Conflicting Subsystems in the Information Space: A Study at the Software and Hardware Levels

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

[1] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*
[2] *State University of Information and Communication Technologies, 7 Solomyanska str., Kyiv, 03110, Ukraine*

Abstract

The study of complex systems led to the development of the theory of conflicts, which allows for modeling and solving information conflicts between elements of information and cybernetic systems. This article is the next step of research in the field of information confrontation and describes the information conflict in the context of "object—object". Based on the analysis of scientific sources, the classification of conflicts at the "object-object" level is presented. It is determined that for information and cybernetic systems, they discussed developments in the theory of conflicts that have specific features for different levels. The definition of information conflict is proposed as a process of interference in the information space and/or information system of the opposite party to violate the confidentiality, reliability, and integrity of the opponent's information. The classification of information conflict is carried out according to the following levels: between the means of information collection and information transmission; as means of radio-electronic warfare between means of information influence for counteraction, protection, or intelligence; between general purpose software applications and information protection programs; between software and technical means of information protection; between communication channels of information networks and protocols of their functioning. For each of them, the types of conflict situations are presented and solutions are recommended through the analysis of scientific developments on this problem. It is proved that the theory of information conflicts in information and cyber security systems has an innovative character, strengthening the creation and development of new technologies for ensuring the integrity, availability, and confidentiality of information. The approaches considered in this study can be used in the training of specialists in the field of information and cyber security.

Keywords

Conflict, information conflict, information security systems, cyber system, cyber conflict, software conflict, conflict between software and hardware, electronic warfare.

1. Introduction

In a rapidly changing world, information about what is happening is becoming a central commodity in international relations [1]. This caused an information conflict between those who want to dominate the information space, and control and manage the processes taking place in it. The theoretical justification for the emergence of information confrontation was presented in the study [1], which emphasized the importance of using the most important means of communication and information technologies—satellite surveillance, direct communication, high-speed computers, and unique opportunities in the integration of complex information systems [2, 3]. It was information conflicts that arose as a result of the introduction of information technologies in various spheres [4–6].

CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2024, Kyiv, Ukraine
EMAIL: s.shevchenko@kubg.edu.ua (S. Shevchenko); y.zhdanova@kubg.edu.ua (Y. Zhdanova); v.astapenia@kubg.edu.ua (V. Astapenya); negodenkoav@i.ua (O. Nehodenko); s.spasitielieva@kubg.edu.ua (S. Spasiteleva)
ORCID: 0000-0002-9736-8623 (S. Shevchenko); 0000-0002-9277-4972 (Y. Zhdanova); 00000-0003-0124-216X (V. Astapenya); 0000-0001-6645-1566 (O. Nehodenko); 0000-0003-4993-6355 (S. Spasiteleva)

Information system conflict is related to the introduction or use of an information system that is perceived as inappropriate and as a threat to tasks, competencies, processes, values, and power relationships of individuals, groups, or organizations. IS conflicts are associated with resisting behaviors that express reservations in the face of pressure from change supporters seeking to alter the status quo by implementing an information system and related organizational changes [7].

Studying the applied aspects of the theory of conflicts in information and cybernetic security systems, the authors of the article [8] proposed to consider this problem in three contexts: "subject—subject," "object—object," "subject—object," and, thus, for each of them, define an information conflict.

Articles [9, 10] became a continuation of these studies, which describe the conflict in the context of "subject—subject" and present an analysis of the problem at four levels (Fig. 1): the level of the individual (criminal—user); business level (internal and/or external violator—company manager); state level (violators/hackers—state institutions, state officials); the level of international relations (states, a group of subjects/hackers—institutions and/or political leaders of another state). Some methods and models of solving these conflicts are defined, in particular, a game-theoretic approach.

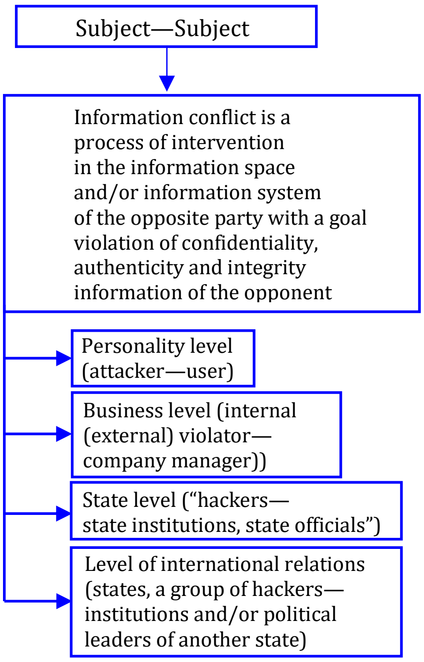
Subject—Subject
Information conflict is a process of intervention in the information space and/or information system of the opposite party with a goal violation of confidentiality, authenticity and integrity information of the opponent
Personality level (attacker—user)
Business level (internal (external) violator—company manager))
State level ("hackers—state institutions, state officials")
Level of international relations (states, a group of hackers—institutions and/or political leaders of another state)

Figure 1: Information conflict "subject—subject"

This study is the next stage of the analysis of applied aspects of the theory of conflicts and is devoted to the problem of modeling informational conflicts in the context of "object—object".

2. Conflicts Between Software and Hardware in Information and Cyber-Systems

Informatization of society requires increasingly complex and resource-intensive information technologies and tools.

Modern computer systems help to solve the most responsible tasks in various industries, in particular, in government institutions of critical infrastructure and defense departments. A computer system is a whole complex that contains both software and hardware, with the help of which processing, storage, protection, and transmission of data is carried out. Therefore, the computer system must be able to integrate with other information tools and programs to ensure the efficiency and speed of the management process.

Thus, the accumulation, improvement, and complication of various components of the computer system leads to the occurrence of undesirable situations in the process of its functioning, which leads to the emergence of information conflicts between the lost and the hardware.

The analysis of the literature [11–33] made it possible to identify the following characteristics of information conflict in the context of "object—object":

1. Information conflict is a clash, or incompatibility between the components of the information system at all stages of the implementation of new information technologies in the process of collecting, processing, transmitting, storing, and interpreting information about the state, intentions, and actions.

2. Information conflict in the context of "object—object" can be presented at the following levels: between means of information collection and information transmission processes; as Radio-Electronic Warfare (EW) between means of information influence for countermeasures, protection, or means of intelligence; between general

purpose software applications and information protection programs; between software and hardware information protection; between communication channels of information networks and protocols of their functioning (Fig. 2).

It is easy to recognize and predict the increasing capabilities of processing and exchanging information. It is much more difficult to catch the legacy of growing information capabilities, especially the interaction between them [1].

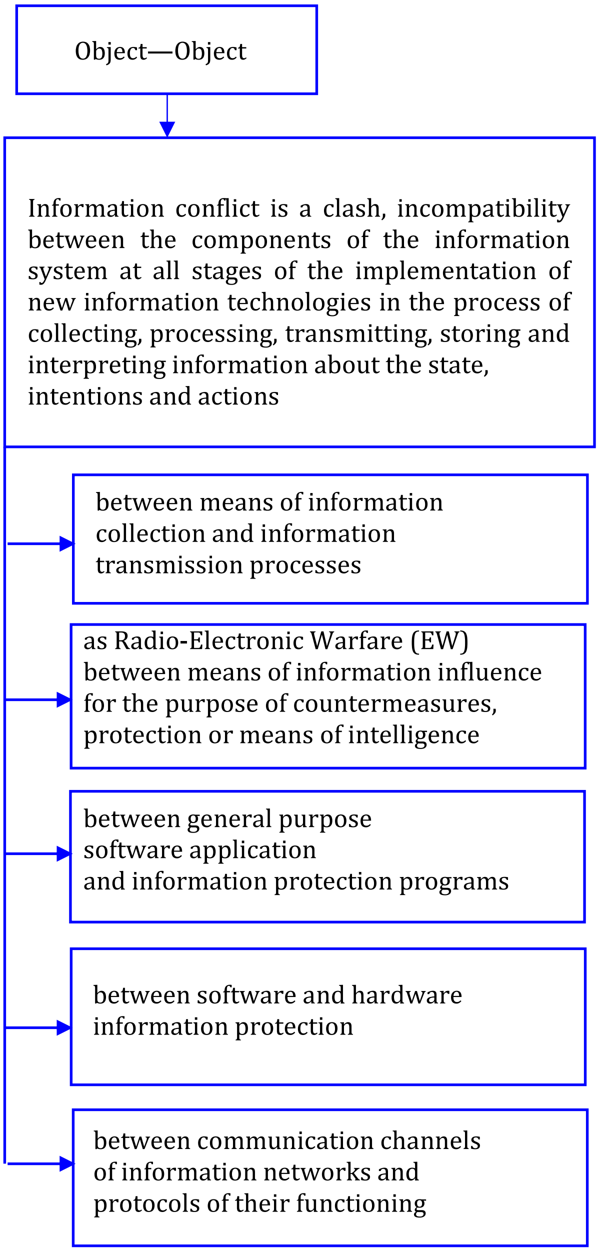
Object—Object
Information conflict is a clash, incompatibility between the components of the information system at all stages of the implementation of new information technologies in the process of collecting, processing, transmitting, storing and interpreting information about the state, intentions and actions
between means of information collection and information transmission processes
as Radio-Electronic Warfare (EW) between means of information influence for the purpose of countermeasures, protection or means of intelligence
between general purpose software application and information protection programs
between software and hardware information protection
between communication channels of information networks and protocols of their functioning

Figure 2: Information conflict "object—object"

2.1. Information Conflict Between the Methods of Collecting Information and the Processes of Transmitting Information

The process of extracting and collecting information requires a wide range of devices, means, and systems: from microphones, binoculars, and cameras to global radio astronomy systems, seismological monitoring systems, meteorological observations, and interplanetary scientific apparatuses. The choice of the specified devices means, and systems of collecting and extracting information, and methods of their application depend on the location of the monitored system, possible unmasking signs due to its design and the functions it performs, as well as on the purpose of the information collected about it, and goals set by the receiver (customer) of information.

The user for whom information is collected is usually located at a certain distance from the means (systems) that control the object or process. Therefore, an integral component of the information collection system is some data transmission system. In addition, the received data must be presented to the user in a form convenient for him (meet ergonomic requirements). The collection of information is carried out to make management decisions both about the objects, processes, and systems that are monitored and about the correction of the monitoring process itself. This involves human participation (which is also inherent in other categories of systems where information is needed to achieve a certain result). Thus, it can be assumed that we are talking about an ergatic system [34] of a higher level, the components of which are the information collection subsystem, the information transmission subsystem, and the message processing and presentation subsystem. To one degree or another, they are under the control and influence of the human consumer. It should also be remembered that the objects and processes that are subject to observation are components of some other system (let's call it the "controlled system" (S_C)), which is of interest to the user in terms of information. In the general case, the "controlled system" is not indifferent to monitoring it and will take measures to reduce the effectiveness of obtaining information about itself. Thus, the so-called Information Conflict (IC) takes place, which is a process of confrontation between the means (system) at the stage of obtaining information (information) about the S_C and its transmission to consumers and the S_C itself. The latter will take passive and active measures to prevent or minimize monitoring of it and access to the information it uses or transmits. Both systems are aimed at achieving their result. Today, it can be considered proven that the results of an information conflict have a decisive influence on the outcome of the conflict as a whole when the interests of certain systems collide (especially in the case of the possibility of conducting radio-electronic warfare, which will be discussed below).

Means and systems of information collection and its transmission, processing, and presentation to the consumer mainly directly or indirectly belong to the category of radio-electronic means and systems (EM, ES).

In a concise form, it is advisable to list them (without observing a certain hierarchy): radar systems of various purposes, systems of radio reconnaissance, radio technical reconnaissance, optical, thermal (in the infrared range), television, radiometric, hydroacoustic reconnaissance, magnetometric, seismic, acoustic, radiological, gravitational, embedded devices for eavesdropping and others.

Each of these systems and their components have their features of construction, work methods, and characteristics that must be taken into account when creating and analyzing a conflict model that is planned to be studied in the future.

Among the large number of tasks related to the assessment of the quality of the functioning of the mentioned means and systems, as well as the quality of their interaction with the consumer(s) of the received information (information exchange), at present, the task of conflict interaction of these means can be attributed to priority and systems:

- With the environment (physical fields that are determined by the objects and processes of observation and are used for observation and transmission of information; physical restrictions imposed by the environment during the implementation of observation and transmission of information: natural obstacles, attenuation of fields and signals, interference, refraction, diffraction, scattering, multipath propagation, Doppler frequency shift, etc.).
- Among themselves and with other third-party systems and means (unintentional interference and electromagnetic compatibility), as well as with Electronic Warfare (EW) systems. If we talk about electromagnetic compatibility, then for radio lines an important factor is the radio frequency resource and its distribution. From a physical point of view, the assignment of operating frequencies to one or another means depends on the functional purpose of the means(s), the characteristics of the propagation of radio waves of the relevant bands, the territorial placement of the means, and international and national regulatory documents. The functioning of the systems takes place in the conditions of disturbances, which will be discussed in the next section.

2.2. Information Conflict as Radio-Electronic Warfare (EW) Between Means of Information Influence for Countermeasures, Protection or Intelligence

Radio-electronic warfare (EW) is the use of radio frequency energy to provide advantages in the information space, as well as to protect one's radio-electronic systems from enemy influence [11]. EW is defined in NATO as: "Military actions using the electromagnetic spectrum, including the search for, interception and identification of electromagnetic radiation, the use of electromagnetic energy, including directed energy, to reduce or prevent enemy use of the electromagnetic spectrum and actions to ensure its effective use by friendly forces" [12].

EW covers a wide range of activities that include detection, jamming, and destruction of enemy radio-electronic means. The main components of EW are means of radio-electronic suppression, radio-electronic intelligence, protection against radio-electronic interference, and control of the radio frequency spectrum.

Electronic Attack (EA)—The use of electromagnetic energy, High-Energy Lasers

(HELs), and High-Power Microwave (HPM) devices or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires [13].

Electronic Protection (EP)—Actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability [13].

Electronic Warfare Support (ES)—Actions taken by, or under direct control, of an operational commander to search for, intercept, identify and locate, or localize sources of intentional and unintentional radiated electromagnetic energy for immediate threat recognition, targeting, planning, and conduct of future operations [13].

EA refers to the actions taken to prevent or reduce the enemy's effective use of the electromagnetic spectrum. EP involves actions taken to protect the effective use of the electromagnetic spectrum for friendly forces. ES comprises all those measures taken to detect, intercept, locate, and analyze sources of radiated electromagnetic energy. So, all of the three components of EW must be carefully integrated to be effective [14].

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 (Table 1).

In the process of interaction of relevant information systems, the following characteristics must be taken into account when developing models of information conflicts between them:

1. Interference as electromagnetic radiation of various origins is inherent in the operating conditions of radio-electronic means under normal conditions and especially when conducting radio-electronic warfare.
2. Sensitivity of receivers (the level of interference determines the sensitivity of receivers, so it is not advisable to have less total power of the most characteristic unintentional interference at the input of the receiver).

Table 1
A list of information systems that may conflict with radio-electronic warfare

Radio Electronic Warfare (EW)	- Terrestrial radio communication - Satellite communication - Radio relay communication - Radio communication based on distant tropospheric radio communication - Office Wi-Fi - Ground radar complex (system) - The radar complex (system) of the air base - Ship radar complex (system) - Space-based radar complex (system). - Missile attack warning radar system - USA: nuclear missile warning system - Ground complex (system) of radio reconnaissance - Aerial complex (system) of radio reconnaissance - Complex (system) of space-based radio reconnaissance - Ground complex (system) of radio technical intelligence - Air complex (system) of radio technical intelligence - Complex (system) of space-based radio-technical intelligence - The complex (system) of reconnaissance in the IR (infra) range of space-based - Complex (system) of satellite radio navigation - A complex (system) of radio technical intelligence based on Unmanned Aerial Vehicles (UAVs)
Radio Electronic Warfare (EW)	- UAV-based radio reconnaissance complex (system). - A complex (system) of radio-technical reconnaissance of visual surveillance based on UAVs

3. Interference resistance—the ability of the system to perform its functions in the presence of disturbances with quality indicators not lower than the established ones.
4. Interference protection—з Interference as electromagnetic radiation of various origins is characteristic of the operating conditions of RES under normal conditions especially when operating RES.
5. Secrecy of an information system is the ability to perform its functions in such a way that the adversary does not have the

opportunity to obtain information about the operation of the system, its characteristics, and the information circulating in it.
6. Electromagnetic compatibility of information systems and radio-electronic means.

The analysis of the literature [14–18] showed that at the current stage, the issue of improving EW with the help of artificial intelligence is being studied. In this direction, an AI-enabled EW system can be effective in identifying the hostile radar emitters to determine the extent of lethality of the threat. Then depending upon the threat perception, a suitable AI-based counter strategy can be formulated to nullify the hostile EW threat. Furthermore, the information gathered during radar signal analysis can be used to prepare a threat library to develop an Electronic Order of Battle (EOB) for situational awareness and develop flexible countermeasures as per the evolving EW scenario [14].

Along with this, there is a problem of inaccurate information, since the network is trained on a large database. Receiving false information in the process of training the network leads to negative consequences on the battlefield [16].

2.3. Information Conflict Between General Purpose Software Applications and Information Protection Programs

A software conflict occurs when programs cannot run on the same computer at the same time, meaning they have incompatible or conflicting code. This is usually due to a software bug and occurs when two programs compete for the same resource (memory, peripheral, register, etc.). It is possible to detect such a conflict most often during the execution process.

Research [19] is devoted to this problem. In their opinion, it is possible to classify such conflicts, which was proposed:

1. Unavailability or Inaccessibility of Shared Resources: Shared resources are often files, but also include other unique system resources such as network ports or C library function names.
2. Conflicts on Shared Data, Configuration Information, or the Information Flow Between Programs.
3. Interactions between Packages: In some cases, a package a using another package b makes a previously undetected fault in b evident; it is possible that other use cases for b could produce the same problem, so the failure can (at least in theory) be reproduced using b.
4. Package Evolution Issues. Problems in this category arise due to incorrect or outdated meta-data.
5. Spurious Conflicts: The last category represents cases where two packages are incorrectly classified as conflicting, although there is no conflict, at least not for the current version of these packages.

The resolution of these conflicts is different for each option. For example, the study [20] proposes an approach based on pre-trained language models to detect conflicts in software.

In the future, we will consider the confrontation between the software responsible for the operation of the product and the software responsible for the protection of information.

The authors of the study [21], characterizing these types of conflicts, proposed four types:

1. IS implementation process conflicts.
2. IS task conflicts.
3. IS structure conflicts.
4. IS value conflicts.

This study emphasizes that the types of information security conflicts that arise are based not only on the technical and functional characteristics of the system but also on insights gained from actual interaction with the new technology in specific organizational settings.

Information conflict in cyber security systems is usually related to ensuring the confidentiality, availability, and integrity of information.

Access control is a fundamental element of cybersecurity that allows you to determine who can access certain data, applications, and resources, and under what conditions. The simplest form of access control is identifying a user based on his credentials and then granting him the appropriate level of permissions [22].

A restriction conflict is a mismatch between an access control policy and the restrictions defined to restrict that policy. For example, a policy that allows an object with high integrity to access data with low integrity violates an integrity constraint. Constraint conflicts differ from typical policy conflicts in that the constraints must never be violated. That is, a conflict with a constraint results in a policy compilation error, while policy conflicts are resolved at runtime [23].

The emergence of an information conflict in software is possible as a result of the implementation of a threat (malware), which affects the functioning of the information system. Our comparison in the previous section presents that there is a limited available methodology to observe and provide requirement engineering to security and privacy together and there are no widely acceptable tools to help design and engineering privacy. there are also no specific techniques to deal with identifying and implementing privacy requirements [24].

Article [25] presents the definition of a conflict situation at this level, as conflict situations are such state of the system in which the possibility of correctly performing at least one of the system tasks (access control, information transfer, encryption, generation, and verification of the signature) due to external influence, or internal failures, errors or failure of software or algorithmic support is excluded. Conventionally, conflict situations can be divided into three categories as a result of:

- Distortion of the input (received) data stream (documents).
- Changes in the system functioning through external intervention (unauthorized access, intentional changes in software, or algorithmic support of the system).
- Distortion of the system functions when the input data flow changes (viruses, Trojan horses, errors, and software bookmarks).

It is known that installing two antivirus programs can also interfere with each other's work and cause a conflict, as one program may see the other as malware.

2.4. Information Conflict Between Software and Hardware Information Protection

Hardware and software are two interconnected and complementary elements of an information system. Information processing hardware is a complex of technical means, the components of which are electronic and electronic computing devices necessary for the functioning of the information system, software is a set of programs of the information processing system and program documents necessary for the operation of these programs. Without software, hardware is useless; and without hardware, software cannot run. From the point of view of information security, this part has the largest number of information conflicts. Thus, a malicious touch screen can record user actions, monitor the phone and install applications, direct the user to phishing websites, and exploit vulnerabilities in the operating system kernel to gain privileged control over the device [26].

Information conflicts between software and hardware are closely related to information conflicts in EW.

The modern state gave an impetus to the development of UAVs. Fig. 3 shows the basic model of the UAV and highlights information risks that create conflict situations between software and hardware. Information leakage: possible through ground controls (computer, programs, media, smartphone, tablet); through attacks on the source of supply; in foreign-made drones, the user does not have the opportunity to track the transmission of information to the manufacturer's servers, which contributes to the violation of information confidentiality.

The solution of such conflicts is proposed in works [27–30].

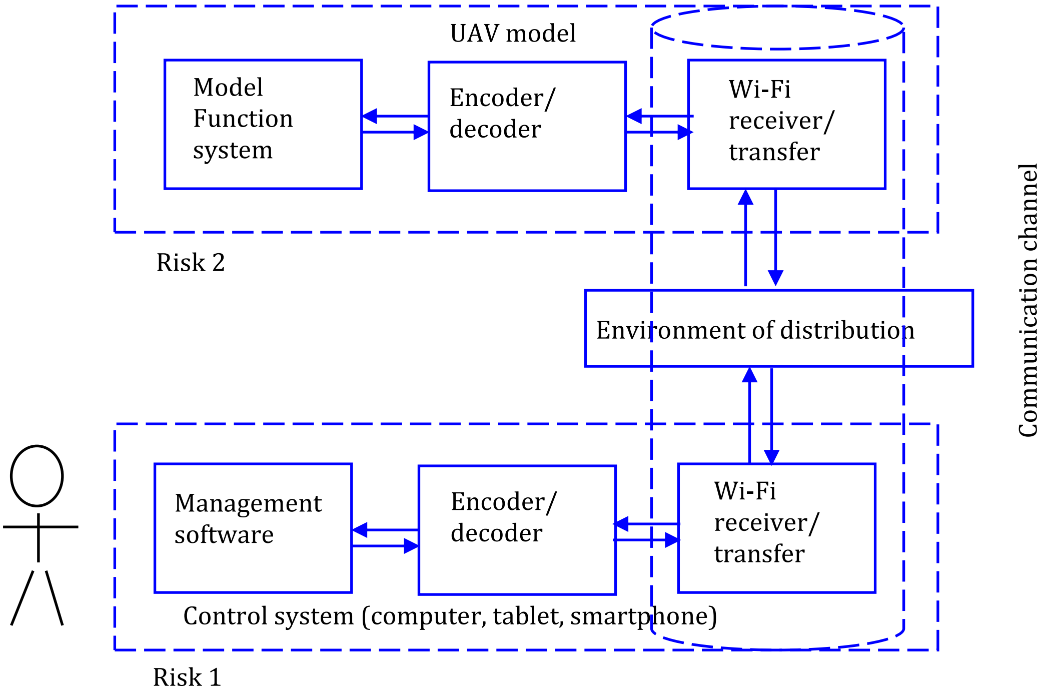

Figure 3: Information conflict between software and cyber security

3. Conclusions

This study is an attempt to carry out a possible classification of information conflicts in the "object—object" perspective in information and cyber security systems. Information technologies are developing very rapidly, so this problem will always be relevant and is obvious, often not solved.

Modeling situations of conflict interaction between the components of the information system allows us to predict fundamental changes in the development of the system to effectively manage this system. No matter what informational conflicts exist between system components, ensuring the desired strategy depends on human actions [31–33].

The vector of further research is planned to be directed to the modeling of conflict resolution scenarios from an "object—object" perspective in information and cyber security systems based on the analysis of existing approaches in the scientific literature.

References

[1] J. Nye Jr., W. Owens, America's Information Edge, Foreign Affairs 75(2) (1996) 20–36

[2] P. Anakhov, et al., Increasing the Functional Network Stability in the Depression Zone of the Hydroelectric Power Station Reservoir, in: Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, vol. 3149 (2022) 169–176.

[3] P. Anakhov, et al., Protecting Objects of Critical Information Infrastructure from Wartime Cyber Attacks by Decentralizing the Telecommunications Network, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3550 (2023) 240–245.

[4] H. Hulak, et al., Dynamic Model of Guarantee Capacity and Cyber Security Management in the Critical Automated System, in: 2nd International Conference on Conflict Management in Global Information Networks, vol. 3530 (2023) 102–111.

[5] V. Grechaninov, et al., Decentralized Access Demarcation System Construction in Situational Center Network, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3188, no. 2 (2022) 197–206.

[6] V. Grechaninov, et al., Formation of Dependability and Cyber Protection

Model in Information Systems of Situational Center, in: Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, vol. 3149 (2022) 107–117.

[7] A. Boonstra, J. Vries, Information System Conflicts: Causes and Types, Int. J. Inf. Syst. Project Manag. 3 (2015) 5–20. doi: 10.12821/ijispm030401.

[8] 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.

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

[10] S. Shevchenko, et al., Game Theoretical Approach to the Modeling of Conflicts in Information Security Systems, Cybersecur. Educ. Sci. Tech. 2 (22) (2023) 168–178. doi: 10.28925/2663-4023.2023.22.168178.

[11] EW (Radio Electronic Warfare)—what it is, its Essence, Definition, how it Works and Why it is Needed. URL: https://termin.in.ua/reb-radioelektronna-borotba/

[12] AAP-6 (2013): NATO Glossary of Terms and Definitions (English and French) (2013). URL: https://www.jcs.mil/Portals/36/Documents/Doctrine/Other_Pubs/aap6.pdf

[13] United States Chairman of the Joint Chiefs of Staff, Joint Publication (JP) 3-13.1, "Electronic Warfare" (2012). URL: https://info.publicintelligence.net/JCS-EW.pdf

[14] P. Sharma, K. Sarma, N. Mastorakis, Artificial Intelligence Aided Electronic Warfare Systems-Recent Trends and Evolving Applications, IEEE Access. 8 (2020) 224761–224780. doi: 10.1109/ACCESS.2020.3044453.

[15] I. Jordanov, N. Petrov, J. Roe, Radar Emitter Signals Recognition and Classification with Feedforward Networks, Procedia Comput. Sci. 22 (2013) 1192–1200. doi: 10.1016/j.procs.2013.09.206.

[16] Z. Davis, Artificial Intelligence on the Battlefield—An Initial Survey of Potential Implications for Deterrence, Stability, and Strategic Surprise, Center for Global Security Research Lawrence Livermore National Laboratory (2019). URL: https://cgsr.llnl.gov/content/assets/docs/CGSR-AI_BattlefieldWEB.pdf

[17] P. Gupta, P. Jain, O. Kakde, Deep Learning Techniques in Radar Emitter Identification, Defence Sci. J. 73(5) (2023).

[18] J. Pan, et al., Embedding Soft Thresholding Function into Deep Learning Models for Noisy Radar Emitter Signal Recognition, Electron. 11 (2022). doi: 10.3390/electronics11142142.

[19] C. Artho, et al., Why do software packages conflict?, 9th IEEE Working Conference on Mining Software Repositories (MSR) (2012) 141–150. doi: 10.1109/MSR.2012.6224274.

[20] R. Helmeczi, M. Cevik, S. Yıldırım, A Prompt-based Few-shot Learning Approach to Software Conflict Detection (2022). doi: 10.48550/arXiv.2211.02709.

[21] A. Boonstra, J. Vries, Information System Conflicts: Causes and Types, Int. J. Inf. Syst. Project Manag. 3 (2015) 5–20. doi: 10.12821/ijispm030401.

[22] What is Access Control? URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-access-control

[23] T. Jaeger, R. Sailer, X. Zhang, Resolving Constraint Conflicts, SACMAT'04: Proceedings of the Ninth ACM Symposium on Access Control Models and Technologies (2004) 105–114. doi: 10.1145/990036.990053.

[24] D. Ganji, et al., Conflicts Between Security and Privacy Measures in Software Requirements Engineering, Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security, CCIS 534 (2015) 323–334. doi: 10.1007/978-3-319-23276-8_29.

[25] R. Biyashev, S. Nyssanbayeva, Y. Begimbayeva, Development and Analysis of Possible Conflict Situations Resolution Systems in an Automated System, Comput. Sci. Res. 89 (2019) 182–184.

[26] O. Shwartz, et al., Inner conflict: How Smart Device Components Can Cause

Harm, Comput. Secur. 89 (2020). doi: 10.1016/j.cose.2019.101665.

[27] Y.-J. Chen, X.-C. Chen, M. Pan, Defense Against Machine Learning Based Attacks in Multi-UAV Networks: A Network Coding Based Approach, IEEE Trans. Netw. Sci. Eng. 9(4) (2022) 2562–2578. doi: 10.1109/TNSE.2022.3165971.

[28] E. Ntizikira, et al., Secure and Privacy-Preserving Intrusion Detection and Prevention in the Internet of Unmanned Aerial Vehicles, Sensors 23(19) (2023) 8077. doi: 10.3390/s23198077.

[29] V. Semko, et al., Model of Information Protection Management in the Information and Telecommunications System, Bulletin of the Lviv Polytechnic National University. Radioelectronics and Telecommunications (818) (2015) 151–155.

[30] V. Semko, The Use of the Method of Integral Truncation of Options when Solving Problems of the Conflict of the Interaction of Objects in the Space of Observation, Telecommun. Inf. Technol. 1 (2015) 59–66.

[31] V. Khoroshko, M. Brailovskyi, Management of Conflicts and Information Security Incidents on the Internet, Inf. Math. Methods Model. 2021. 11(1–2) 15–25.

[32] H. Haken, Information and Self-Organization a Macroscopic Approach to Complex Systems, Springer-Verlag (1988).

[33] A. Ivakhnenko, Origins of the theory of Ergatic Systems, Cybern. Syst. Anal. 11 (1975) 513–514. doi: 10.1007/BF01069 484.

[34] Dictionary of Cybernetics, Main Editorial Office of USE (1989).