Conflict Model of Radio Engineering Systems under the Threat of Electronic Warfare

Volodymyr Astapenya[1], Yuliia Zhdanova[1], Svitlana Shevchenko[1], Svitlana Spasiteleva[1], and Olena Kryvoruchko[2]

[1] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*
[2] *State University of Trade and Economics, 19 Kioto str., Kyiv, 02156, Ukraine*

Abstract

The purpose of the article is to determine the necessary conditions for creating a conflict model of radio technical systems that function in the information space under the threat of radio Electronic Warfare (EW). The starting points of the theory of conflict about complex technical systems are given. It is determined that the Information Conflict (IC) is a key component of the conflict in the conditions of modern radio-electronic warfare. The information conflict is considered a process of combating radio electronic systems at the stage of obtaining information about the opponent and its transmission to consumers and radio suppression systems, which oppose them. The composition and functions of the subsystems included in the radio-electronic warfare system were analyzed: Radio Electronic Reconnaissance (RER), Radio Electronic Suppression (RES), and Radio Electronic Protection (REP). The list of modern systems that use radio waves to obtain and transmit information, as well as other types of information support, assuming the action of EW means against them, is considered. When creating a model of information conflict between similar systems and the EW system, factors that need to be identified are the interferences of various origins and especially intentional ones, the creation of which is one of the main tasks of EW. The main characteristics of information systems that can be violated and should be defined in the conflict model are interference resistance, interference protection, and secrecy. In a conflict, they are points of contact and, together with the characteristics of EW tools, need to be adequately reflected in a mathematical model. A list of conflicts between EW systems and other information systems is provided. An example of estimating the range of radio communication, radio reconnaissance, and navigation is given. The results of the research can be used as educational material for students of the specialty 125 Cybersecurity and Information Protection.

Keywords

Conflict, information conflict, information security systems, cyber system, cyber conflict, electronic warfare, radio-electronic reconnaissance, radio-electronic suppression, radio-electronic protection.

1. Introduction

Technical systems of various purposes, among which large-scale technical systems play an increasingly important role, have gained global distribution and occupy a dominant place in the main areas of people's lives. They form a technosphere in which the dominant role is occupied by complex ergatic systems with wide capabilities, tendencies to self-organization, a large volume of internal information and memory (as the ability to store one's experience and use it), and a certain freedom of behavior. The majority of such systems involve human participation as a subject of management and decision-making. This means that we are talking about ergatic systems [1–3] of a rather high level. Despite all their attractiveness, such systems are

CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2024, Kyiv, Ukraine
EMAIL: v.astapenia@kubg.edu.ua (V. Astapenia); y.zhdanova@kubg.edu.ua (Y. Zhdanova); s.shevchenko@kubg.edu.ua (S. Shevchenko), s.spasitielieva@kubg.edu.ua (S. Spasitielieva); ev_kryvoruchko@ukr.net (O. Kryvoruchko)
ORCID: 00000-0003-0124-216X (V. Astapenia); 0000-0002-9277-4972 (Y. Zhdanova); 0000-0002-9736-8623 (S. Shevchenko); 0000-0003-4993-6355 (S. Spasitielieva); 0000-0002-7661-9227 (O. Kryvoruchko)

inevitably characterized by conflict and poor predictability of some consequences, which sometimes leads to instability and catastrophic consequences [2–3]. For example, information exchange systems will not be able to ensure its integrity, availability, and confidentiality, which can lead to severe consequences in a system where this information is needed for proper functioning. In a certain sense, the prevention of such events is connected with the difficulties of forming adequate models of the relevant conflicts. Work on their creation is being carried out [4–9] and needs to be continued.

The conflict should be interpreted as a form of interaction of complex systems. Then, within the framework of the system approach, two options for describing this interaction (conflict) are possible:

- A general description taking into account the essential factors followed by the identification of the nature of the interaction, conflicting components, causes, mechanisms of development, and the result (such a model is complex, multifaceted, but relatively reliable).
- Proceeding assuming that the parties, causes and nature of the conflict are known, identify the main factor(s) and build a model to calculate the factor's contribution and the outcome of the conflict.

2. EW System Characteristics and Potential Conflicts with Radio Systems

One of the example of complex systems where there is a permanent conflict is the functioning of information systems of various purposes in the conditions of a potential threat of conducting Radio-Electronic Warfare (EW). Moreover, radio communication and countermeasures to it developed almost simultaneously.

Thus, the first episode of EW in the radio range took place in 1904, when near Port Arthur, jamming was used against the radio channel of the Japanese ship's artillery fire adjusters [10]. In the future, by the creation and development of other systems, where electromagnetic (as well as acoustic) waves are used, the development of EW was parallel. First of all, it is inherent in the military sphere, which left a certain mark on the terminology.

EW is a type of armed struggle in which radio emissions (radio jamming) are used to influence the radio-electronic means of the enemy's control, communication, and intelligence systems to change the quality of the information circulating in them, to protect one's systems from similar influences, as well as a change in the conditions (properties of the environment) of radio wave propagation.

Radio-electronic warfare (some authors [11] have long used the term radio-electronic or electronic war about it) is implemented by a corresponding system, which consists of the following main subsystems [10]:

- Radio-electronic reconnaissance (the main types of which are radio reconnaissance and radio technical reconnaissance).
- Management and control of the process and results of EW conducting.
- Radio suppression by radiation of interference.
- Electromagnetic damage to equipment by powerful electromagnetic pulses.
- Electronic protection of own means.

Radio-electronic reconnaissance collects reconnaissance information based on the reception and analysis of electromagnetic radiation. Radio electronic reconnaissance includes radio reconnaissance, the task of which is to intercept signals from communication channels and determine the content of messages, and radio technical reconnaissance, which, based on the analysis of the parameters of the received signals of working radars, communication stations, radio jamming stations, and other radio-electronic means, determines the type of appropriate means, their operating frequency, spectrum width, time parameters of signals, characteristic of antenna directionality, polarization of radiation, direction to the source of the signal and its location (this is also done by radio reconnaissance), parameters of the movement of the source and some other characteristics of radio-electronic means.

Radio and radio technical reconnaissance can monitor electromagnetic emissions in the range from 3 MHz to 30 GHz and above.

Based on the data received by radio-electronic reconnaissance, measures for radio-electronic suppression are implemented. Radio-electronic suppression is a set of measures and

actions related to disruption (violation) of work or reducing the effectiveness of the enemy's use of radio-electronic systems and means by affecting their receiving devices with radio-electronic interference. It includes radio, radio engineering, optical-electronic, and hydroacoustic suppression. Radio electronic suppression is provided by creating active and passive interference, using false targets, traps, and other methods.

Electromagnetic damage to the equipment is carried out due to the formation and emission of powerful electromagnetic pulses, which disable the enemy's electronic, communication, and power equipment. The damage effect is a consequence of the targeting of induction currents in electronic elements especially in long conductors. (For the first time such an effect was detected during nuclear explosions in the atmosphere.) Generators based on magnetrons can be used to create electromagnetic pulses. Such means are in service with the United States and other NATO countries.

Management and control of the process and results of EW management is a complex organizational and technical process, which involves monitoring the state of operation of one's radio-electronic means and their protection against the enemy's technical means of intelligence, evaluating the results of suppressing his means. It includes radio, radiotechnical, photographic, and visual-optical control, as well as control of the effectiveness of information protection against its leakage through technical channels during the operation of means of information transmission and processing. In the course of the current control and based on its results, management decisions are made in favor of radio-electronic protection and optimization of the EW system.

Radio-electronic protection is an integral part of radio-electronic warfare aimed at ensuring the stable operation of radio-electronic means under the influence of intentional radio interference by the enemy, electromagnetic radiation of weapons of functional damage, electromagnetic and ionizing radiation arising from the use of nuclear weapons, exposure to unintentional radio interference.

The basis of electronic protection is a set of organizational and technical measures aimed at:

- Ensuring electromagnetic compatibility of radio-electronic means.
- Ensuring the stability of radio-electronic means in the presence of unintentional interference.
- Protection of radio-electronic devices against intentional interference and ensuring their interference protection.
- Protection of radio-electronic means from electromagnetic and ionizing radiation (unintentional as well as intentional so-called electromagnetic weapons) to ensure the reliability of the functioning of radio-electronic means and to avoid functional damage to the elemental base.
- Protection against the influence of false signals and disinformation.

Measures to ensure the secrecy of the functioning of one's information systems and components of the radio-electronic warfare system should also be included in the radio-electronic protection.

The radio-electronic struggle brought a specific "coloring" to the content of the conflict of opposing radio-electronic means (radio-electronic systems), which acquired all the characteristic features of a severe (antagonistic) conflict. At the same time, an antagonistic conflict is understood as a specific form of interaction between some parties opposing each other, pursuing directly opposite interests, when a change in the efficiency of one party (radio engineering system, means, etc.) leads to the same magnitude, but opposite in sign changes in the effectiveness of the other (opposite) side.

For many years, EW was limited to solving the tasks of radio suppression of separately allocated radio-electronic means in favor of disorganizing the management of the forces and means of the opposing side and ensuring the stability of the management of its forces. Such a concept fully corresponded to the narrow specialization of radio equipment in the assumption of low interference resistance and conflict resistance in general. The simplest static model of the conflict (duel) of means and objects of radio suppression at the energy ("signal") level of its representation sufficiently corresponds to the conditions of radio suppression of such radio-electronic means. Such a model was based on the equations of anti-radio communication, anti-radiolocation,

and the well-known relations of the theory of potential jamming by V. A. Kotelnikov.

It should be noted that, traditionally, all classic tasks of radio communication, radar location, and radio navigation when applying this model are solved under the mandatory condition of the presence of unintentional interference, at least of natural origin—against the background of interference (thermal noise, noise of the atmosphere, space, and so on).

Thanks to the achievements in the field of element base, digital methods of signal processing, and information technologies, in recent years a qualitative leap in the development of radio-electronic means for various purposes and a significant expansion of their functional capabilities has been outlined. Such significant transformations are associated with two main factors. The first is the formation (creation) of single integrated information and control systems (structures) based on previously separated individual types of radio-electronic means (radio communication, radar, radio navigation, etc.). The second is a significant increase in the conflict resistance of both the specified integrated systems in general and the components of their separate specialized radio-electronic means.

In such conditions, the conflict as a form of interaction of radio-electronic systems will be a process of conflict of interests of at least two very complex multi-level goal-oriented systems, which form an even more complex conflict super-system (or meta-system) during interaction. At the same time, individual elements (subsystems) of each of the opposing systems are united by a single general goal of the system as a whole and are not completely "independent", but complement and mutually "help" each other. Therefore, the confrontation of the opposing parties in modern conditions during the conduct of the ERB acquires all the characteristic features of a complex coalition conflict.

A somewhat conventional structure of one of the variants of a complex antagonistic conflict is presented in Fig. 1.

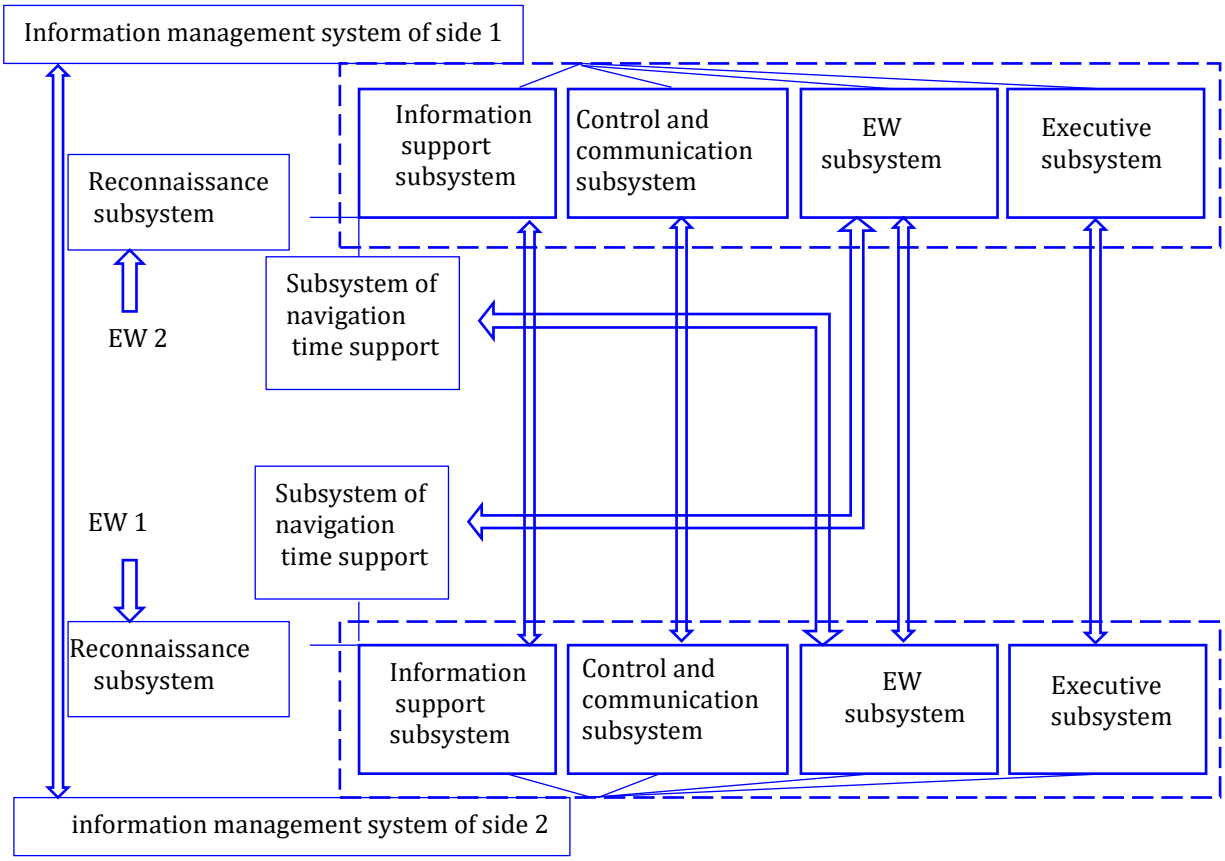

Figure 1: The structure of one of the variants of a complex antagonistic conflict

Based on the above general provisions and components of EW, it is possible to specify the conflict interaction (influence) of the EW system with other information systems,

depending on the specifics of their purpose, construction, and functioning. In the classical sense, EW is carried out about military, dual, and special purpose systems. Although its potential application does not exclude systems of another purpose.

Here is a list of such conflicts:

Terrestrial radio communication—EW system.

Satellite communication—EW system.

Radio relay communication—EW system.

Office Wi-Fi—EW system.

Radio communication based on distant tropospheric propagation—the EW system.

The ground radar complex (system)—the EW system.

The air-based radar complex (system)—the EW system.

The ship's radar complex (system)—the EW system.

The space-based radar complex (system)—the EW system.

Missile attack warning radar systems (in the USA this system is called a nuclear missile strike warning system, its purpose is to detect warheads of strategic ballistic missiles)—EW system.

The ground complex (system) of radio reconnaissance—the EW system.

The airborne complex (system) of radio reconnaissance—the EW system.

The space-based radio reconnaissance complex (system)—the EW system.

The ground complex (system) of radio technical reconnaissance—the EW system.

The aerial complex (system) of radio technical reconnaissance—the EW system.

The complex (system) of space-based radio-technical reconnaissance—the EW system.

The complex (system) of reconnaissance in the infrared range of space-based—the REB system.

The complex (system) of satellite radio navigation is the EW system.

The complex (system) of radio technical reconnaissance based on UAVs is the EW system.

The UAV-based radio reconnaissance complex (system)—the EW system.

The complex (system) of radio-technical intelligence and visual surveillance based on UAVs—the EW system.

Each of these options has its specifics, but also certain common features. Each of them can be analyzed both separately and in combination.

3. Operating Conditions and Indicators of Radio Systems, Which Should Be Defined in the Conflict Model

Let's try to dwell on important factors (characteristics) that are relevant to most of the listed conflicting systems and situations both between the means of information collection and information transmission processes and in the conditions of radio-electronic warfare. These factors should appear in the formation and application of information conflict models. Among them: are interference, sensitivity of receivers, interference resistance, interference protection, secrecy of the information system, electromagnetic compatibility of information systems, and radio-electronic means. Let's consider them in more detail.

3.1. Interference as Electromagnetic Radiation

Interference as electromagnetic radiation of various origins is inherent in the operating conditions of radio-electronic means under normal conditions especially when conducting EW. Their main characteristics:

- The width of the interference spectrum Δf_i.
- The average (carrier) interference frequency f_i.
- The average interference power $P_{ave\,i}$.
- The maximum interference power $P_{max\,i}$.
- Minimum interference power $P_{min\,i}$.
- Peak interference factor $K_{\text{peak}\,i} = P_{max\,i}/P_{ave\,i}$ (or in dB $K_{\text{peak}\,i} = 10lg(P_{max\,i}/P_{ave\,i})$.
- The dynamic range of interference is the ratio of the maximum and minimum instantaneous powers $D_i = P_{max\,i}/P_{min\,i}$ (or in dB $D_i = 10lg(P_{max\,i}/P_{min\,i})$.

Depending on the location of the source of interference, internal and external interferences are distinguished.

Internal interferences arise in the system itself (noises of the input cascades of the receiver, receiving antenna, signal channel lines and electrical signals entering the receiver through internal circuits due to poor shielding or decoupling between cascades). The internal noise caused by the chaotic movement of charge carriers is fundamentally ineradicable, although it can be minimized.

Thermal and shot noise are distinguished.

Thermal noise is caused by the thermal movement of charge carriers. It is a Gaussian random process with zero mean and power spectral density in the radio frequency range:

$$N_0(f) = k_B\, T^o = N_0 \ (\text{V/Hz}), \quad (1)$$

where $k_B = 1{,}38 \times 10^{-23}$ (J/K) is the Boltzmann constant, T^o is the absolute temperature of the noise source (in Kelvin), f is the frequency.

Thermal noise can be interpreted as White Gaussian Noise (WGN) with a constant one-sided power spectral density:

$$N_0 = k_B\, T^o \quad (2)$$

and the Gaussian probability density distribution of instantaneous amplitude values *n*:

$$w(n) = \frac{1}{\sigma_n\sqrt{2\pi}} e^{-\frac{n^2}{2\sigma_n^2}}, \quad (3)$$

where σ_n is root mean square noise amplitude.

The graph of this distribution at different rms amplitudes is shown in Fig. 2.

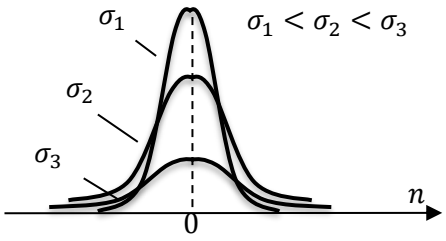

Figure 2: Distribution (3) graph at different rms amplitudes

The WGN autocorrelation function is the inverse Fourier transform of its power spectral density and is an δ-function.

In real systems, the frequency bandwidth is limited, and the power of the noise passing to the receiver input:

$$P_n = N_0 \cdot \Delta f_{\text{rec path}}, \quad (4)$$

where $\Delta f_{\text{rec path}}$ is receiving path bandwidth.

External interference. This is a fairly wide range of obstacles of various origins. There are two groups among them: unintentional and intentional. They, in turn, include several subgroups. Depending on the range of frequencies and conditions in which the information system works, one or another type of interference prevails.

Unintentional include natural, inter-system (industrial and from third-party radio equipment), and intra-system.

Natural disturbances arise due to various electromagnetic processes occurring in the troposphere, ionosphere, and outer space, as well as due to radiation from the earth's surface. Accordingly, there are atmospheric (tropospheric) interferences, cosmic interferences (present in frequency ranges above 30 MHz)—and cosmic noises from interstellar gases, the Sun, and radio stars of Jupiter. Obstacles from the earth's surface; it, like any heated body, emits electromagnetic waves (the power of these noises at the receiver input is determined by the orientation and shape of the antenna's directional pattern, as well as the temperature and characteristics of the surface). According to their statistical characteristics, they are similar to thermal noise.

Intersystem interference (industrial and from third-party radio equipment). They are created by various radio stations (station interference), industrial installations, medical equipment, electric motors, etc.

Industrial interference is created by various electrical equipment of industrial enterprises, transport, power transmission lines, and other electrical installations. More often, they are sequences of pulses with a constant or variable follow-up period. Spread in the atmosphere and along cable lines. The level of industrial interference depends on the location of the receiver of industrial facilities and the power of electrical equipment.

Interference from third-party radio equipment (station interference) is one of the most common types of external interference. The saturation of radio means (radio communication, radar, radio navigation, etc.) is constantly growing. Therefore, the loading of radio bands is such that very often interference from third-party radio equipment exceeds other types of interference. Station interference is due to various reasons. Their minimization is related to compliance with the provisions of electromagnetic compatibility of radio-electronic devices.

A simplified physical model of the formation of station interference at high channel loading can be presented in the form of a series-connected white noise generator and a filter with a frequency response that varies over time according to a random law.

The spectral density of interference power $N(f,t)$ as a random process (often non-stationary) can be sufficiently fully characterized by the probability density $w_{f,t}(n)$ and the correlation functions (preferably normalized) of fluctuations in the time and frequency domains $r_n(\tau)$ and $r_n(f)$. The parameters of the correlation functions are the time correlation interval and the frequency correlation interval.

If the number of station interferences falling into the signal band is limited, then the mixture $x(t)$ entering the receiver input is represented as the sum of the useful signal $S(t)$ and a limited number of additive interferences with known or unknown statistical characteristics:

$$x(t) = s(t) + n(t) + \sum_{k=1}^{M_i} \gamma_k(t), \quad (5)$$

where M_k is the number of sources of interference, $\gamma_k(t)$ is the external interference, the frequency spectrum of which falls into the bandwidth of the receiver, $n(t)$ is the WGN.

Intentional interference is a more important process in the implementation of EW. Therefore, their characteristics need to be carefully considered when creating a conflict model.

Deliberate disturbances are created with the help of special devices—troublemakers to disrupt the operation of the information system. From the point of view of the nature of the influence on the functioning of the system against which the interference acts, they are divided into noise-like and imitative.

Noise-like ones are designed to worsen signal reception conditions by creating an increased interference background at the receiver input. According to the method of formation, they are divided into direct noise (direct noise process) and harmonic processes modulated by noise. According to the relationship with the parameters of the useful signal, which they counteract, these types of interference are divided into blocking, narrowband, and targeting.

Blocking interference has a spectrum width that is significantly greater than the signal spectrum width at approximately the same average frequencies of the interference and the signal: $\Delta f_i >> \Delta f_S$.

Narrowband interference has a spectrum width that is significantly smaller than the signal spectrum width, provided that the interference spectrum falls into the signal frequency band: $\Delta f_i < \Delta f_S$.

Aiming interference has a spectrum width that coincides with the signal spectrum width, provided that the average (carrier) frequencies of the interference and the signal coincide: $\Delta f_i = \Delta f_S$.

The latter interferences are the most effective because all the power of the interfering transmitter is concentrated in the band of the receiver that is being suppressed. But for this, you need to monitor the operating frequency of the receiver and estimate or predict (by observing the signals of the system to be suppressed using electronic reconnaissance).

The total power of the interference perceived by the receiver is convenient to estimate in the frequency plane, knowing the power spectral densities of each of the interferences at the location of the receiver. In the general case, with a rectangular amplitude-frequency characteristic of the receiving path:

$$P_{\Sigma\, rec} = K_n \cdot \int_{f_{min}}^{f_{max}} \left[\sum_{k=1}^{M_k} N_k(f) \right] df \quad (6)$$

where K_n is a receiver noise ratio (>1), f_{min} is the minimum bandwidth frequency of the receiving path, f_{max} is the maximum bandwidth frequency of the receiving path, $N_k(f)$ is the power spectral density of the i^{th} interference, M_k is the number of interferences.

When the spectral densities of interference powers in the reception band are uniform, the formula is simplified:

$$P_{\Sigma rec} = K_{Ш} \cdot \Delta f_{rec} \sum_{k=1}^{M_k} N_k(f) \quad (7)$$

where Δf_{rec} is the bandwidth of the receiving path.

In all cases, the jamming side (carrying out radio-electronic suppression) aims for the total power of the frequency components of the interference within the receiver's bandwidth to exceed the signal power. That is, the ratio of the signal power to the power of the interference(s) was as small as possible one—$P_S/P_{\Sigma rec} << 1$. In this case, the purpose of EW

will be achieved if the system against which suppression is carried out is not equipped with sufficient means of protection against interference.

In addition to continuous ones, there are interferences in the form of pulse sequences, as a rule, with a chaotic structure in terms of the follow-up period, duration, and shape of pulses. As a rule, these are obstacles of artificial origin. They can be unintentional or intentional.

Simulating deliberate interference is intended to misinform. By structure and parameters, they repeat the signal, so they are perceived as a useful signal, but carry false information.

The above-mentioned interferences (noise-like and imitative) are also used to protect information systems by setting such interferences to systems and means of information interception. That is, there will be a counter-conflict with the use of EW methods.

3.2. Sensitivity of Receivers

Means of radio-electronic intelligence as part of EW systems and means against which radio-electronic suppression is carried out function in the presence of unintentional interference (internal noise of radio-electronic devices, atmospheric and space noise, industrial interference, intersystem interference, etc.). Their presence and intensity at the input of the corresponding receiving devices depends on the selected range of electromagnetic waves, the time of day and season, the width of the interference spectrum, the location of the devices, the characteristics of the antennas, etc. The level of these interferences determines the sensitivity of receivers—$P_{rec\,min}$ means of radio-electronic reconnaissance, means of communication, radars, and radio navigation receivers. It is impractical to have the $P_{rec\,min}$ value less than the total power of the most characteristic unintentional interference at the receiver input (noise background), which should exceed the power of the expected useful signal. As a rule, the situation is non-stationary and creates a "micro-conflict" between the receiving component of the system and the interference background.

3.3. Interference Resistance

Interference resistance—is the ability of the system to perform its functions in the presence of disturbances with quality indicators not lower than the established ones. This means the presence of not only the noise background mentioned above but also a certain level of interference from another origin.

Interference resistance depends on modulation, reception method, coding methods, etc. Quantitatively, the interference immunity of discrete message transmission systems can be characterized by the probability of error P_{err} at a given ratio of average signal power and interference at the input of the system receiver.

3.4. Interference Protection

Interference protection is the ability of the system to counteract the harmful effects of interference and to perform its functions with quality indicators not lower than those specified under the conditions of interference. Interference protection can be provided by active and passive methods.

Active methods consist of counteracting the functioning of the source of interference. If the source creates interference unintentionally, organizational and technical measures are taken to turn off the source or eliminate defects in its operation that led to the unauthorized creation of interference. If the source creates a deliberate disturbance, then decisive measures are taken to destruction using destruction (for example, in military conflicts).

Passive methods consist of the application of additional methods and devices of signal formation and processing, which are used when the interference situation worsens:

- Switching to another operating frequency, where the level of interference is lower.
- Switching to a signal with a more interference-resistant type of modulation; increase in radiation power.
- A decrease in the technical speed of transmission (which is equivalent to an increase in the duration of the signal, which means its power).
- Moving to fault-tolerant code with higher error detection or correction capabilities.

- Rejection of frequency components of interference (if its spectrum is narrower than the signal spectrum) using appropriate filters.
- Application of methods of narrowing the directional diagrams of transmitting and/or receiving antennas [12–15], when the direction of arrival of the interference and the useful signal are different, it is possible to change the orientation and/or shape of the directional characteristic of the receiving antenna in such a way that it reduces the intensity of the interference at the input of the receiving device under the condition of a slight decrease in the level of the useful signal.
- Readjusting the polarization of the receiving and transmitting antenna [16–17] (if there is a difference in the polarization of the useful signal and the interference).

In modern systems, the listed methods are mostly implemented in adaptive mode.

3.5. Secrecy of an Information System

The secrecy of the information system is the ability to perform its functions in such a way that the opposing party does not have the opportunity to obtain information about the operation of the system, its characteristics, and the information circulating in it. Three main levels of secrecy are considered: energetic, structural, and informational.

Energetic secrecy (also called absolute) is the kind of secrecy in which the opposing party is unable to detect the very fact of the system's operation and detect its signals against the background of existing disturbances; such stealth is achieved by using complex (noise-like) signals, and in some cases also by creating an increased level of interference in the city where the receiving means of the opposing side are located.

Structural secrecy is the type of secrecy in which the adversary can perceive the information system signal, but cannot distinguish it from other signals or determine its structure and identify the symbols of the message; this is achieved by various methods: the emission of false signals, the transmission of separate component signals and messages at different frequencies and through different channels, etc.

Measures to ensure energy and structural secrecy contribute to the increase of Interference protection of the information system because they will deprive the opposing party of information about the parameters of the signal, thereby reducing its ability to create intentional interference with the appropriate parameters.

Information secrecy is such secrecy in which the adversary can perceive the IS signal, distinguish it from other signals, determine its structure, and identify the symbols of the message, but cannot determine the content of the message, that is, information; such secrecy is achieved by cryptographic methods.

The presence and high level of interference resistance, interference protection, and secrecy are components of the conflict resistance of a tool or system. Therefore, the task of radio-electronic reconnaissance consists of overcoming secrecy, and radio-electronic suppression consists of reducing Interference resistance and Interference protection both by creating additional interference and by other methods.

3.6. Electromagnetic Compatibility of Information Systems and Radio-Electronic Means

Electromagnetic compatibility of information systems and radio-electronic means their ability to function together in real operating conditions with specified quality indicators without creating unacceptable interference with each other.

The conditions of propagation of radio waves, energy loss in the environment, loss of signal power in the equipment, the shape of the characteristics of the directionality of the antennas, and their polarization characteristics about the polarization of the radio wave have a noticeable influence on the operation of information systems and electronic warfare systems. These factors affect such an important indicator of radio systems as the operating range.

For example, the range of radio communication, radio and radio technical intelligence, and radio navigation in ideal conditions (against the noise background and the orientation of the antennas with the

maxima of the directional characteristics towards each other):

$$R_{con.max} = \sqrt{\frac{P_{trans} \cdot G_{trans} \cdot G_{rec} \cdot \lambda^2}{(4\pi)^2 \cdot P_{rec\,min}}} \quad (8)$$

where P_{trans} is a transmitter output power, G_{trans} is the maximum amplification factor of the transmitting antenna, G_{rec} is the maximum amplification factor of the receiving antenna, λ is the wavelength, $P_{rec\,min}$ is the sensitivity of the receiver, which is equal to the power of the background noise spread above.

To ensure sufficient reception quality (and ultimately the availability and integrity of information), the signal at the receiver input must exceed the noise level by a certain number of ν times. Then the communication equation (navigation, reconnaissance) will be:

$$R_{com.(\text{nav.recon.})} = \sqrt{\frac{P_{trans} \cdot G_{trans} \cdot G_{rec} \cdot \lambda^2}{(4\pi)^2 \cdot P_{rec\,min} \cdot \nu}} \quad (9)$$

Losses of signal energy during the propagation of waves in the environment and in the equipment, which are taken into account by the appropriate Γ_{prop} and Γ_{equip} coefficients and the arbitrary orientation of the antennas (Fig. 3.) lead to a decrease in range.

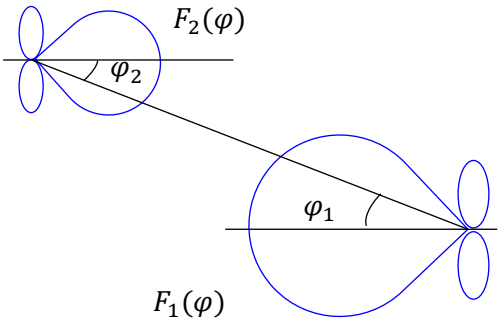

Figure 3: $F_{1,2}(\varphi)$ are directional diagrams in the horizontal plane of the object 1(2)

Then the range of radio communication (radio navigation, radio reconnaissance):

$$R_{com.(\text{nav.recon.})loss}(\theta,\varphi) = \sqrt{\frac{P_{trans} \cdot G_{trans}(\theta,\varphi) \cdot G_{rec}(\theta,\varphi) \cdot \lambda^2}{(4\pi)^2 \cdot P_{rec\,min} \cdot \nu \cdot \Gamma_{\text{prop}} \cdot \Gamma_{\text{equip}}}} \quad (10)$$

In the conditions of suppression using EW, the power of intentional interferences PN from the input at the receiver input will significantly exceed $P_{rec\,min}$.

$$P_{\text{intent.interf.input}} = \frac{P_{\text{trans.interf}} \cdot G_{\text{trans.interf}} \cdot G_{rec} \cdot \lambda^2}{(4\pi)^2 \cdot R^2_{\text{interf.}}} \quad (11)$$

where: $P_{rec.\text{interf}}$ is the output power of the interference transmitter, $G_{\text{trans.interf}}$ is the maximum amplification factor of the interference generator transmission antenna, R_{interf} is the distance to the interference generator.

Then the range of radio communication (radio navigation, radio reconnaissance) will become very small, and obtaining information may become impossible.

4. Conclusions

The so-called informational conflict is a key component of the conflict in the conditions of the modern electronic security system. The information conflict is understood as the process of combating radio-electronic means (systems) at the stage of obtaining information (data) about the opponent and its transmission to consumers and means (systems) of radio suppression, that oppose them. Today it can be considered that the outcome of the information conflict has a decisive influence on the outcome of the conflict in EW systems as a whole. Typical representatives of radio-electronic means include the most common and promising means of radio communication, radio-electronic intelligence, and promising types of air-space-based reconnaissance radar stations, which are the most traditional objects of radio suppression. At the same time, of course, it is determined that the objects of radio suppression themselves can be constituent elements of some higher hierarchical level systems, which indicates a known “subordination” of the information conflict.

Conflicting mutual radio suppression of electronic warfare means with radio communication means and means of obtaining information (radio-electronic reconnaissance, radar location, radio navigation) is an important component of information conflict. The specified factors, as well as the conditions of the surrounding environment, should be adequately taken into account in the complex model of the conflict of radio technical systems of the information space in the conditions of the action of EW systems against them.

Analysis of the current state of development of electronic warfare means allows us to assert the use of cognitive information technologies in the development of EW, in particular, artificial intelligence. As a result of the implementation of these technologies, these electronic warfare systems can learn and adapt to changing natural conditions and enemy tactics; and use a database of sensors and other sources of intelligence for analysis and forecasting in the management of these assets. However, the implementation of artificial intelligence technologies creates certain risks related to the sensitivity and quality of data, ensuring the confidentiality, availability, and integrity of information.

The direction of further work of the authors will be the formalization of the components and the creation of a model of the corresponding information conflict.

References

[1] V. Mikhalevich, Dictionary of Cybernetics, Main Editorial Office of USE (1989).

[2] H. Haken, Information and Self-Organization, A Macroscopic Approach to Complex Systems, Springer (1988). doi: 10.1007/3-540-33023-2.

[3] J. Thompson, Instabilities and Catastrophes in Sciense and Engineering, John Wiley & Sons (1982).

[4] S. Shevchenko, et al., Study of Applied Aspects of Conflict Theory in Security Systems, Cybersecur. Educ. Sci. Tech. 2(18) (2022) 150–162. doi: 10.28925/2663-4023.2022.18.150162.

[5] S. Shevchenko, et al., Conflict Analysis in the Information Security System: Subject, in: Cybersecurity Providing in Information and Telecommunication System Vol. 3421 (2023) 56–66.

[6] S. Shevchenko, et al., Game Theoretical Approach to the Modeling of Conflicts in Information Security Systems, Cybersecur. Educ. Sci. Tech. 2 (2023) 168–178. doi:10.28925/2663-4023.2023.22.168178.

[7] O. Pinchuk, et al., ICT for Training and Evaluation of the Solar Impact on Aviation Safety, 16th Int. Conf. ICTERI II (2020) 786–792.

[8] V. Semko, Conflict Model of the Interaction of Objects of Cybernetic Space, Probl. Inf. Manag. 2(38) (2012) 88–92.

[9] A. Bondarchuk, Model of Interaction of Information Systems in Conflict Conditions, Telecommun. Inf. Technol. 4(57) (2017) 34–42.

[10] R. Schlesinger, Principles of Electronic Warfare; Prentice-Hall Space Technology Series, Literary Licensing (2012).

[11] V. Tyravskyi, Ukrainian Servicemen Began to Successfully Destroy Russian Electronic Warfare Systems (2023). URL: https://foreignukraines.com/2023/12/07/ukrainian-servicemen-began-to-successfully-destroy-russian-electronic-warfare-systems/

[12] V. Astapenya, V. Sokolov, The Use of an Accelerating Lens to Increase the Efficiency and Interference Protection of Networks IEEE 802.11b, Zv'yazok 2 (98) (2012) 33–37.

[13] V. Astapenya, V. Sokolov, Modified Accelerating Lens as a Means of Increasing the Throughput, Range and Noise Immunity of IEEE 802.11 Systems, 10th Int. Conf. on Antenna Theory and Techniques (2015) 267–269. doi: 10.1109/ICATT. 2015.7136852.

[14] V. Astapenya, V. Sokolov, Experimental Evaluation of the Shading Effect of Accelerating Lens in Azimuth Plane, XI Anniversary International Conference on Antenna Theory and Techniques (2017) 389–391. doi: 10.1109/ICATT. 2017.7972671.

[15] V. Astapenya, V. Sokolov, D. Ageyev, Experimental Evaluation of an Accelerating Lens on Spatial Field Structure and Frequency Spectrum, IEEE Ukrainian Microwave Week (2020). doi: 10.1109/ukrmw49653.2020.9252755.

[16] V. Astapenya, V. Sokolov, Increasing the Bandwidth of Wireless Communication Channels Due to Polarization Effects in IEEE 802.11 Standard Networks, Zv'yazok 3(99) (2012) 36–40.

[17] V. Astapenya, V. Sokolov, Research Results of the Impact of Spatial and Polarization Value of the Antennas on Network Capacity of Wireless Channels Standard IEEE 802.11, IX International Conference on Antenna Theory and Techniques (2013) 172–174. doi: 10.1109/ICATT.2013.6650715.