming and data interception.

Materials and methods. To address the scientific tasks and achieve the article's main aim, a set of approaches and methods was used. These methods and approaches are widely recognised and tested in modern scientific research on the cyber protection of infocommunication systems.

At the first stage, an analysis and generalisation of the main cyber threats and methods of countering them was carried out. The main focus was on radio-electronic jamming and signal interception. This enabled the formulation of requirements for a computer model and the identification of its main research stages.

The initial stage of the research was based on computer experiments and simulation modelling. This made it possible to reproduce the processes at the physical level of a wireless communication channel, accounting for noise, interference, and deliberate attacks. Modelling, testing, and graphical interpretation of results were performed in Python using the Google Colab service, which enabled flexibility in implementation, reproducibility of experiments, and scalability of the model. During the research, a model of the physical-layer baseband signal was formulated as a complex I/Q signal corresponding to real digital signals in mobile and satellite systems, as shown in Fig. 1. The signal was modulated using quadrature phase-shift keying (QPSK). The main parameters of the synthesised test signal are as follows: number of symbols is equal to 300; number of samples per symbol is equal to 8; symbol values are equal to ±1 for in-phase (I) and quadrature (Q) components. Additionally, the signal contained phase fluctuations that simulate the instability of generators in real transmitters [25].

In the research, an additive white Gaussian noise (AWGN) component with a zero mean value was added to the signal. Deliberate destabilising influences in the

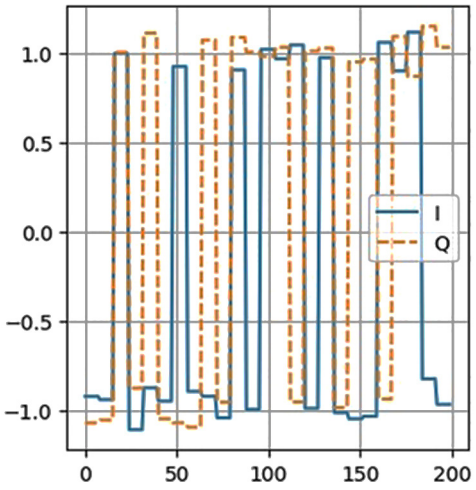


Fig. 1. Generated test signal (X-axis – sample index, Y –axis – amplitude of I and Q components)

form of selective, narrowband jamming, reflecting typical electronic warfare methods, were also modelled. The FHSS mechanism was implemented at the physical level by frequency-modulating the base I/Q signal according to a sequence of frequency jumps. The study considered three transmission modes: No FHSS (fixed frequency), FHSS with a random sequence (Random FHSS), and FHSS based on a linear feedback shift register (LFSR FHSS). On the receiving side, a reverse-frequency de-hopping process was implemented, allowing the signal to be correctly restored before demodulation. All this enabled objective accounting for the actual operating conditions of wireless communication channels in mobile and satellite systems. A detailed description of the studied FHSS types is provided in Table 1.

The main types of destabilising influences and simulated attacks in this study were: channel noise, selective narrowband jamming, and spectral-signature ML interception of frequency transitions.

During the implementation of the computer model, a standard set of Python libraries was used, the purpose of which is specified in Table 2.

A set of metrics was used to quantitatively assess the effectiveness of the approaches under study. These metrics are informative for assessing the physical-layer interference immunity of infocommunication systems [26, 27]. Their substantive purpose and formalised description are given in Table 3. These metrics were calculated for conditions without attacks and with jamming. This enabled a comparative analysis of the stability of different transmission modes.

A separate stage of the research was the modelling of signal interception. For this purpose, a machine learning (ML) approach based on the Random Forest (RF) algorithm was used. The implemented approach simulates the following scenario. The interceptor analyses the signal's spectral characteristics in each hopping interval and attempts to recover the active frequency chan-

Table 1

Studied types of FHSS algorithms

Type of FHSS	Implementation in the model	Expected applied effect
Fixed frequency (No FHSS)	Basic mode at a fixed frequency without hopping	Used as a baseline in comparative analysis, characterised by the highest vulnerability to jamming
FHSS with a random sequence (Random FHSS)	The frequency of each interval is selected from a uniform distribution (using a Python random number generator)	Reduced predictability of transitions
FHSS based on a linear feedback shift register (LFSR FHSS)	The sequence is formed by a linear shift register with feedback (a bit LFSR generator with mapping to channel indices has been implemented)	Improving reproducibility, pseudo-randomness, and structure

Table 2

Python libraries used and their purpose in creating and testing the computer model

Library	Version	Purpose of the use
NumPy	2.0.2	Generation of test sequences, working with complex I/Q signals, implementation of pseudo-random frequency hopping algorithms, and calculation of quantitative metrics
SciPy	1.16.3	Spectral analysis of signals, in particular, the creation of spectrograms in the time-frequency domain
Matplotlib	3.10.0	Graphical interpretation of results in the form of time diagrams of I/Q signals, modulation constellations, classical spectra, and comparative metric diagrams
Scikit-learn	1.6.1	Implementation of machine learning algorithms for modelling the interception process and predicting frequency transitions

Table 3

Metrics for evaluating FHSS algorithms in information and communication systems

Metrics	Formalised description
Bit error rate (*BER*). Used to estimate the proportion of incorrectly received bits, which characterizes the reliability of digital data transmission	$BER = \frac{N_{errors}}{N_{bits\ total}}$, where N_{errors} is the number of errors in the received bit sequence; $N_{bits\ total}$ is the total number of bits transmitted
Error of vector modulation (*EVM*). Used to evaluate modulation quality and signal distortion levels	$EVM = \sqrt{\frac{\frac{1}{N}\sum_{i=1}^{N}\left\|E_{r,i} - E_{t,i}\right\|^2}{P_a}}$, where N is the number of characters in the analysed sequence; $E_{r,i}$ is the complex value of the accepted i^{th} character; $E_{t,i}$ is the reference value of the i^{th} character; P_a is an average power of transmitted characters
Output signal-to-noise ratio (SNR_{out}). Used for generalised assessment of signal reception quality	$SNR_{out} = 10\lg\left(\frac{E\left[\left\|S_{ref}\right\|^2\right]}{E\left[\left\|S_{rx} - S_{ref}\right\|^2\right]}\right)$, where S_{ref} is a reference signal; S_{rx} is a received signal; $E[\|...\|]$ – is the mathematical expectation of a signal sample

Table 4

The main stages of development and research of a computer model for evaluating the effectiveness of the FHSS implementation

Stage	Applied effect	Software and algorithmic implementation	Quantitative and qualitative results
Formation of a test I/Q signal	Objective simulation of physical-level processes in mobile and satellite systems	Generation of a complex QPSK I/Q signal with phase fluctuations and oversampling	Graphical interpretation of the I/Q signal in the form of time diagrams
Formation of a noisy I/Q signal	Assessment of the basic noise immunity of the communication channel	Adding AWGN component	Graphical interpretation of a noisy I/Q signal in the form of time diagrams
Implementation of FHSS algorithms and spectral analysis of signals	Comparative analysis of FHSS algorithms	Algorithm implementation: No FHSS, Random FHSS, LFSR FHSS; frequency hopping and de-hopping on the receiver	Graphical interpretation in the form of spectrograms and comparative constellation diagrams
Simulation of a selective narrowband jamming attack	Assessment of resistance to selective narrowband noise jamming	Adding frequency-localised interference components	Distorted signal spectra and constellation diagrams
Interception modelling and ML prediction of hop sequences	Assessment of the predictability of frequency transitions	Extraction of spectral features at hop intervals and implementation of the RF classifier	Graphical interpretation in the form of a confusion matrix
Quantitative assessment of communication quality and comparative analysis of transmission modes	Objective comparison of FHSS algorithms' performance	Unified set of calculated BER, EVM, SNR_{out} metrics for No FHSS, Random FHSS, and LFSR FHSS modes	Comparative metric diagrams

nel number. Averaged spectral components were used as features, and the effectiveness of interception was evaluated using an error matrix. This enabled a quantitative assessment of the reduction in the predictability of frequency transitions in FHSS systems.

Thus, based on the above description, a detailed algorithm for developing and researching a computer model to assess the effectiveness of implementing the FHSS was synthesized. The proposed algorithm is presented in detail in Table 4.

Thus, the proposed research approach integrates computer modelling methods, statistical analysis, and the formalisation of cyber threats and countermeasures. This may provide an assessment and analysis of the effectiveness of implementing FHSS as a mechanism to increase interference immunity and reduce the probability of signal interception in wireless systems. The proposed research methodology allows assessing the effectiveness of various FHSS implementations at the early stages of designing physical-level protection measures for mobile and satellite communications.

Results. This section presents the results of computer modelling of signal transmission processes with frequency-hopping spread spectrum. During the experiments, in the first stage, a complex I/Q signal was formed with oversampling, phase fluctuations, and the influence of deliberate jamming interference, as shown in Fig. 2. On the receiving side, for modes with FHSS, a software implementation of the reverse frequency compensation (de-hopping) procedure was implemented.

The time diagrams (Fig. 2) show fragments of the I and Q components of the signal for three states: without interference, with AWGN (SNR = 12 dB) and with additional jamming. Analysis of the graphical interpretation of these signals showed the following. In the mode "No FHSS", a regular structure is observed, corresponding to QPSK symbols with oversampling. Adding AWGN results in a moderate amplitude spread. The effect of narrowband interference in this mode manifests itself as a noticeable deformation of the oscillations of the I and Q components. There is also an increase in amplitude deviations and phase distortions. Since the signal is constantly in one frequency channel, the inter-

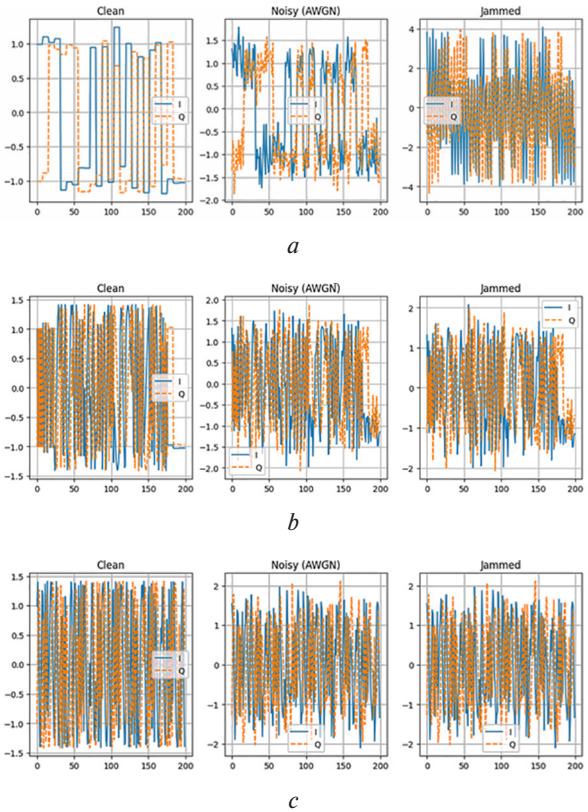


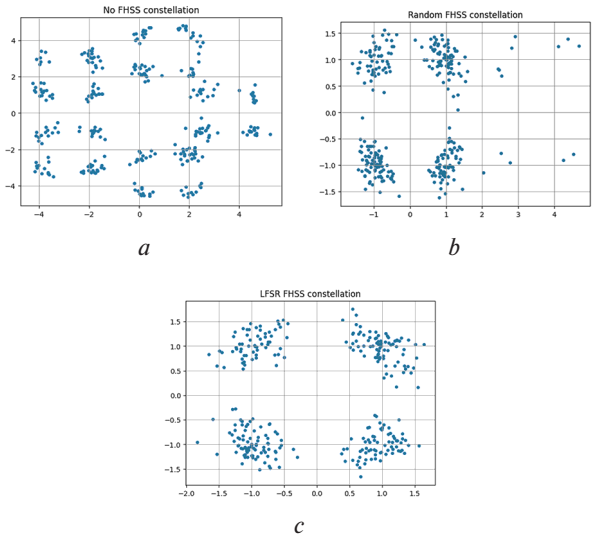
Fig. 2. Test I/Q signal fragments (X-axis – sample index, Y-axis – amplitude of I and Q components):
a – No FHSS; b – Random FHSS; c – LFSR FHSS

ference affects it continuously. In FHSS modes, distortions are fragmented. They are localised only in those intervals where the frequency jump falls into the noisy channel. On the graphs, this manifests itself as short sections of signal degradation against a background of a relatively stable structure in other intervals. Thus, the modelled dependencies accurately reflect real processes during data transmission at the physical level of wireless systems.

The constellation diagrams shown in Fig. 3 were used to graphically interpret and analyse the degree of symbol dispersion in the I/Q plane after reception and demodulation. As shown in these graphs, in the presence of noise and jamming, the mode without FHSS exhibits a significant expansion of the point clouds around the ideal positions of the QPSK constellation. In some cases, overlapping between neighbouring quadrants occurs, which increases the probability of bit errors. In modes with FHSS, after performing the de-hopping procedure, the constellation points remain noticeably more compact. Despite interference, a significant portion of the symbols falls close to their ideal positions. This indicates that frequency hopping, together with frequency offset compensation on the receiver's side, reduces the impact of selective jamming on the received symbols. Compared to a random sequence, the LFSR sequence shows a similar but slightly more structured scattering pattern. This is due to the more deterministic properties of the hopping sequence. This indicates that the use of the frequency-hopping mechanism reduces the total impact of interference on symbols and improves modulation-state recovery.

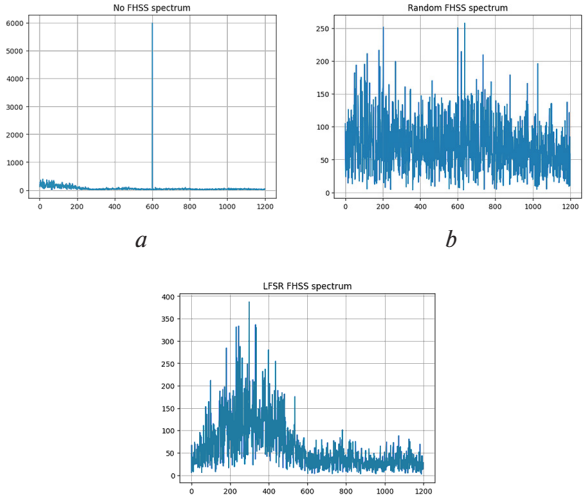
For a more detailed analysis of the effectiveness of the FHSS mechanism, a set of classical spectral characteristics and spectrograms was constructed and shown in Figs. 4 and 5.

Analysis of spectral characteristics has proven the following. In the mode "No FHSS", the energy peak of the signal is concentrated in a narrow band. Therefore, selective interference forms a pronounced spectral maximum in the same area. This means effective energy



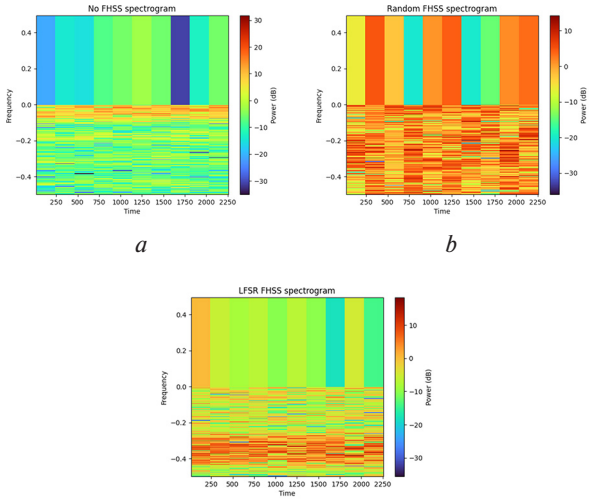
a *b* *c*

Fig. 3. Constellation diagrams:
a – No FHSS; b – Random FHSS; c – LFSR FHSS



a *b* *c*

Fig. 4. Spectral characteristics (X-axis – frequency bins, Y-axis – spectrum amplitude):
a – No FHSS; b – Random FHSS; c – LFSR FHSS



a *b* *c*

Fig. 5. Spectrograms:
a – No FHSS; b – Random FHSS; c – LFSR FHSS

overlap of the useful signal by interference. In FHSS modes, a multi-peak distribution is observed, confirming the signal energy distribution across several frequency positions. Therefore, in the presence of selective interference in one channel, other frequency positions remain less susceptible to be damaged.

Graphical interpretation of the results in the form of spectrograms showed that for the mode "No FHSS", the spectrogram contains mainly one horizontal band. This corresponds to a fixed carrier frequency, so the interference is superimposed on the same band throughout the entire transmission time. For FHSS modes, a characteristic 'step' or 'dash' pattern is observed, in accordance with the "Random FHSS" and "LFSR FHSS" approaches. This is due to sequential energy transitions between different frequency channels. Selective interference manifests as a local energy increase only at certain time intervals. This approach confirms the increased probability of avoiding interference through frequency hopping.

At the final stage of the study on the effectiveness of FHSS application, a comparative analysis of the main metrics across different modes was conducted. A graphical interpretation of the obtained averaged estimates is shown in Fig. 6.

The BER in "No FHSS" mode is the highest, reflecting high sensitivity to selective jamming. For FHSS modes, the BER decreases because only a portion of the symbols are transmitted in the affected channel. The EVM is minimal for FHSS modes, which is also confirmed by the more compact arrangement of the constellation points (Fig. 3). The output SNR_{out} after reception and processing is higher for FHSS modes, since de-hopping and frequency spreading reduce the effective power of interference relative to the useful signal. In "No FHSS" mode, in the presence of selective jamming, the SNR_{out} value in a series of experiments can take negative values. This indicates that the average power of interference distortions exceeds the power of the useful signal after reception. In FHSS modes, this effect is not observed due to the time-frequency dispersion of the interference. Thus, the results shown in Fig. 6 proved the effectiveness of FHSS in protecting the physical layer of infocommunication systems from selective narrowband jamming. In this case, the most effective algorithm is LFSR FHSS.

As mentioned above, an additional stage of research in this article was the modelling of interception and the ML prediction of hop sequences. This enabled assessment of the predictability of frequency transitions by identifying spectral features at hop intervals with a Random Forest (RF) classifier. To assess resistance to interception, a passive spectral signal analysis scenario was modelled. In this case, the interceptor does not affect the transmission but only analyses short-time frequency fragments of the received signal. Based on spectral features, the active frequency channel was classified using the RF algorithm. The interception quality was evaluated using a confusion matrix, which enabled a quantitative assessment of the level of concealment of the frequency transition sequence in FHSS systems, as shown in Fig. 7.

The confusion matrix shown in Fig. 7 demonstrated the implemented ML model's ability to determine the active frequency channel based on the spectral characteristics of the hopping interval. In this matrix, the diagonal elements correspond to correct channel predictions, while the off-diagonal elements correspond to errors. The computer experiment revealed the following. All non-zero values are concentrated on the main diagonal or in cells adjacent to it. All other off-diagonal elements are equal to zero. This means that the proposed model determines the frequency channel in each hopping interval with high probability. This result indicates the high spectral distinctiveness of frequency positions in the modelled signal and the potential vulnerability of the considered FHSS mode to interception attacks when using spectrally oriented ML analysis methods. The results indicate that, in the presence of FHSS, the physical layer of wireless systems remains vulnerable to intellectualised interception attacks. This confirms the need to further develop adaptive FHSS methods, mechanisms for masking spectral features, and combined physical protection schemes to improve the resilience of wireless infocommunication systems.

Discussions, limitations and prospect research directions. The research results confirm that the use of FHSS mechanisms at the physical level significantly increases the resistance of wireless signals to frequency-localised interference and selective narrowband jamming. The qualitative results are consistent with the classical principles of FHSS theory, in which signal energy spreading in the frequency domain and rapid carrier frequency changes reduce the probability of prolonged channel damage. Quantitative results of computer experiments in the form of constellation diagrams, spectrograms, and metric distribution diagrams showed the ability of FHSS algorithms to complicate the task of continuous suppression of transmission using narrowband interference.

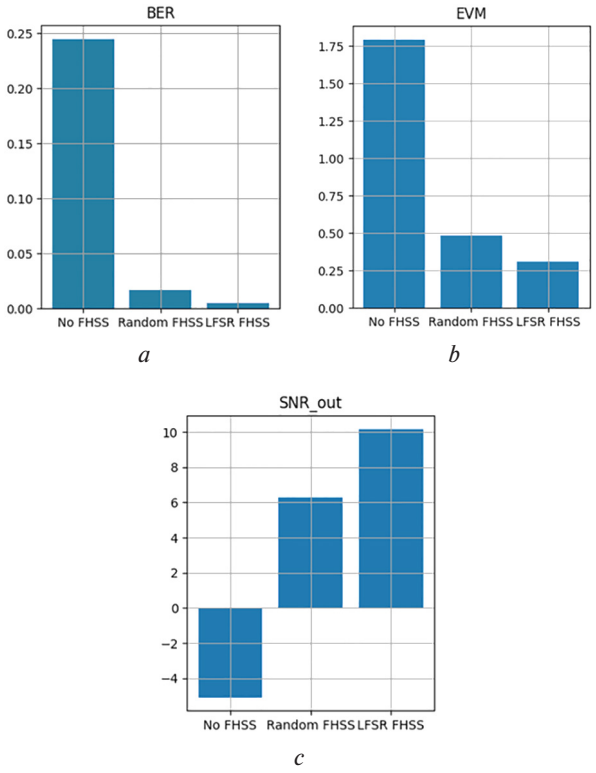


Fig. 6. Averaged metrics distribution diagrams: a – BER; b – EVM; c – SNR_{out}

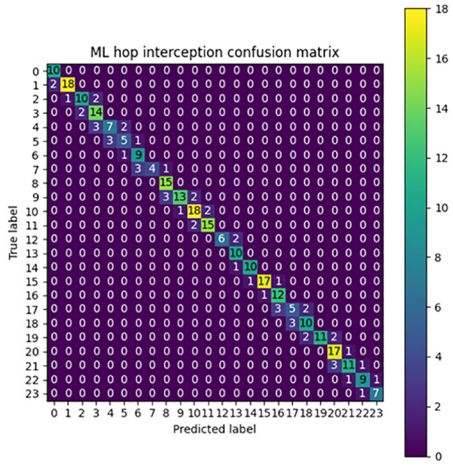


Fig. 7. Interception confusion matrix based on RF algorithm

At the same time, ML-based interception modelling results show that, given sufficiently distinct spectral characteristics at frequency positions, the classification algorithm can recover the active channel number with high accuracy. This means that the mere use of FHSS does not guarantee sufficient protection against modern intellectualised attacks and requires a combination with additional masking and adaptation mechanisms.

Additionally, it is worth emphasising certain limitations of the proposed computer model. The research was conducted in a simulation channel with AWGN and relatively simplified jamming scenarios (narrowband selective damage to the communication channel). Furthermore, the FHSS algorithms used do not cover all possible cryptographically secure and adaptive frequency sequence generation schemes.

Based on this, further research should focus on the following:

- formalising and considering more types of attack models, such as broadband and reactive jamming, adaptive jammer attacks, combined interception scenarios, and others;
- formalising and considering hardware instabilities in the model, such as synchronisation errors, freezes, frequency switching delays, and others;
- integrating FHSS mechanisms with spectral masking methods, signal expansion, and intelligent control of physical layer parameters.

All this, in turn, will improve the efficiency of designing secure wireless information and communication systems and their subsequent use in real-world scenarios.

Conclusions. A computer model to study the impact of FHSS algorithms on the security of the physical layer of information and communication systems was developed and validated. The main focus was on the use of FHSS mechanisms to counter jamming and signal-interception attacks. The model is implemented in specialised software that generates a complex QPSK I/Q signal, adds noise and intentional interference, implements FHSS algorithms, and performs ML-based frequency transition interception.

Spectral and time-frequency analysis results showed that in "No FHSS" mode, the signal energy is concentrated in a single frequency channel, leading to persistent damage from selective interference. In "Random FHSS" and "LFSR FHSS" modes, energy is spread across frequency and time, reducing the probability of affected spectrum areas and generally increasing the transmission's noise immunity.

Quantitative analysis of the research results showed the following. The probability of bit error in modes with frequency hopping is an order of magnitude lower compared to the mode without frequency hopping. The vector modulation error for "LFSR FHSS" mode is minimal and does not exceed 0.3 units, which is on average 7 times less than the mode without frequency hopping. The output signal-to-noise ratio for FHSS modes is sufficient (from 6 to 10 dB), whereas in "No FHSS" mode, negative values are observed in some experiments under selective jamming conditions.

Thus, based on computer experiments, it was established that the best generalised indicators for the set of relevant metrics were demonstrated by the FHSS algorithm based on the LFSR. This makes its integration into mobile and satellite communication systems promising.

The results of ML modelling of interception showed that when using spectral features and the Random Forest classifier, the accuracy of determining the active frequency channel can be high. This indicates the potential predictability of frequency transitions in simplified FHSS schemes and confirms the need to develop adaptive and spectral masking algorithms for FHSS.

In general, the results confirm the effectiveness of FHSS in improving the physical-layer interference immunity of wireless information and communication systems. This, in turn, substantiates the feasibility of using the proposed computer model when designing cyber protection measures for information and communication systems by objectively comparing jamming and interception protection algorithms.

Acknowledgements. *The article was prepared within the framework of the project 2025.06/0047 'Information technologies of cryptographic protection and data authentication for mobile and satellite communication systems'. This project received funding from the National Research Foundation of Ukraine.*

References.

1. *ENISA: Telecom security incidents 2024* (n.d.). Retrieved from https://www.enisa.europa.eu/sites/default/files/2025-07/ENISA_Telec om_Security_Incidents_2024_en_1.pdf

2. *UNDRR: Radio and Other Telecommunication Failures* (n.d.). Retrieved from https://www.undrr.org/understanding-disaster-risk/terminology/hips/tl0212

3. *EUPOS: GNSS Jamming and Spoofing: how serious can it be?* (n.d.). Retrieved from https://www.eupos.org/sites/default/files/Meetings/EUPOS_2022_GNSS_Jamming_and_Spoofing.pdf

4. Radoš, K., Brkić, M., & Begušić, D. (2024). Recent Advances on Jamming and Spoofing Detection in GNSS. *Sensors*, *24*(13), 4210. https://doi.org/10.3390/s24134210

5. Laktionov, I., Diachenko, G., Moroz, D., & Getman, I. (2025). A Comprehensive Review of Cybersecurity Threats to Wireless Infocommunications in the Quantum-Age Cryptography. *Internet of Things*, *6*(4), 61. https://doi.org/10.3390/iot6040061

6. Nagpal, M., Pattnaik, S. C., Baxi, P., Rani, H. J. R., Canessane, R. A., & Chaudhary, P. (2025). Physical Layer Security Techniques for Wireless Communication Systems. *2025 International Conference on Automation and Computation (AUTOCOM)*. Dehradun, 673-678. https://doi.org/10.1109/AUTOCOM64127.2025.10957012

7. Boodai, J., Alqahtani, A., & Frikha, M. (2023). Review of Physical Layer Security in 5G Wireless Networks. *Applied Sciences*, *13*(12), 7277. https://doi.org/10.3390/app13127277

8. Purkayastha, T., De, D., & Das, K. (2016). A novel pseudo random number generator based cryptographic architecture using quantum-dot cellular automata. *Microprocessors and Microsystems*, *45*(A), 32-44. https://doi.org/10.1016/j.micpro.2016.03.001

9. Wang, L., & Cheng, H. (2019). Pseudo-Random Number Generator Based on Logistic Chaotic System. *Entropy*, *21*(10), 960. https://doi.org/10.3390/e21100960

10. Pirayesh, H., & Zeng, H. (2022). Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials*, *24*(2), 767-809. https://doi.org/10.1109/COMST.2022.3159185

11. Huang, T., Liu, Y., Liu, X., & Wang, M. (2025). A New Improved Multi-Sequence Frequency-Hopping Communication Anti-Jamming System. *Electronics*, *14*(3), 523. https://doi.org/10.3390/electronics14030523

12. Wang, H., Yang, L., Bin, J., Gou, C., Hou, B., & Qin, M. (2026). A Detection Method for Frequency-Hopping Signals in Complex Environments Using Time–Frequency Cancellation and the Hough Transform. *Electronics*, *15*(2), 429. https://doi.org/10.3390/electronics15020429

13. Schmidt, J. H. (2020). Using Fast Frequency Hopping Technique to Improve Reliability of Underwater Communication System. *Applied Sciences*, *10*(3), 1172. https://doi.org/10.3390/app10031172

14. Lan, M., Luo, Z., & Jiang, M. (2025). Intelligent Modulation Recognition of Frequency-Hopping Communications: Theory, Methods, and Challenges. *Big Data Cogn. Comput.*, *9*(12), 318. https://doi.org/10.3390/bdcc9120318
15. Duan, R., Jin, L., & Lan, X. (2025). Analysis of Anti-Jamming Performance of HF Access Network Based on Asymmetric Frequency Hopping. *Sensors*, *25*(9), 2950. https://doi.org/10.3390/s25092950
16. Djuraev, S., & Nam, S. Y. (2020). Channel-Hopping-Based Jamming Mitigation in Wireless LAN Considering Throughput and Fairness. *Electronics*, *9*(11), 1749. https://doi.org/10.3390/electronics9111749
17. Thiele, P., Bernado, L., Löschenbrand, D., Rainer, B., Sulzbachner, C., Leitner, M., & Zemen, T. (2023). Machine Learning Based Prediction of Frequency Hopping Spread Spectrum Signals. *2023 IEEE 34th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 1-6. Toronto. https://doi.org/10.1109/PIMRC56721.2023.10293939
18. Zhu, J., Wang, A., Wu, W., Zhao, Z., Xu, Y., Lei, R., & Yue, K. (2023). Deep-Learning-Based Recovery of Frequency-Hopping Sequences for Anti-Jamming Applications. *Electronics*, *12*(3), 496. https://doi.org/10.3390/electronics12030496
19. Ayoub, H. G., Abdulrazzaq, Z. A., Fathil, A. F., Hasso, S. A., & Suhail, A. T. (2024). Unveiling robust security: Chaotic maps for frequency hopping implementation in FPGA. *Ain Shams Engineering Journal*, *15*(1), 103016. https://doi.org/10.1016/j.asej.2024.103016
20. de Curtò, J., de Zarzà, I., Cano, J.-C., & Calafate, C.T. (2024). Enhancing Communication Security in Drones Using QRNG in Frequency Hopping Spread Spectrum. *Future Internet*, *16*(11), 412. https://doi.org/10.3390/fi16110412
21. Șorecău, M., Popa, G.-E., Șorecău, E., & Bechet, P. (2025). SDR system for real-time FHSS communications detection and jamming. *International Conference KNOWLEDGE-BASED ORGANIZATION*, *31*(3), 168-176. https://doi.org/10.2478/kbo-2025-0093
22. Fernández de Gorostiza, E., Berzosa, J., Mabe, J., & Cortiñas, R. (2018). A Method for Dynamically Selecting the Best Frequency Hopping Technique in Industrial Wireless Sensor Network Applications. *Sensors*, *18*(2), 657. https://doi.org/10.3390/s18020657
23. Lei, Z., Yang, P., & Zheng, L. (2018). Detection and Frequency Estimation of Frequency Hopping Spread Spectrum Signals Based on Channelized Modulated Wideband Converters. *Electronics*, *7*(9), 170. https://doi.org/10.3390/electronics7090170
24. Liu, F., & Jiang, Y. (2023). Knowledge-Enhanced Compressed Measurements for Detection of Frequency-Hopping Spread Spectrum Signals Based on Task-Specific Information and Deep Neural Networks. *Entropy*, *25*(1), 11. https://doi.org/10.3390/e25010011
25. Laktionov, I. S., Hnatushenko, V. V., Udovyk, I. M., & Olevskyi, V. I. (2025). Simulation-driven assessment of cryptographic algorithms for resource-constrained infocommunication networks. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, (6), 148-156. https://doi.org/10.33271/nvngu/2025-6/148
26. Fatadin, I. (2016). Estimation of BER from Error Vector Magnitude for Optical Coherent Systems. *Photonics*, *3*(2), 21. https://doi.org/10.3390/photonics3020021
27. Jia, J., Zou, P., Hu, F., Zhao, Y., & Chi, N. (2020). Flexible Data Rate V2X Communication System beyond 1.84 Gb/s Based on MIMO VLC and Radar Integration. *Applied Sciences*, *10*(19), 6636. https://doi.org/10.3390/app10196636

Програмно-реалізоване оцінювання псевдовипадкового перелаштування частот для кібербезпеки бездротової інфокомунікації

В. В. Гнатушенко[*], *І. С. Лактіонов, І. М. Удовик*

Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна

[*] Автор-кореспондент e-mail: Hnatushenko.V.V@nmu.one

Мета. Підвищення ефективності проєктування систем мобільного й супутникового зв'язку шляхом розробки та валідації комп'ютерної моделі, що дозволяє об'єктивно симулювати й порівнювати різні алгоритмічні підходи до псевдовипадкового перелаштування частоти (ППРЧ).

Методика. Використані методи комп'ютерного експерименту в середовищі Python із формуванням комплексного I/Q сигналу із передискретизацією й фазовими флуктуаціями. Програмно реалізовані три режими передачі даних: без ППРЧ, випадкове ППРЧ і ППРЧ на основі лінійного регістру зсуву зі зворотним зв'язком. Змодельовані атаки типу селективного вузькосмугового глушіння й перехоплення на основі машинного навчання. Оцінювання ефективності алгоритмів виконано за сукупністю метрик: BER, EVM та SNR_{out}. Графічна інтерпретація реалізована у вигляді часових і спектральних залежностей, сузір'я-діаграм і матриці помилок.

Результати. Реалізована комп'ютерна модель, що дозволила оцінити ефективність і придатність алгоритмів ППРЧ під час кіберзахисту засобів мобільного й супутникового зв'язку. Встановлено, що найкращі узагальнені показники за сукупністю метрик продемонстрував алгоритм ППРЧ на основі лінійного регістру зсуву зі зворотним зв'язком. Для режимів із ППРЧ спостерігається рознесення енергії за частотою й часом, що забезпечує зменшення вірогідності уражених ділянок спектру й загалом підвищує завадостійкість передачі даних. Вихідне співвідношення сигнал/шум для цих варіантів в умовах селективного глушіння знаходиться на задовільному рівні. Обґрунтована необхідність подальших досліджень із розробки адаптивних методів ППРЧ і механізмів маскування спектральних ознак.

Наукова новизна. Встановлені закономірності впливу алгоритмів ППРЧ на показники завадостійкості й перехоплюваності даних на фізичному рівні бездротових систем. Одержали подальшого розвитку підходи до комплексного порівняльного оцінювання ефективності застосування алгоритмів ППРЧ в умовах адитивного шуму, навмисного глушіння та інтелектуалізованого перехоплення.

Практична значимість. Розроблена комп'ютерна модель придатна для порівняльного аналізу алгоритмів ППРЧ у бездротових системах в умовах шуму, глушіння й перехоплення. Запропонована модель може бути використана для вибору раціональних схем ППРЧ під час проєктування кіберзахищених систем мобільного й супутникового зв'язку.

Ключові слова: *перелаштування частоти, алгоритм, глушіння, перехоплення, інфокомунікаційна система, комп'ютерна модель*

The manuscript was submitted 02.12.25.