ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

UDC 629.7.014-519:004.056 doi: 10.32620/reks.2023.4.11

Heorhii ZEMLIANKO, Vyacheslav KHARCHENKO

National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine

CYBERSECURITY RISK ANALYSIS OF MULTIFUNCTIONAL UAV FLEET SYSTEMS: A CONCEPTUAL MODEL AND IMECA-BASED TECHNIQUE

The subject of this study *is to ensure the cybersecurity of systems of multifunctional UAV fleets (SMF UAV).* ***The purpose of this study*** *is to identify and analyze the risks associated with the cybersecurity of multi-functional UAV fleets, develop models of threats, vulnerabilities, and attacks, and conduct IMECA analysis of cyber-attacks.* ***Tasks:*** *1) analyze threats that may affect the security of multifunctional UAV fleets; 2) identify system vulnerabilities and their possible consequences in case of exploitation; 3) develop models of the system infrastructure and threats, vulnerabilities, and attacks, considering the specifics of the functionality and communication between system elements; 4) perform a risk-based analysis, identifying and classifying potential threats and their impact. The following results were* ***obtained****. The following results were obtained. 1. Cybersecurity threats to multifunctional UAV fleets are described and classified. 2. Identified and analyzed system vulnerabilities and their potential consequences. 3. Developed models of threats, vulnerabilities, and cyberattacks, considering the specifics of the UAV fleet. 4. Conducted a risk-based analysis, determined the level of threat, and developed recommendations for improving the cybersecurity of the UAV fleet based on the results of the IMECA analysis.* ***Conclusions.*** *The research emphasizes the importance of the developed model and tool for the detection and analysis of cyber threats to the SMF UAV. This allows increasing the cybersecurity and reliability of the system and ensuring timely response to cyber threats.* ***Areas for further research:*** *development of a model and method to consider the specifics of cyber threats and the technological characteristics of the SMF infrastructure; development and implementation of proactive protection tools in the context of combined cyber-attacks; and expansion of the scope of these tools in various industries, including smart cities.*

Keywords*: cybersecurity; multifunctional UAV fleets; threats; vulnerabilities; attack modeling; risk-based analysis; system security; IMECA.*

Introduction

Motivation

One of the most important goals of technology is to overcome obstacles and support human life. Fleets of unmanned aerial vehicles (UAVs) are a technology developed in this direction. Special attention is paid to tasks that affect human health and life. Another purpose of their use is the ability to perform operations that are beyond human capabilities, difficult to perform and inaccessible without the use of UAVs. UAVs or drones are increasingly used to perform specific missions (e.g., search operations), no longer as independent units, but as part of organized groups that can be called swarms (or fleets) [1].

The current development of UAVs defines a new stage in the strategy of using technology in defense, transportation, logistics, and other areas. The growing functionality and application of UAVs in various industries poses significant cybersecurity challenges.

As the use of UAVs increases, so do concerns about their safety and security. Potential risks include collisions, interference with other aircraft, and cyber-attacks that could lead to data leakage or unauthorized UAV control. These issues have led to a surge in research into UAV safety and security.

The systems of multi-functional UAV fleets are under increasing scrutiny because of their growing role in reconnaissance, surveillance, and navigation. In this context, ensuring cybersecurity is becoming a critical aspect for the efficiency and safety of such systems.

State of the art

The growing number of cyber-attacks on UAVs and their control systems requires a systematic approach to developing cybersecurity for UAV fleet systems. The dynamic nature of cyber threats and the constant evolution of technologies require continuous improvement of protection measures.

A fleet of UAVs is a group of unmanned aerial vehicles or flying robots working on a mission to achieve a specific goal [1]. UAV fleets have several advantages over individual UAVs. The entire system is flexible; therefore, the failure or loss of one UAV does not affect the performance of the entire system. The flexibility of the UAV fleet is greatly enhanced by the dynamic adaptation of different styles and configuration standards. Communication plays an important role in the management and coordination of the UAV fleet. The communication architecture describes how data are exchanged between UAVs or between UAVs and a central control center. With the development of UAV fleet technologies, one of the main challenges is to track drones in free space and monitor their status in spatial and temporal aspects.

In the world of advanced robotics, it is expected to overcome the limitations of individual robots and enable large groups to work together. This is inspired by animal behavior, where creation and outcome combine to achieve complex goals. Depending on the application paradigm, a complete and easily scalable UAV fleet is a collection of UAVs that can be increased or decreased in number [2]. The production of unmanned aerial vehicles is becoming cheaper, making them more affordable. The application of this technology is expanding, creating a variety of challenges in diverse areas such as agriculture, military operations, supply chain management, and rescue operations [3, 4].

There are many academic studies; for example, Hammoud et al. [5] presented the control and security of critical infrastructure, Falorka et al. [6] considered the visual inspection of buildings and structures, and Ahmad et al. [7] discussed the use of UAVs in the film and advertising industry.

One of the first papers in the field of UAV security was published in [8, 9]. This section provides an overview of the challenges and issues in UAV security, including the need for secure communications, data storage, and critical mission decisions.

In [10], the authors highlighted the security and privacy issues in UAV communication in flying disorderly networks, presented a broad overview of existing security mechanisms, including authentication, confidentiality, data integrity, and availability, and identified the limitations of these mechanisms. Similarly, the authors of [11] presented an overview of existing research on UAV security, including different types of attacks, vulnerabilities, and defense methods. They emphasized the importance of securing UAVs against cyber-attacks such as jamming, eavesdropping, and tampering.

In recent years, researchers have been actively investigating the security of UAVs in cloud environments. In [12, 13], the authors discuss the problems and security threats for UAVs in cloud environments, provide an overview of current solutions to address these problems, and identify prospects for future research.

During natural disasters such as floods, fires, earthquakes, and funerals, access to areas is difficult and rescue operations are delayed [14, 15]. Rescue operations are important to humanity because they involve the lives of living beings. The use of UAVs in rescue operations can speed them up. These small flying robots, equipped with various sensors such as cameras and night vision devices, can help assess large-scale disasters, search for and locate survivors, and search for targets. Aerial images can also be captured in real time and transmitted to ground stations for greater clarity and visualization; some UAVs are designed to carry several kilograms of emergency supplies. Fleets of drones can speed up search and rescue operations. In disaster areas, where cell phone coverage has been damaged, there is no reliable means of communication; a fleet of UAVs can provide a temporary communication channel, allowing survivors to interact with rescue teams [16].

UAV fleets are typically remotely controlled by a ground station (GS), which enables fully autonomous flight. Smartphones connected to cellular networks are an option for implementing ground stations. From a security perspective, UAV fleets are vulnerable to various intruder attacks because they are targets of wireless computer networks. These attacks can have serious consequences, including commercial and non-commercial losses. Disruptions to UAV fleets are typically carried out with malicious intent.

One of the main challenges is to ensure the cybersecurity of the UAV fleet. The study [17] emphasized the importance of encrypting transmitted information to ensure the security [18, 19] of the UAV fleet.

One of the most studied aspects of UAV cybersecurity is their vulnerability to GPS jamming and spoofing attacks [20]. Research confirms that UAVs that use commercial GPS systems for positioning are easy targets for jamming attacks [21]. In addition, the lack of encryption in commercial GPS systems exposes them to spoofing attacks [22]. Both types of attacks can lead to the failure or unauthorized control of critical components of the SMF UAV, posing significant risks to city infrastructure or other systems.

Despite the growing interest in UAV security, there is still a lack of attention to important aspects. Although there are numerous studies on UAV vulnerabilities, there is a gap in the study of cybersecurity of the digital infrastructure of the SMF related to data transmission in the UAV fleet. This aspect is critical for monitoring infrastructure and other objects.

Objectives and structure

The goal of this work is to develop models and a conceptual scheme of the SMF UAV infrastructure to ensure the cybersecurity of multifunctional UAV fleets and assess their reliability, considering functional states, security vulnerabilities, system degradation, and targets and types of intruders.

To solve this problem, it is necessary to:

– develop a conceptual model of the infrastructure and its components to study possible scenarios of cyber-attacks on the SMF UAV;

– formulate a mathematical description of models for the SMF UAV infrastructure;

– identify countermeasures and strategies to reduce risks and ensure effective cybersecurity of the SMF UAV;

– perform a consistent analysis of cyber threats using the IMECA methodology;

– provide recommendations for improving the resilience and security of multi-functional UAV fleet systems against potential cyber threats.

The paper has the following structure. The first section describes the methodology (principles and limitations) of the investigation. The second section covers a comprehensive conceptual model of the multifunctional systems of the UAV fleet with an emphasis on cybersecurity. It outlines the hierarchical infrastructure of the SMF UAV, emphasizing its coordination among systems, subsystems, components, and elements. It examines threat and vulnerability patterns and emphasizes the importance of cybersecurity measures (section 2). Threat of considers control channels, software, hardware, and data channels represented by the TSV matrix. It also discusses adversary and attack models, risk assessment, and IMECA analysis (section 3). Suggested countermeasures include standardized communication protocols and enhanced security techniques to address the vulnerability of SMF UAVs to cyber-attacks, emphasizing the need for effective cybersecurity strategies (section 4). Section 5 describes a case study including IMECA analysis for one of the UAV fleets and suggests countermeasures to decrease cybersecurity risks. The last section describes the novelty, main contribution, and directions of future investigations.

Methodology

The research methodology is based on the following three principles:

- the development of a component-hierarchical and theoretical-set description of SMF UAV as a complex cyber-physical system and an object of cybersecurity assessment and provision;

- risk-oriented analysis of the criticality of possible threats and attacks on the vulnerabilities of SMF UAV, considering the potential of violators/intruders using the modified IMECA technique that considers cybersecurity attributes, and

- determining a rational set of countermeasures.

Note that the analysis of functional safety was not considered within the scope of this study. The functional safety of these systems is defined as a property that minimizes the risks of transition to a critical state when UAVs or their fleets are threats to other systems or people and minimizes the consequences of such transition. System critical failures can be caused by physical faults and cyber-attacks on internal and communication assets.

Safety analysis methods for such systems are based on the well-known FMECA/FMEDA [23] and modern SISMECA [24] techniques and their modifications.

1. Conceptual model of multi-functional fleets of UAVs

1.1. Structure of MFF-UAV

The conceptual framework for the SMF UAV is a system-within-a-system (SWS) architecture that maximizes the utility of the larger system and understands the function, interaction, and use of each small component. This design approach helps to consider the system as a whole and focuses on the interaction of components, their function in the time dimension, and their function in the context of a larger evolving system that can be scaled to meet missions and situations [25, 26].

On the basis of this analysis, Figure 1 illustrates a diagram that conceptualizes the overall structure of the system and the interaction between its components (UAV fleets, charging stations, databases, cloud storage, communication centers, operators, satellites, mobile charging stations, and other components). These components play a key role in the operation and management of the system. The focus is on the main aspects of interconnection and interaction with a multi-functional UAV fleet.

1. Charging stations: UAVs need to be recharged regularly; therefore, charging stations are an essential part of their infrastructure. These stations are used to recharge batteries and prepare the UAV for its next mission.

2. Databases: UAV fleet management involves the use of databases that store information about each vehicle, its characteristics, current status, flight history, and other data. These databases provide centralized management and monitoring of the UAV fleet.

3. Cloud storage: Cloud storage is used to store large amounts of data, such as videos, photos, flight logs, and so on. They provide access to data from any device and ensure its security and availability.

4. Communication Center: The communication center acts as an integral link between the operator and the UAV, providing commands and feedback. It is responsible for monitoring and controlling the UAV fleet and ensuring reliable communication and data transmission.

5. Operator: Operators are responsible for managing and controlling UAV fleets, using specialized devices such as tablets to monitor flights, process data, and perform necessary operations. Operators also interact with other systems and components to make decisions based on the data they receive.

6. Satellites: UAV fleets can use satellites for global positioning, navigation, and data communications, providing precise location and long-range data transmission.

7. Mobile charging stations: In addition to stationary charging stations, UAV fleets can use mobile charging stations to quickly charge remote vehicles, providing flexibility and mobility.

8. Communication Control Points: In some cases, UAV fleets can use Communication Control Points to ensure communication and transmission in specific areas or over long distances.

These system components and elements provide the necessary infrastructure to manage, control and organize the SMF UAV in various scenarios and operations. Their interaction contributes to the effective use and management of UAVs, ensuring their reliability, safety and efficiency.

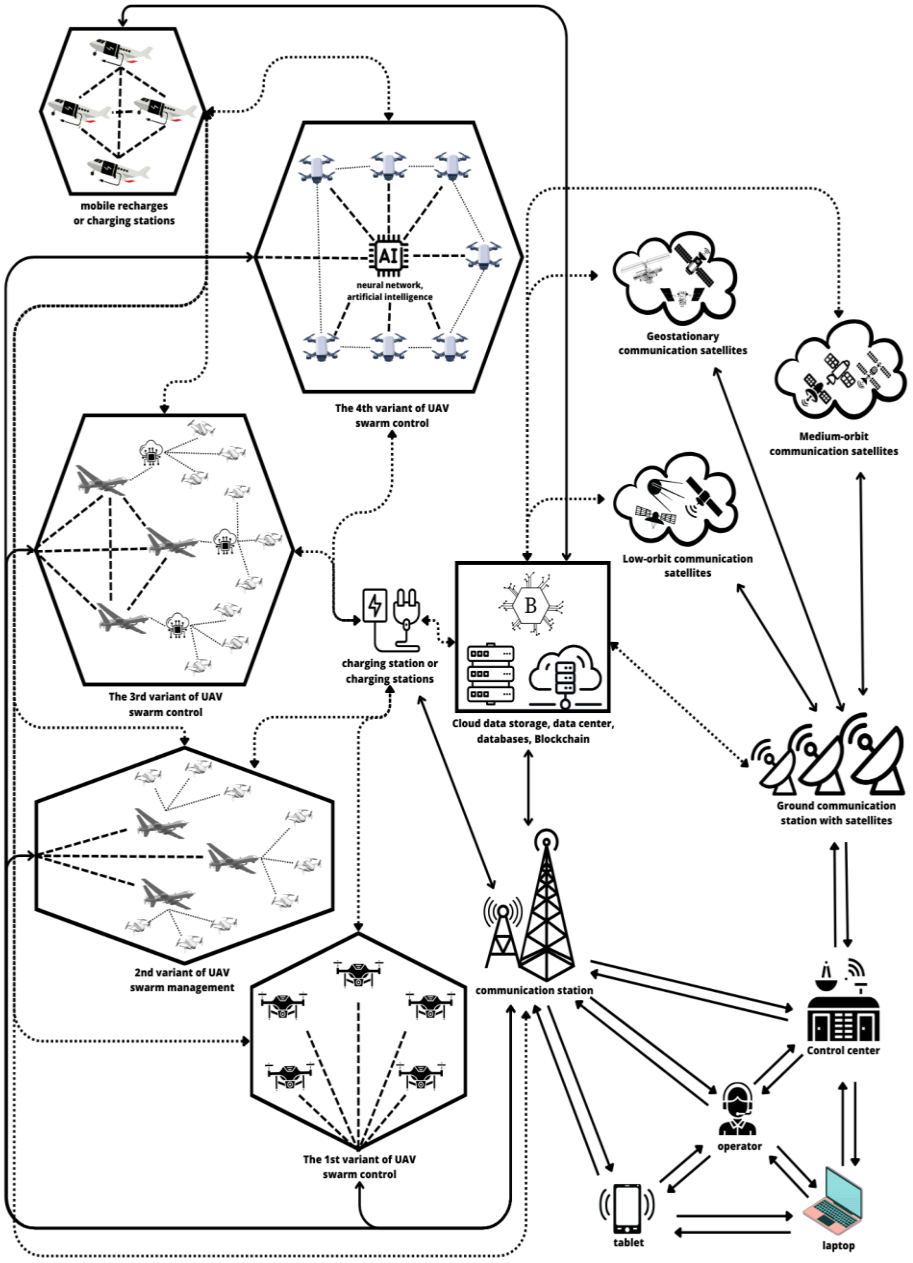

Fig. 1. Conceptual model of a system of multifunctional UAV fleets

1.2. Hierarchical model

The hierarchical model of the SMF UAV infrastructure provides a structure consisting of different levels: systems, subsystems, components and elements, as shown in Figure 1. Each level interacts with the lower levels to form a comprehensive infrastructure for the operational management of UAV fleets, Figure 2.

At the top level are systems that integrate multi-functional UAV fleets, define commonalities, and interact with certain aspects of management and security. The next level of subsystems comprises groups of interconnected components that collectively perform specific functions and provide specific aspects of UAV fleet management and surveillance.

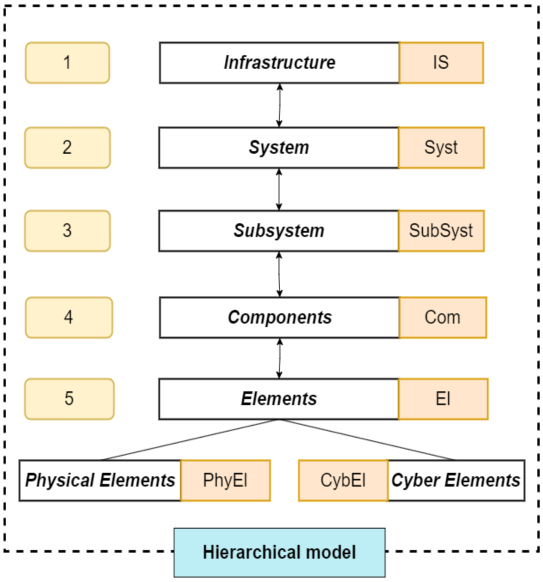

Fig. 2. The hierarchical model of the SMF UAV

Components and elements are the lowest level of infrastructure and the individual physical parts that make up a subsystem. They can perform various functions such as data collection and transmission, motion control and stabilization, and communication with control centers and other UAVs. The interaction between different levels of infrastructure maximizes the potential functionality and efficiency of a multi-functional UAV fleet in performing different tasks and missions. The hierarchical infrastructure model includes both cyber and physical elements. The interaction between these elements defines the structure and ensures the effectiveness of the system as a whole.

This hierarchical infrastructure model provides a high level of coordination and management in a multi-functional UAV fleet, balancing the interconnections between different levels of the system. The interaction between components creates the ability to effectively detect and respond to complex attacks, increasing the cybersecurity and reliability of the UAV fleet in various scenarios.

1.3. Theoretical-set description of the infrastructure of the SMFF UAV

In the above theoretical description of the infrastructure of the multifunctional UAV fleet, according to subsection 1.2, the system is represented as a set of different sets: systems, subsystems, components, and elements, as shown in Figure 2. The following notations are used to form mathematical sets and define the names of infrastructure elements in the SMF UAV:

1) IS – infrastructure;
2) Syst – systems;
3) SubSyst – subsystems;
4) Com – components;
5) El – elements.

These notations make it possible to create a systematic structure and establish relationships between different elements by applying mathematical operations to sets:

– IS – a set of infrastructure facilities:

$$IS=\{Syst_i, L_i\}, \qquad (1)$$

where Syst$_i$ – systems that are part of the infrastructure according to Fig. 1, L_i – a set of links between systems that can have both cyber and physical links. The matrix of connections can be written in the form of a matrix, where the element L(i, n) corresponds to the presence of a connection between system i and system n:

$$L_{IS}=\begin{array}{cc} & \begin{array}{ccccc} Syst_1 & \cdots & Syst_i & \cdots & Syst_n \end{array} \\ \begin{array}{c} Syst_1 \\ \vdots \\ Syst_i \\ \vdots \\ Syst_n \end{array} & \begin{bmatrix} - & \cdots & L_{1,i}^{cyber}, L_{1,i}^{phys} & \cdots & L_{1,n}^{cyber}, L_{1,n}^{phys} \\ L_{i,1}^{cyber}, L_{i,1}^{phys} & \cdots & - & \cdots & L_{i,n}^{cyber}, L_{i,n}^{phys} \\ L_{n,1}^{cyber}, L_{n,1}^{phys} & \cdots & L_{n,i}^{cyber}, L_{n,i}^{phys} & \cdots & - \end{bmatrix} \end{array}, \qquad (2)$$

where $L_{IS_{b,q}}$ – the relationship between elements b and q of the IS component described by two (cyber and physical) components:

$$L_{IS_{b,q}}=\{L_{ib,iq}^{cyber}, L_{ib,iq}^{phys}\}, \qquad (3)$$

this connection can be described using four codes:

$$L_{IS_{b,q}}=\begin{cases} 00, \text{ no cyber and physical connections;} \\ 01, \text{ only physical connections;} \\ 10, \text{ only cyber connections;} \\ 11, \text{ cyber and physical connections.} \end{cases}$$

– Syst – a set of system objects:

$$Syst_i=\{Syst_i^{cyber}, Syst_i^{phys}, F_i, L_{ij}\}, \qquad (4)$$

where $Syst_i^{cyber}=\left\{Syst_{ij}^{cyber}, j=1,2,\ldots,m\right\}$ – set of cyber systems, $Syst_i^{phys}=\left\{Syst_{ik}^{phys},k=1,2,\ldots,m\right\}$ – s the set of physical systems, and m is their number in the $Syst_i$ system. Examples of such systems are UAV fleets, communication centers, data storage centers, etc., where the set $F_i=\{F_{iv},v=1,2,\ldots,m\}$ – is a set of functions performed by the system depending on the tasks or goals, where m is their number in the $Syst_i$ system, and L_{ij} is the link between subsystems i and j in the system:

$$L_{Syst_i}=\begin{array}{c} \\ SubSyst_{i1} \\ \vdots \\ SubSyst_{ij} \\ \vdots \\ SubSyst_{in_i} \end{array} \begin{array}{c} \begin{array}{ccccc} SubSyst_{i1} & \cdots & SubSyst_{ij} & \cdots & SubSyst_{in_i} \end{array} \\ \begin{bmatrix} - & \cdots & L_{i1,ij}^{cyber},L_{i1,ij}^{phys} & \cdots & L_{i1,in_i}^{cyber},L_{i1,in_i}^{phys} \\ & & & & \\ L_{ij,i1}^{cyber},L_{ij,i1}^{phys} & \cdots & - & \cdots & L_{ij,in_i}^{cyber},L_{ij,in_i}^{phys} \\ & & & & \\ L_{in_i,i1}^{cyber},L_{in_i,i1}^{phys} & \cdots & L_{in_i,ij}^{cyber},L_{in_i,ij}^{phys} & \cdots & - \end{bmatrix} \end{array}, \qquad (5)$$

where $L_{Syst_{ib,iq}}$ – is the relationship between elements b and q of component $Syst_i$ described by two components (cyber and physical):

$$L_{Syst_{ib,iq}}=\{L_{ijb,ijq}^{cyber},L_{ijb,ijq}^{phys}\}, \qquad (6)$$

this connection can be described using four codes:

$$L_{Syst_{ib,iq}}=\begin{cases} 00, \text{no cyber and physical connections;} \\ 01, \text{only physical connections;} \\ 10, \text{only cyber connections;} \\ 11, \text{cyber and physical connections;} \end{cases}$$

– SubSyst – a set of subsystem objects:

$$SubSyst_j=\left\{SubSyst_j^{cyber},SubSyst_j^{phys},F_{ij}, L_{ijk}\right\}, \quad (7)$$

where $SubSyst_j^{cyber}=\left\{SubSyst_{js}^{cyber}, s=1,2,\ldots,m\right\}$ – set of cyber subsystems,

$SubSyst_j^{phys}=\left\{SubSyst_{jk}^{phys},k=1,2,\ldots,m\right\}$ – is the set of physical subsystems and m is their number in the subsystem $SubSyst_j$. Examples of such subsystems are UAVs, operators, satellites, etc., where the set $F_{ij}=\left\{F_{ijw},w=1,2,\ldots,m\right\}$ – is a set of functions that the subsystem performs depending on the system in which it is located (according to formula 4) and the tasks or objectives set, where m is their number in the subsystem $SybSyst_j$,

L_{ijk} – is the connection between infrastructure objects, where i is the system, j is the subsystem, k is the component located at different levels of the hierarchy, according to formulas 2 and 5, and where $L_{SubSyst_{ijb.ijq}}$ – is the link between elements b and q of component $SubSyst_{ij}$ described by two (cyber and physical) components:

$$L_{SubSyst_{ijb,ijq}}=\{L_{ijb,ijq}^{cyber},L_{ijb,ijq}^{phys}\}, \qquad (8)$$

this connection can be described by four codes:

$$L_{SubSyst_{ijb,ijq}}=\begin{cases} 00, \text{no cyber and physical connections;} \\ 01, \text{only physical connections;} \\ 10, \text{only cyber connections;} \\ 11, \text{cyber and physical connections;} \end{cases}$$

– Com – set of components:

$$Com_k=\{Com_k^{cyber},Com_k^{phys},L_{ijkp}\}, \qquad (9)$$

where $Com_k^{cyber}=\left\{Com_{kj}^{cyber}, j=1,2,\ldots,m\right\}$ – set of cyber components, $Com_k^{phys}=\left\{Com_{kc}^{phys},c=1,2,\ldots,m\right\}$ – is the set of physical components and m is their number in Com_k. Examples of components are e.g. sensors, actuators, navigation devices or applications for UAVs, etc. L_{ijkp} – is the connection between elements i, j, k, p of the multifunctional UAV fleet infrastructure according to formulas 2 and 5 and where $L_{Com_{ijkb,ijkq}}$ – is the connection between elements b and q of the Com_{ijk} component described by two (cyber and physical) components:

$$L_{Com_{ijkb,ijkq}}=\{L_{ijkb,ijkq}^{cyber},L_{ijkb,ijkq}^{phys}\}, \qquad (10)$$

this connection can be described by four codes:

$$L_{Com_{ijkb,ijkq}}=\begin{cases} 00, \text{no cyber and physical connections;} \\ 01, \text{only physical connections;} \\ 10, \text{only cyber connections;} \\ 11, \text{cyber and physical connections;} \end{cases}$$

– El – set of elements:

$$El_q=\left\{CybEl_q,PhyEl_q,L_{ijkp}\right\}, \qquad (11)$$

where $CybEl_q=\left\{CybEl_{qj}, j=1,2,\ldots,m\right\}$ – set of cyber elements, $PhyEl_q=\left\{PhyEl_{qk},k=1,2,\ldots,m\right\}$ – is the set of physical elements, and m is their number in El_i. Examples of elements are hardware and software components of devices.

This approach allows for more accurate and systematic tracking and analysis of the SMF UAV infrastructure in terms of cybersecurity and vulnerability to combined attacks.

2. Model of threats and vulnerabilities

2.1. Conceptual model

Cybersecurity is a set of measures, technologies, and strategies to protect information systems, networks, software, and data from unauthorized access, theft, destruction, loss, or modification [27, 28].

A conceptual security model (CSM) defines the key aspects of security in a system or organization, serves as a basis for designing and implementing security measures, and enables better understanding and management of risks and threats [29].

An information security (IS) management system (ISMS) framework for a UAS fleet is an organized plan for managing and securing information and data in a complex UAS fleet infrastructure. The IS of a UAV fleet includes measures to protect the confidentiality, integrity, availability, and observability of components and elements in the fleet system and infrastructure networks with which UAVs interact [30], Figure 3.

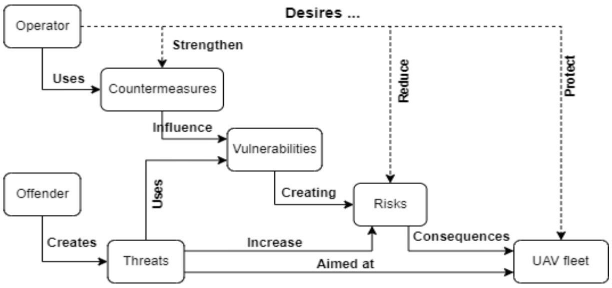

Fig. 3. Schematic of the ISMS in the SMF UAV

In accordance with the 27001:2022 standard, Figure 3 shows a diagram of the UAV fleet Information Security Management System (ISMS). This scheme defines key aspects of the fleet's infrastructure and system elements that help protect information from potential threats such as data leakage or privacy violations [30].

Based on the SMF UAV, Figure 1, and the ISMS, Figure 3, a threat classification and CSM was created that details potential attack scenarios for the SMF UAV. This model helps to track the actions of intruders, identify risks and costs, and plan for the implementation of legal and regulatory requirements for information security.

According to the analysis presented in [29], the use of the SMF UAV's CSM (Figure 4) allows separation from influences beyond the researcher's control while providing the ability to effectively counter threats.

In the model presented in Figure 4, the key elements are UAVs and fleets, which are represented in this paper as different levels and infrastructure objects in the SMF UAV.

The use of the SMF UAV CSM forms a threat model that allows the creation of a holistic and effective security system, taking into account various security aspects and adapting to changing conditions and threats in the UAV CSM and its components.

The threat and vulnerability model for a multi-functional UAV fleet aims to ensure the integrity, confidentiality, observability and availability of the system. The main task is to develop effective measures to protect against potential threats and vulnerabilities, and to ensure resilience and safety under changing operating conditions.

As shown in Figure 1, which provides an overview of the UAV fleet's infrastructure structure, the model incorporates key components and interactions of the entire system and illustrates key locations in the system

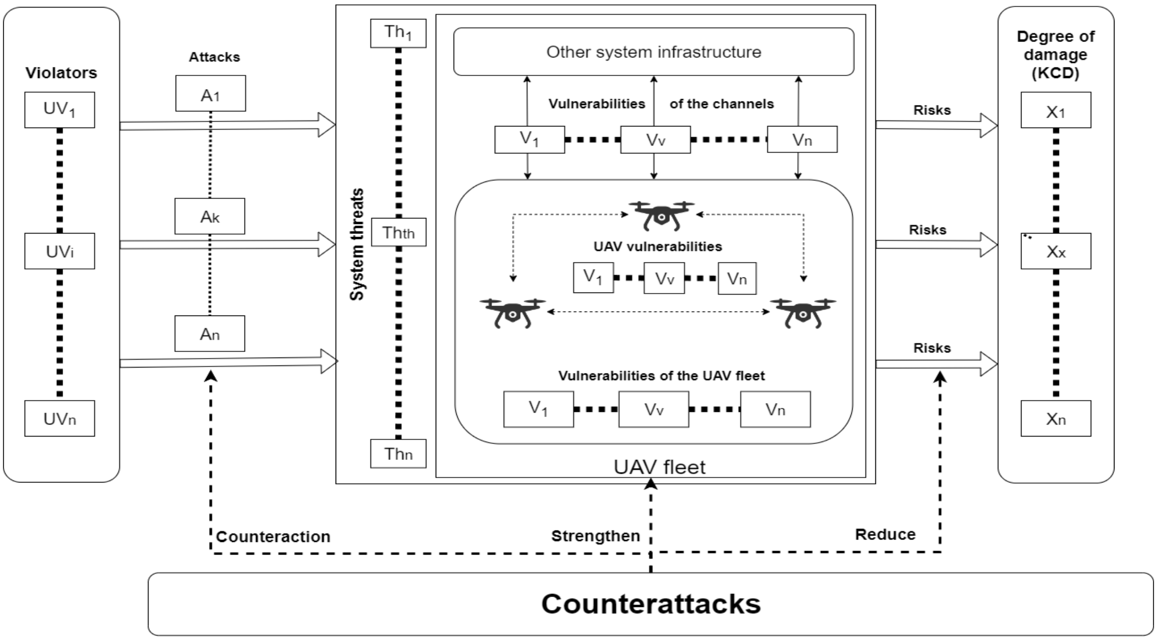

Fig. 4. Conceptual model of UAV safety and security

where threats and vulnerabilities may occur, serving as a basis for further analysis and development of cybersecurity strategies. Developing a threat based on the identified vulnerabilities of UAVs allows the identification of critical components to ensure their safety. Considering various components and their interactions, this model helps identify, avoid, or reduce the criticality and severity of potential threats that may arise from vulnerabilities in the UAV control system.

2.2. Classification of threats for the SMMF UAV

In the UAV industry, security and reliability have been identified as key elements that require constant attention and protection. Given the variety of components and systems in the UAV operating environment, it is important to analyze and protect the core elements such as control channels, software, hardware, and data channels, Figure 5.

According to the DSTU 7371:2020 standard, control channels are defined as communication paths for the transmission of information commands between the control system and the controlled object. UAVs are specially designed communication systems that allow the operator or control system to control and direct the flight of the UAV [31].

Software plays a key role in the operation and management of UAVs. It includes low-level software that works directly with the hardware and high-level software that provides a more abstract level of functionality and control.

UAV equipment includes various physical components such as sensors, cameras, and navigation systems. Threats to equipment can include physical damage, malfunction, or theft. For the purposes of this study, the UAV model in Figure 5 is considered to be a combination of six major systems, including the data acquisition module, AHRS, NAV, control module, data acquisition module, and telemetry module.

The communication system module is not shown separately in this approach because it encompasses all modules and all control and data signals pass through it, Figure 5.

The data links from the UAV to the operator or control system play a key role in providing communication and transmitting information such as UAV status, video, imagery, telemetry and other parameters. Threats to these channels include jamming, blocking, disconnection, unauthorized access and data interception.

Data (multimedia) channels in UAVs are used to exchange audio, video and images between the UAV and the ground station. They differ from control channels in their purpose and methods of information transmission.

Control channels transmit commands and signals to control the flight and functions of the UAV over low-speed, reliable radio or wire links. Data links require high bandwidth and are used for multimedia information over a variety of high frequency radio channels or data networks.

Because of the physical capabilities of the control channels, they can also be used for data (multimedia) transmission, depending on the configuration of the UAV and its communication system.

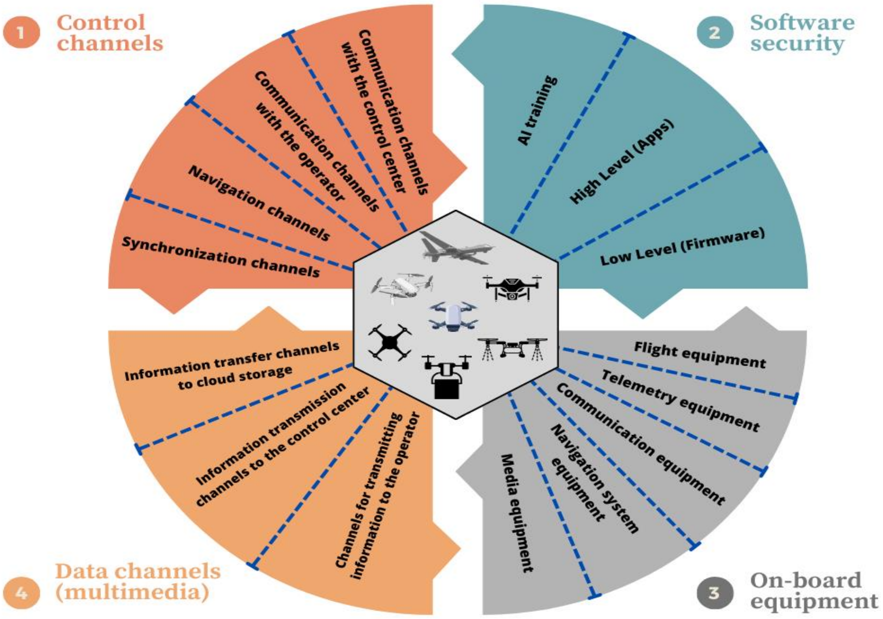
1 Control channels
Communication channels with the control center
Communication channels with the operator
Navigation channels
Synchronization channels
2 Software security
AI training
High Level (Apps)
Low Level (Firmware)
Flight equipment
Telemetry equipment
Communication equipment
Navigation system equipment
Media equipment
3 On-board equipment
Information transfer channels to cloud storage
Information transmission channels to the control center
Channels for transmitting information to the operator
4 Data channels (multimedia)

Fig. 5. Classification of threats in the SMF UAV

It is important to use separate channels for control and data transmission to meet different bandwidth, reliability, and latency requirements. A systematic approach and effective security measures are required to ensure the safety of the SMF UAV.

2.3. Theoretical and multiple description of the model of threats and vulnerabilities

A systematic approach to identifying information security threats involves an ongoing process that defines the scope of the threat identification process, identifies sources of threats and the information security threats themselves, and assesses the likelihood of threats materializing and the potential consequences. It also includes monitoring and reassessment of information security threats [27, 28].

The threat model for the SMF UAV analyzes various potential hazards and adverse events that may affect the system’s security, reliability, and operation. According to the Department of Special Telecommunication Systems and Information Protection of the Security Service of Ukraine, threats include cyber-attacks, physical impacts such as natural disasters, and unauthorized access to physical equipment [27, 28], and can be both external and internal.

Threat modeling involves analyzing the impact of threats of various components of the system, assessing the probability of occurrence, and assessing the impact on the system. Sources of threats can be individuals, organizations, states, and man-made accidents, natural disasters, and other phenomena. According to the regulatory act [30], threats are classified by the purpose of implementation, degree of damage caused, type of manifestation, and other characteristics.

These threats can be intentional or unintentional and manifest in natural disasters, UAV infrastructure component failures, equipment failures, human error, etc. In the context of safety systems, it is important to consider various aspects of threats to effectively prevent and identify potential risks.

The following notations are used to form mathematical sets and define the names of the elements of the threat model:

- Th – threats, which can be physical or cyber;
- V – vulnerabilities;
- UV – violators who implement security threats to the system.

Set of threats (Th):

$$Th=\left\{Th^{cyber},Th^{phys}\right\}, \qquad (12)$$

where $Th^{cyber}=\left\{Th_j^{cyber}, j=1,2,\ldots,h\right\}$ – set of cyber threats, $Th^{phys}=\left\{Th_k^{phys},k=1,2,\ldots,h\right\}$ – is the set of physical threats, and h is the number of threats of two types Th_i, that can affect the infrastructure of multifunctional UAV fleets. Accordingly, the mathematical formula for the threat model can be expressed as follows:

$$Th= UV_i \times V_v , \qquad (13)$$

where UV_i identifies a specific violator, for example, the type of violator:

$$\text{user violator (UV)} = \{UV_1, UV_2, ..., UV_n\},$$

where V_v represents a specific vulnerability that can be exploited by the violator to implement the threat: $V = \{V_1, V_2, ..., V_m\}$.

Identified threats to information security are subject to neutralization if they are relevant (Th^A) to the system infrastructure and the adversary who will use it, i.e. there is a possibility of the threat being implemented by an adversary with some potential for its implementation:

$$Th^A= \begin{array}{cc} & \begin{array}{ccccc} V_1 & \cdots & V_v & \cdots & V_m \end{array} \\ \begin{array}{c} UV_1 \\ \vdots \\ UV_i \\ \vdots \\ UV_n \end{array} & \left[\begin{array}{ccccc} Th_{1,1} & \cdots & Th_{1,v} & \cdots & Th_{1,m} \\ & & & & \\ Th_{i,1} & \cdots & Th_{i,v} & \cdots & Th_{i,m} \\ & & & & \\ Th_{n,1} & \cdots & Th_{n,v} & \cdots & Th_{n,m} \end{array}\right] \end{array} \qquad (14)$$

Then, the constructed TS (System Threats) matrix between infrastructure elements and threats, according to formulas 1 and 14, will look like this:

$$TS= \begin{array}{cc} & \begin{array}{ccccc} Syst_1 & \cdots & Syst_i & \cdots & Syst_m \end{array} \\ \begin{array}{c} Th_1^A \\ \vdots \\ Th_{th}^A \\ \vdots \\ Th_n^A \end{array} & \left[\begin{array}{ccccc} TS_{1,i} & \cdots & TS_{1,i} & \cdots & TS_{1,m} \\ & & & & \\ TS_{th,1} & \cdots & TS_{th,i} & \cdots & TS_{th,m} \\ & & & & \\ TS_{n,1} & \cdots & TS_{n,i} & \cdots & TS_{n,m} \end{array}\right] \end{array}. \qquad (15)$$

Thus, the TS matrix reflects all possible combinations of relationships between infrastructure elements and threats, considering the parameters where TS_i – combinations of relationships between infrastructure systems and threats, $TS_{b,q}$ – the relationship between elements b and q of components Th and $Syst_i$, described by two (cyber and physical) components:

$$TS_{b,q}=\left\{TS_{thb,iq}^{cyber},TS_{thb,iq}^{phys}\right\}, \qquad (16)$$

this connection can be described using four codes:

$$TS_{b,q}=\begin{cases} 00, \text{no threats;} \\ 01, \text{only physical threats;} \\ 10, \text{only cyber threats;} \\ 11, \text{both cyber and physical threats.} \end{cases}$$

Vulnerability modeling of multi-functional UAV fleets identifies weaknesses and deficiencies that could be attacked and result in system damage. Potential vulnerabilities include software and hardware, communication protocols, control systems, and other aspects of the infrastructure.

The vulnerability modeling process involves analyzing various system components to identify weaknesses and potential vulnerabilities. Each vulnerability is rated according to its severity and potential for exploitation by malicious actors. This allows you to develop strategies to protect and improve the security of the system by eliminating the identified vulnerabilities.

Vulnerability models should also consider human factors such as inadequate operator training or the possibility of unauthorized access to hardware and software.

Vulnerabilities can vary on the basis of various factors, including their type, occurrence, nature, and duration. Vulnerabilities can also be classified on the basis of intent, time of occurrence in the system lifecycle, and other important attributes.

The system vulnerability set includes an analysis of the potential vulnerabilities of system components and their impact on the infrastructure. For this purpose, the following vulnerability mapping (V) is used:

$$V = \{V_1, V_2, ..., V_m\}, \qquad (17)$$

where V_v represents a specific vulnerability that can be exploited by an intruder to implement a threat.

According to the threat model in equations 14 and 15, the vulnerability matrix will look like this:

$$TSV=\begin{array}{cc} & \begin{array}{ccccc} Syst_1 & \cdots & Syst_i & \cdots & Syst_m \end{array} \\ \begin{array}{c} V_1 \\ \vdots \\ V_v \\ \vdots \\ V_m \end{array} & \begin{bmatrix} TSV_{1,1} & \cdots & TSV_{1,i} & \cdots & TSV_{1,m} \\ & & & & \\ TSV_{v,1} & \cdots & TSV_{v,i} & \cdots & TSV_{v,m} \\ & & & & \\ TSV_{m,1} & \cdots & TSV_{m,i} & \cdots & TSV_{m,m} \end{bmatrix} \end{array}. \qquad (18)$$

Thus, the TSV matrix reflects all possible combinations of connections between infrastructure systems and vulnerabilities of that system, where TSV – к are specific vulnerabilities on the infrastructure system and that connection can be described by two codes:

$$TSV=\begin{cases} 0, \text{no vulnerabilities;} \\ 1, \text{cyber and physical vulnerabilities exist.} \end{cases}$$

3. Models of intruders and attacks

3.1. Intruders

According to the established Ukrainian standards and legislation, violators of the SMF UAVs are individuals, legal entities, or groups of individuals who commit actions that violate the established norms in the use and operation of these fleets [32, 33].

Modeling the actions of SMF UAV attackers in accordance with Ukrainian national standards involves a thorough analysis of possible threats and a study of the impact of attackers on the functioning of the system. According to Ukrainian legislation [32, 33], attackers can be classified according to the following characteristics:

1. Intruder Type: Identifies whether the intrusion is cyber or physical. This helps distinguish attacks that occur in the electronic space from those that may have a physical impact.
2. Intruder Motivation: Reflects the goals or incentives that drive the intruder to attack, such as financial gain, disclosure of confidential information, and political motivation.
3. Intruder Skill Level: Reflects the level of technical knowledge and skills possessed by the intruder, ranging from ignorance to high expertise.
4. Source of threat: considers whether the intruder is internal (from within the organization) or external (from outside the organization). This may indicate possible means of intrusion.

Classification of the intruder's objectives (motivation) considers the goals and objectives of the information system, the type of information processed, and the consequences (losses) that may result from a breach of the confidentiality, integrity, availability, or accountability of information. The types of intruders and their possible motivations are listed in Table 1.

When assessing the capabilities of the infringers, it must be assumed that type 4 infringers may collude with type 6, 7, 8, 9, 1, 2 and 10 infringers to increase their capabilities. Type 5 infringers may collude with type 7, 1, 2 and 3 infringers. Type 6 infringers may collude with type 7, 1, 2 and 3 infringers. When such assumptions are made, the goals (motivation) and capabilities of the infringers are subject to combination.

The potential of an intruder to implement information security threats is determined by its competence, resources and motivation. According to [27, 32, 33], offenders are classified by potential:

- low-potential offenders use only publicly available information. This includes "external" parties, internal employees, and system users;
- intermediate attackers analyze software code to find and exploit vulnerabilities. This includes terrorists, criminal groups, competing organizations, system administrators, and software developers;
- high potential attackers bookmark the system, conduct specialized research, and use tools to penetrate and extract information. These are primarily foreign intelligence services.

Table 1

Classification of offenders

Type. viol.	№.	Types of offenders	Possible goals (motivation) for the realization of threats
1	2	3	4
Internal	1	Workers involved in installation and commissioning	Deception and breach of trust, as well as reckless actions that cause property damage.
	2	System infrastructure maintainers (admins, security, cleaners, etc.).	Property damage caused by fraud or negligence. Unintentional, reckless or unskilled actions.
	3	Information system administrators and security administrators	Fraud, revenge, selling vulnerabilities, and negligent actions leading to damage.
External	4	Special services of foreign states (blocs of states)	Damaging the state, its sectors, or destabilizing authorities and organizations.
	5	Terrorist and extremist groups	Damaging the state, sectors, or economy; committing terrorism; driven by ideological or political reasons; disrupting public authority and organizations.
	6	Criminal groups (criminal organizations)	Causing property damage by fraud or other criminal means. Identification of vulnerabilities for the purpose of their further sale and financial gain
	7	External entities (individuals), former employees (users)	Ideological or political motives. Identification of vulnerabilities for the purpose of selling them and obtaining financial gain. Revenge for previous actions
	8	Competing organizations	Gaining competitive advantages. Causing property damage through fraud or breach of trust.
	9	Developers, manufacturers, and suppliers of software, hardware, and software and hardware tools	Implementation of additional functions in the software or software and hardware during the development phase. Unintentional, reckless or unskilled acts.

The intruder model analyzes potential system intruders and their impact on the infrastructure. The following mathematical representations are used:

– UV (user violator) – a set of possible offenders;

– A – the set of possible attacks used by the offender.

The set of possible violators:

$$UV= \{UV_1, UV_2, ..., UV_n\},$$

where UV_i defines a specific offender, for example, a type of offender.

Every offender is a Cartesian multiplication:

$$UV_i = A \times Syst \;, \tag{19}$$

where A – is the set of ways to realize threats (attacks) (A): $A = \{A_1, A_2, ..., A_k\}$, Syst – is the set of objects of influence, i.e. the UAV infrastructure in Figure 1 (Syst): $Syst = \{Syst_i, i=1,2,\ldots,m\}$. Here, A represents a method or technique that can be used by the perpetrators to implement threats. Each Syst represents a specific fleet of UAVs in the system that can be targeted by the threat:

$$UV_i = \begin{array}{c} \\ A_1 \\ \vdots \\ A_k \\ \vdots \\ A_n \end{array} \begin{array}{c} \begin{array}{ccccc} Syst_1 & \cdots & Syst_i & \cdots & Syst_m \end{array} \\ \begin{bmatrix} UV_{1,1} & \cdots & UV_{1,i} & \cdots & UV_{1,m} \\ & & & & \\ UV_{k,1} & \cdots & UV_{k,i} & \cdots & UV_{k,m} \\ & & & & \\ UV_{n,1} & \cdots & UV_{n,i} & \cdots & UV_{n,m} \end{bmatrix} \end{array} \tag{20}$$

3.2. Attacks

Attacks on SMF UAVs are attempts by unlawful actors (intruders, hackers, etc.) to gain unauthorized access to the information, physical, or functional components of a UAV system to cause damage or gain advantage. Attacks may use cyber and physical methods to achieve their objectives.

The proposed classification of combined attacks on the SMF UAV, covering the type of attacks and their effects, can be summarized as follows (see Figure 6):

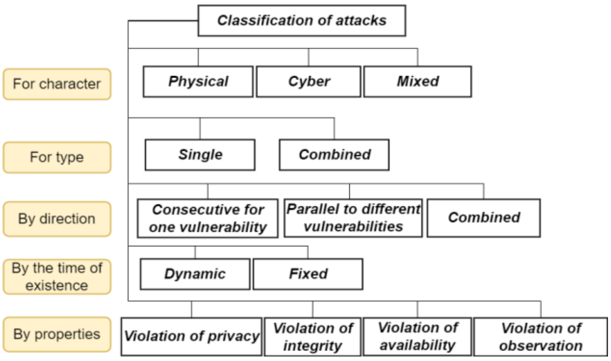

Fig. 6. Classification of attacks on the SMF UAV

1. Type of attack:

– physical-cyber-attacks: combine physical actions with cyber components, such as physical damage to equipment and cyber-attacks on control or navigation systems;

– cyber-physical attacks: combine cyber-attacks with physical consequences, for example, changing the kinematic parameters of a UAV, leading to a physical collision or crash.

2. Impact:

– physical and cyber destabilizing attacks: Cause physical disruption, combining it with cyber-attacks to increase impact;

– espionage and cyberattacks: aimed at leaking confidential information using cyber tools to obtain and transmit it.

3. Other:

This classification helps to understand the various aspects of combined attacks on the SMF UAV and to develop effective security policy strategies.

Attack models on the SMF UAV divide attacks into two main categories: physical attacks and cyber-attacks. As mentioned above in formula 20: A is the set of ways to implement threats (attacks) (A): $A = \{A_1, A_2, ..., A_k\}$.

Physical attacks include attempts to influence the infrastructure of UAV fleets by penetrating or manipulating physical objects. The physical attack model can be described as follows:

$$A^{phys} = \{A_1^{phys}, A_2^{phys}, ...,A_k^{phys}\},$$

where A^{phys} – is the set of possible physical attacks.

Generalizing, the complex of physical attacks (A^{phys}) can be represented as a Cartesian product of different physical attacks (A_k^{phys}) can be represented as a Cartesian product of different physical attacks ($Syst_i$):

$$A^{phys}=\begin{array}{cc} & \begin{array}{ccccc} Syst_1 & \cdots & Syst_i & \cdots & Syst_m \end{array} \\ \begin{array}{c} A_1^{phys} \\ \vdots \\ A_k^{phys} \\ \vdots \\ A_n^{phys} \end{array} & \begin{bmatrix} A_{1,1}^{phys} & \cdots & A_{1,i}^{phys} & \cdots & A_{1,m}^{phys} \\ \\ A_{k,1}^{phys} & \cdots & A_{k,i}^{phys} & \cdots & A_{k,m}^{phys} \\ \\ A_{n,1}^{phys} & \cdots & A_{n,i}^{phys} & \cdots & A_{n,m}^{phys} \end{bmatrix} \end{array} \quad (21)$$

It follows that the model of physical attack can be expressed as follows:

$$A^{phys}=\{A_k^{phys}\times Syst_i | A_k^{phys} \in A^{phys}, Syst_i \in Syst\}.$$

Cyber-attacks are malicious interferences that damage or gain unauthorized access to the information and computer infrastructure of the UAV fleet. The cyber-attack model can be described as follows:

$$A^{cyber} = \{A_1^{cyber}, A_2^{cyber}, ...,A_k^{cyber}\},$$

where A^{cyber} – is the set of possible cyber-attacks.

In summary, the complex of cyber-attacks (A^{cyber}) can be represented as in formula 19:

$$A^{cyber}=\begin{array}{cc} & \begin{array}{ccccc} Syst_1 & \cdots & Syst_i & \cdots & Syst_m \end{array} \\ \begin{array}{c} A_1^{cyber} \\ \vdots \\ A_k^{cyber} \\ \vdots \\ A_n^{cyber} \end{array} & \begin{bmatrix} A_{1,1}^{cyber} & \cdots & A_{1,i}^{cyber} & \cdots & A_{1,m}^{cyber} \\ \\ A_{k,1}^{cyber} & \cdots & A_{k,i}^{cyber} & \cdots & A_{k,m}^{cyber} \\ \\ A_{n,1}^{cyber} & \cdots & A_{n,i}^{cyber} & \cdots & A_{n,m}^{cyber} \end{bmatrix} \end{array} \quad (22)$$

The model of a cyber-attack can be expressed as follows:

$$A^{cyber}=\{A_k^{cyber}\times Syst_i | A_k^{cyber} \in A^{cyber}, Syst_i \in Syst\}.$$

Some attacks combine physical and cyber elements to maximize their effect:

$$CombA_{ij}=A_k^{cyber} \cup A_k^{phys}, \quad (23)$$

$$CombA=\{CombA_{ij} | A_k^{cyber} \in A^{cyber}, A_k^{phys} \in A^{phys}\} \quad (24)$$

Complex attack scenarios against multi-functional UAV fleets are complex combinations of different types of attacks and exploitation methods that attackers use to achieve their objectives and cause damage to the system. Combined attack scenarios are important to increase efficiency, bypass defenses, exploit a combination of vulnerabilities, and make them more difficult to detect and counter.

Combination attack scenarios can be classified as follows:

1. against a single vulnerability: an attacker uses multiple attacks or exploits against a single vulnerability to effectively exploit or neutralize it.

2. against multiple vulnerabilities: an attacker launches parallel attacks on different vulnerabilities in the system, increasing the opportunities for intrusion and damage.

These scenarios can be used by attackers for various reasons, including economic gain, political purposes, espionage, and sabotage.

4. Risk assessment

The realization of security threats to multifunctional UAV fleets and to the UAVs themselves can have direct or indirect impacts on the Confidentiality, Integrity, Availability, and Observability (CIAO) of information in the SMF UAV.

A direct impact on these properties can occur as a result of direct security threats. A risk assessment system is used to evaluate the potential consequences of attacks on various security aspects, such as CIAO, and to assess the potential impact of such attacks. Damage to security assets is assessed using the following indicators:

1. Confidentiality: The level of likelihood that confidential information will be compromised.

2. Integrity: The degree of potential alteration or threat to the integrity of information.

3. Availability: the impact of an attack on the availability of systems and information.

4. Observability: requirements for identification and control that may be lost or destroyed.

The risk assessment of attacks on the SMF UAV is determined according to Table 2, where the impact of the threat on each security asset (CIAO) is assessed separately.

Table 2

The Result of Information Loss Risks
to the Security Properties of the SMF UAV

Security properties		Result of realization of security threats to UAV fleets	
		No effect on	Influence
1		2	3
Confidentiality	X_{rl}^{C}	There is no opportunity for unauthorized access, copying, disclosure, or distribution of information as a result of information security threats.	Information can be unlawfully accessed, copied, shared, or distributed due to security threats.
Integrity	X_{rl}^{I}	No potential to destroy or alter information as a result of information security threats	Information can be destroyed or altered as a result of information security threats.
Availability	X_{rl}^{A}	No ability to block information due to information security threats	Information may be blocked due to information security threats.
Observability	X_{rl}^{O}	As a result of the information security threat, there is no way to identify and control information.	Information security threats can change or destroy information identification and control.

When determining the degree of possible damage, it is necessary to proceed from the fact that, depending on the goals and objectives of the SMF UAV, the types of information processed, and the impact on the CIAO of each type of information contained in the system may result in different types of damage. At the same time, the different types of damage are characterized by different information owners and violators.

The level of potential damage from security threats to SMF UAV data is determined by the degree of negative consequences for each CIAO property included in the system. Each indicator is assigned a symbolic coefficient according to its importance to a particular system, as defined in Table 2.

In cases where different types of information are processed (official secrets, personal data, military secrets, etc.), the impact on the CIAO is assessed separately for each type of UAV fleet and UAV itself in the system (r, ..., m).

A single scale for measuring the degree of negative consequences includes the values "minor", "moderate" and "significant". To assess the violations of each type, they are defined in the specified unified scale for all goals and objectives of the system.

The degree of damage was determined by an expert according to Table 3.

Table 3

Degree of damage (CIAO)

Degree of damage	Characterization of the degree of damage
High	Compromising a key security aspect (CIAO) can lead to major issues. It might render the UAV fleet, individual UAVs, or the operator (holder of fleet credentials) unable to carry out their duties.
Middle	A breach in information security (CIAO) could lead to moderate adverse outcomes, causing a disruption in the performance of functions for the UAV fleet, UAV, or the operator with access to the fleet.
Low	A breach in information security (CIAO) could lead to minor disruptions. It might hinder the UAV fleet, individual UAVs, or the operator, impacting their efficiency or requiring extra tools to perform tasks.

The assessment of potential damage is determined by the highest values of the degree of potential damage for the CIAO of each type of UAV, UAS, or communications system fleet with respect to each type of damage. We refer to this final degree of potential damage as X_r and calculate it using the following formula:

$$X_r = \max\left(X_r^l\right);\ l = C, I, A, O\ . \qquad (25)$$

According to formula 17 and considering the structural and functional characteristics and operating conditions of the system, the relevance of security threats to these UAV fleets and UAVs for the system is determined in accordance with Table 4.

This risk assessment serves as the basis for making decisions on cybersecurity implementation and setting priorities for protecting the system of multifunctional UAV fleets from possible cyberattacks.

Table 4

Determining Threat Severity Level

Probability of threat realization (Th^A)	Degree of probable loss (X_r)		
	Low	Middle	High
Low	Not relevant	Not relevant	Relevant
Middle	Not relevant	Relevant	Relevant
High	Relevant	Relevant	Relevant

5. Case study

5.1. An example of IMECA analysis

After analyzing models, conceptual schemes, and assessing risks to SMF UAV, IMECA scrutinized cyber threats (see Figure 1) from four perpetrator types (see Table 1): internal system administrators, foreign intelligence agencies, criminal groups, and ex-employees. Using threat classification (see Figure 5), we'll systematically assess SMF UAV attacks based on threat levels according to the IMECA guidelines. The evaluation will consider the following parameters:

– offender potential (VP) as per Table 1;

– threat method;

– vulnerability of system weak points;

– attack type;

– impact of attacks on security properties;

– post-attack consequences;

– probability (P) of attack occurrence (A – High, B – Medium, C – Low);

– severity (S) of attack consequences (A – High, B – Medium, C – Low);

– risk (R) to the system based on probability and severity (A – High, B – Medium, C – Low);

– countermeasures to combat attacks.

Combining probability and severity indicates the criticality level. Effective countermeasures mitigate criticality. High severity coupled with low countermeasures pose significant risk to SMF UAVs. IMECA analysis results are shown in Table 5.

IMECA is a methodology that allows the integration of various aspects of cybersecurity assessment using multi-criteria analysis. In this context, the columns related to criticality (probability, severity, risk), consequences after an attack, and implementing countermeasures are considered integral to the vulnerability in order to consider several criteria and assess risks using the so-called conservative approach (the worst scenario for the analyzed system).

Based on the results of the analysis of attacks by the level of danger to the SMF UAV, we will build a matrix of criticality of these systems (see Table 6) and a matrix of criticality after implementation of the considered countermeasures (see Table 7). Green indicates a low level of risk (attack), yellow indicates a medium level of risk (attack), and red indicates a high level of risk (attack) [34].

Table 6

Cyber risk criticality matrix of the SMF UAV

Probability of occurrence	Severity		
	Low	Middle	High
Low	11, 12	9, 10	
Middle		3, 7, 8	2, 6
High			1, 4, 5

Based on the analysis of the criticality matrix (see Table 7), the attacks "Gaining access to UAV control" (2) and "Using UAVs for disruption and espionage" (7) change the level of probability of occurrence by one position due to effective countermeasures. However, injecting malicious code (1), providing false GPS signals (4) and using UAVs for disruption and espionage (5) remain in the high risk zone because existing countermeasures do not address the consequences of these attacks.

Table 7

Matrix of criticality of cyber risks of the SMF UAV after implementation of countermeasures

Probability of occurrence	Severity		
	Low	Low	Low
Low	11, 12	9, 10	
Middle	7	3, 8	6
High		2	1, 4, 5

5.2. Countermeasures

To ensure the security of cyber-physical systems using SMF UAVs, it is important to standardize wireless communication protocols exclusively for UAV networks. It is proposed to combine the latest security techniques to protect the infrastructure from possible cyber threats, considering the security challenges.

It is recommended that the following basic security methods be used to protect the SMF UAV:

1. Trusted authentication: coordinated at the control station to ensure that an illegal UAV does not remain in the air network.

2. Lightweight cryptographic protocols: use mutual authentication protocol for secure communication, thereby reducing energy and computational resource consumption [35].

3. Artificial intelligence waveform design: used to ensure jamming resistance and make it difficult for enemy transceivers to detect the signal.

4. Artificial intelligence and Blockchain: Ensure the integrity and confidentiality of data in unmanned systems by providing transparency.

The proposed security measures are superior to existing mechanisms by providing specific, tailored tools to effectively protect the SMF UAV from cyber threats. These methods, which use artificial intelligence, can effectively protect the SBF UAV and increase the security of the system as a whole.

6. Discussion

An understanding of the problems with the current design of countermeasures is important. Currently, they appear to be too general and unspecific, making it difficult to understand their effectiveness in addressing specific vulnerabilities. This means that more work is needed to analyze countermeasures in more detail and break them down into more specific, tailored defenses for each vulnerability.

Table 5

IMECA cyber-attack analysis and countermeasures to ensure the security of the SMF UAV

№	👤	VP	Threat	Vulnerability	Attack	Security properties				Consequences	Criticality			Countermeasures
						C	I	A	O		P	S	R	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	A	Software interference	Invalid input data	Insertion of malicious code	Y	Y	Y	Y	Functionality change or UAV malfunctions	A	A	A	Validation and Filtering of Input Data
2		A	Unauthorized access to control channels	Issues related the control access to UAV controls	Accessing UAV control	N	Y	Y	Y	UAV abduction, route alteration, and manipulation	B	A	A	Authentication, encryption, control.
3		B	Embedding malicious hardware	Absence of device authentication and control	Embedding malicious hardware on UAVs	Y	Y	Y	Y	Remote control, sensitive data collection, loss of UAV control	B	B	B	Continuous security checks, authentication
4	2	A	GPS-Spoofing	Vulnerability of GPS Systems and Receivers	Providing Fake GPS Signals	N	N	Y	Y	Flight route change and UAV loss	A	A	A	Using encrypted navigation systems
5		A	UAV control channel interference	Lack of communication protocol protection	UAVs for interference and espionage	N	Y	Y	Y	Theftof UAVs or change its route, possibility of mission disclosure	A	A	A	Monitoring and detecting suspicious activity
6		A	Impact on telemetry and feedback	Open telemetry data transfer	Using UAVs as "kamikazes"	N	Y	Y	Y	The impact of UAV safety & navigation, crash execution, collision risk	B	A	A	Encryption, control & blocking access, authentication & validation
7	3	B	UAV control channel interference	Lack of communication protocol protection	UAVs for interference and espionage	N	Y	Y	Y	Theftof UAVs or change its route, possibility of mission disclosure	B	B	B	Monitoring and detecting suspicious activity
8		B	Intercepting data transmission channels (multimedia)	Unprotected data channels	Intercept or block data transfer	Y	Y	Y	Y	Leaking confidential data, interfering a UAV's operation	B	B	B	Using encryption & data protection, VPN, authentication
9		C	Physical attacks on UAVs	Lack of physical access protection	Destruction or theft of hardware components	Y	Y	Y	Y	Loss of hardware, disruption of UAV operation	C	B	C	Remote monitoring, backup and encryption of the UAV system
10	4	C	Manipulating former colleagues	Insufficient education of the staff	Obtaining information or access from employees	Y	Y	Y	Y	Unauthorized access, privacy leakage, loss of finances, UAV theft	C	B	C	Establishing a security policy, identity verification, monitoring and auditing of personnel
11		C	Software vulnerabilities	Doesn't validate input data	Introducing malicious code	Y	Y	Y	Y	Changing functionality or failures in UAVs	C	C	C	Validation and filtering of incoming data, monitoring
12		C	Physical attack on UAV hardware	Insecurity of hardware components	Attacks or installation of malware	Y	Y	Y	N	Damage or loss of hardware components, loss of functionality	C	C	C	Establishing identity policies and controls

In addition, it should be noted that the future evolution of Table 5 according to the IMECA analysis will depend on the characteristics of the information. This means that in the future, as the characteristics of information change, new vulnerabilities and more optimal countermeasures may appear. At the current stage, the task of choosing optimal countermeasures has not been set, but this is a very important aspect. The effectiveness of countermeasures can vary greatly depending on the broad range of vulnerabilities they can cover. Therefore, more research and analysis are needed to identify more universal and effective countermeasures to close vulnerabilities in the future.

The design of countermeasures is the cornerstone of ensuring system security. It has a direct impact on the end result of the defense. Understanding how countermeasures affect vulnerabilities highlights the need to develop a strategy for optimal countermeasure selection in the future. Minimizing risk and creating a clear algorithm to determine the optimal countermeasure for each vulnerability plays an important role in closing most vulnerabilities.

In addition, countermeasure groups have different characteristics and properties that cover different aspects of vulnerabilities. Their ability to cover a wide range of characteristics and properties of vulnerabilities makes the selection of optimal countermeasures more flexible and universal, which in turn contributes to a more complete protection of the system against a variety of threats.

Conclusions

The main contribution of the investigation is, first, a theoretical-set model of multi-functional UAV cybersecurity as a complex cyber physical system operated under conditions of information (cyber) and physical influences (intrusions) on its assets and, second, a modified method of cybersecurity analysis based on IMECA technique.

This article provides a thorough risk-based analysis of the cybersecurity of multi-functional UAV fleets. Threats, vulnerabilities, and attack models that identify potential risks to these complex systems are considered. Multifunctional UAV fleets are vulnerable to various cyber-attacks that can compromise their confidentiality, integrity, availability, and observability.

It should be noted that for such types of UAV fleets and systems as a whole IMECA analysis has to be enhanced by considering the hierarchical model of the system. This means that hierarchical IMECA can be developed and applied.

One of the main conclusions is the need to develop and implement effective cybersecurity strategies and measures for multifunctional UAV fleets. Trusted authentication systems, lightweight cryptographic protocols, artificial intelligence-based waveforms, and blockchain technologies have been identified as effective security methods.

Future research steps in this area are to further develop and improve the proposed strategies, adapt them to growing threats, and improve attack models in line with the rapidly changing cyber environment. It is also important to explore the possibilities of integrating the latest cybersecurity technologies to ensure the highest level of protection.

As part of the analysis of cyber-attacks and countermeasures to ensure the security of the SMF UAV using the IMECA methodology, the need for further improvement and development was identified. Further research is planned to develop a model and methodology for evaluating countermeasures to increase their effectiveness in preventing cyberattacks and minimizing threats.

This process involves identifying and analyzing the types of attacks, and developing strategies and methods for responding to them. It is planned to create criteria and indicators that will consider different types of expert assessments. This will not only allow assessing the current level of protection but also adapting countermeasures to more effectively counter various attacks.

Future research is aimed at creating a system capable of predicting and analyzing the evolution of threats, which will allow for a rapid response to new types of cyberattacks and minimize their impact on UAV security systems. Future work is planned to increase the level of protection and ensure the safe operation of UAVs in various scenarios.

Another important research direction is the assessment of SMF UAV safety using a security-informed safety approach and SISMECA technique [24].

Contributions of authors: conceptualization, methodology, formulation of tasks – **Heorhii Zemlianko**, **Vyacheslav Kharchenko**; development of models – **Heorhii Zemlianko**; verification, analysis of results, visualization, writing, original draft preparation – **Heorhii Zemlianko**, **Vyacheslav Kharchenko**; review and editing – **Vyacheslav Kharchenko**.

All the authors have read and agreed to the published version of this manuscript.

Acknowledgements. This article was prepared with the support of the project *"Fundamentals and methods for providing dependability of UAV fleets for intelligent systems of monitoring potentially unsafe and military objects"* which is financed by the Ministry of Education and Science of Ukraine, No. 0121U112172.

References

1. Gupta, A., & Gupta, S. K. A survey on green unmanned aerial vehicles- based fog computing: Challenges and future perspective. *Transactions on Emerging Telecommunications Technologies*, 2022, vol. 33, iss. 11, pp. 1-29. DOI: 10.1002/ett.4603.

2. Coppola, M., McGuire, K. N., De Wagter, C., & de Croon, G. C. H. E. A Survey on Swarming with Micro Air Vehicles: Fundamental Challenges and Constraints.

Frontiers in Robotics and AI, 2020, vol. 7, pp. 1-26. DOI: 10.3389/frobt.2020.00018.

3. Deng, H., Huang, J., Liu, Q., Zhao, T., Zhou, C., & Gao, J. A Distributed Collaborative Allocation Method of Reconnaissance and Strike Tasks for Heterogeneous UAVs. *Drones*, 2023, vol. 7, no. 2, pp. 138-160. DOI: 10.3390/drones7020138.

4. Chen, Y., Jiao, Y., Wu, M., Ma, H., & Lu, Z. Group Target Tracking for Highly Maneuverable Unmanned Aerial Vehicles Swarms: A Perspective. *Sensors*, 2023, vol. 23, no. 9, pp. 4465-4484. DOI: 10.3390/s23094465.

5. Hammoud, B., & Wehn, N. Recent Advances in Oil-Spill Monitoring Using Drone-Based Radar Remote Sensing. *Environmental Sciences*. *IntechOpen*, 2022, no. 24, pp. 4090-4110. DOI: 10.5772/intechopen.106942.

6. Falorca, J. F., Miraldes, J. P. N. D., & Lanzinha, J. C. G. New trends in visual inspection of buildings and structures: Study for the use of drones. *Open Engineering*, 2021, vol. 11, no. 1, pp. 734-743. DOI: 10.1515/eng-2021-0071.

7. Ahmad, H., Farhan, M., & Farooq, U. Computer Vision Techniques for Military Surveillance Drones. *Wasit Journal of Computer and Mathematics Science*, 2023, vol. 2, no. 2, pp. 56-63. DOI: 10.31185/wjcms.148.

8. Abdulhae, O. T., Mandeep, J. S., & Islam, M. Cluster-Based Routing Protocols for Flying Ad Hoc Networks (FANETs). *IEEE Access*, 2022, no. 10, pp. 32981-33004. DOI: 10.1109/access.2022.3161446.

9. Al-Bkree, M. Managing the cyber-physical security for unmanned aerial vehicles used in perimeter surveillance. *International Journal of Innovative Research and Scientific Studies*, 2023, vol. 6, no. 1, pp. 164-173. DOI: 10.53894/ijirss.v6i1.1173.

10. AL-Dosari, K., Hunaiti, Z., & Balachandran, W. Systematic Review on Civilian Drones in Safety and Security Applications. *Drones*, 2023, vol. 7, no. 3, pp. 210-222. DOI: 10.3390/drones7030210.

11. Omolara, A. E., Alawida, M., & Abiodun, O. I. Drone cybersecurity issues, solutions, trend insights and future perspectives: a survey. *Neural Computing and Applications*, 2023, vol. 35, no. 31, pp. 1-39. DOI: 10.1007/s00521-023-08857-7.

12. McEnroe, P., Wang, S., & Liyanage, M. A Survey on the Convergence of Edge Computing and AI for UAVs: Opportunities and Challenges. *IEEE Internet of Things Journal*, 2022, vol. 9, no. 17, pp. 15435-15459. DOI: 10.1109/jiot.2022.3176400.

13. Yang, W., Wang, S., Yin, X., Wang, X., & Hu, J. A Review on Security Issues and Solutions of the Internet of Drones. *IEEE Open Journal of the Computer Society*, 2022, vol. 3, pp. 96-110. DOI: 10.1109/ojcs.2022.3183003.

14. Subbarayalu, V., & Vensuslaus, M. A. An Intrusion Detection System for Drone Swarming Utilizing Timed Probabilistic Automata. *Drones*, 2023, vol. 7, no. 4, pp. 248-267. DOI: 10.3390/drones7040248.

15. Gladence, L. M., Anu, V. M., Anderson, A., Stanley, I., Fernando J., J. A., & Revathy, S. Swarm Intelligence in Disaster Recovery. *5th International Conference on Intelligent Computing and Control Systems (ICICCS)*, May 6-8, 2021, Madurai, India. IEEE, 2021, pp. 1-8. DOI: 10.1109/iciccs51141.2021.9432146.

16. Jeon, C., Ko, H., Ha, J., Lee, B., & Ryu, B. SwarmSense: Effective and Resilient Drone Swarming and Search for Disaster Response and Management Application. *Wireless Innovation Forum, WInnComm 2019 Proceedings*. Available at: Presentation – https://www.wirelessinnovation.org/assets/Proceedings/2019/TS6.2%20Jeon%20presentation.pdf; Paper – https://www.wirelessinnovation.org/assets/Proceedings/2019/TS6.2%20Jeon%20paper.pdf (accessed 18.08.2023).

17. Torianyk, V., Kharchenko, V., & Zemlianko, H. IMECA Based Assessment of Internet of Drones Systems Cyber Security Considering Radio Frequency Vulnerabilities. *2nd International Workshop on Intelligent Information Technologies and Systems of Information Security (IntelITSIS'2021)*, March 24–26, 2021, Khmelnytskyi, Ukraine, 2021, vol. 2853, pp. 460–470. Available at: https://ceur-ws.org/Vol-2853/paper50.pdf (accessed 10.08.2023).

18. Niyonsaba, S., Konate, K., & Soidridine, M. M. A Survey on Cybersecurity in Unmanned Aerial Vehicles: Cyberattacks, Defense Techniques and Future Research Directions. *International Journal of Computer Networks and Applications*, 2023, vol. 10, no. 5, pp. 688-701. DOI: 10.22247/ijcna/2023/223417.

19. Arshad, I., Alsamhi, S. H., Qiao, Y., Lee, B., & Ye, Y. A Novel Framework for Smart Cyber Defence: A Deep-Dive Into Deep Learning Attacks and Defences. *IEEE Access*, 2023, no. 11, pp. 88527-88548. DOI: 10.1109/access.2023.3306333.

20. Shafik, W., Mojtaba Matinkhah, S., & Shokoor, F. Cybersecurity in Unmanned Aerial Vehicles: a Review. *International Journal on Smart Sensing and Intelligent Systems*, 2023, vol. 16, no. 1, pp. 1-10. DOI: 10.2478/ijssis-2023-0012.

21. Omolara, A. E., Alawida, M., & Abiodun, O. I. Drone cybersecurity issues, solutions, trend insights and future perspectives: a survey. *Neural Computing and Applications*, 2023, vol. 35, no. 31, pp. 1-39. DOI: 10.1007/s00521-023-08857-7.

22. Altaweel, A., Mukkath, H., & Kamel, I. GPS Spoofing Attacks in FANETs: A Systematic Literature Review. *IEEE Access: The Multidisciplinary Open Access Journal*, 2023, vol. 11, pp. 55233-55280. DOI: 10.1109/access.2023.3281731.

23. Babeshko, I., Illiashenko, O., Kharchenko, V., & Leontiev, K. Towards Trustworthy Safety Assessment

by Providing Expert and Tool-Based XMECA Techniques. *Mathematics,* 2022, vol. 10, article no. 2297. DOI: 10.3390/math10132297.

24. Illiashenko, O., Kharchenko, V., Babeshko, I., Fesenko, H., & Di Giandomenico, F. Security-Informed Safety Analysis of Autonomous Transport Systems Considering AI-Powered Cyberattacks and Protection. *Entropy*, 2023, vol. 25, article no. 1123. DOI: 10.3390/e25081123.

25. *ISO/IEC/IEEE 21839:2019 Systems and software engineering – System of systems (SoS) considerations in life cycle stages of a system. ISO*. Available at: https://www.iso.org/ru/standard/71955.html. (accessed 05.08.2023).

26. *ISO/IEC/IEEE 21840:2019 Systems and software engineering – Guidelines for the utilization of ISO/IEC/IEEE 15288 in the context of system of systems (SoS).* Available at: https://www.iso.org/ru/standard/71956.html. (accessed 05.09.2023).

27. *Zahal'ni polozhennya shchodo zakhystu informatsiyi v komp"yuternykh systemakh vid nesanktsionovanoho dostupu: Norm. dok. systemy tekhn. zakh. informatsiyi vid 28.05.1999 r. № ND TZI 1.1-002-99: stanom na 28 hrud. 2012 r.* [General provisions on the protection of information in computer systems against unauthorized access: Norm. dock. technical systems west information dated 05/28/1999 № ND TZI 1.1-002-99: as of December 28 2012]. Available at: https://tzi.com.ua/downloads/1.1-002-99.pdf (accessed 03.09.2023). (In Ukrainian).

28. *Terminolohiya v haluzi zakhystu informatsiyi v komp"yuternykh systemakh vid nesanktsionovanoho dostupu: Norm. dok. systemy tekhn. zakh. informatsiyi vid 28.05.1999 r. № ND TZI 1.1-003-99* [Terminology in the field of information protection in computer systems against unauthorized access: Norm. dock. technical systems west information dated 05/28/1999 № ND TZI 1.1-003-99]. Available at: https://tzi.ua/assets/files/1.1_003_99.pdf (accessed 03.09.2023) (In Ukrainian).

29. Pevnev, V., Tsuranov, M., Zemlianko, H., & Amelina, O. Conceptual Model of Information Security. У: *Lecture Notes in Networks and Systems.* Cham: Springer International Publishing, 2021, vol. 188, pp. 158–168. DOI: 10.1007/978-3-030-66717-7_14.

30. *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection.* To replace EN ISO/IEC 27001:2017; ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015; valid from 2022-12-28. Kind. officer 3, 2022. 19 p. Available at: https://www.iso.org/ru/standard/27001 (accessed 03.09.2023).

31. *DSTU 7371:2020. Tekhnika aviatsiyna derzhavnoyi aviatsiyi. Aparaty lital'ni bezpilotni. Osnovni terminy ta vyznachennya ponyat'. Klasyfikatsiya.* Na zaminu DSTU V 7371:2013; chynnyy vid 2021-07-01. Nakaz pro pryynyattya ND: 2020-05-06 № 88. Vyd. ofits. Ukrayina: DP «UkrNDNTs» [DSTU 7371:2020. Aviation equipment of state aviation. Unmanned aerial vehicles. Basic terms and definitions. Classification. To replace DSTU B 7371:2013; valid from 2021-07-01. Order on the adoption of the ND: 2020-05-06 № 88. Ed. officer Ukraine: SE "UkrNDNC"]. 2020. 21 p. (In Ukrainian).

32. *Kryteriyi otsinky zakhyshchenosti informatsiyi v komp"yuternykh systemakh vid nesanktsionovanoho dostupu: Norm. dok. systemy tekhn. zakh. informatsiyi vid 28.05.1999 r. № ND TZI 2.5-004-99: stanom na 28 hrud. 2012 r.* [Criteria for evaluating the security of information in computer systems against unauthorized access: Norm. dock. technical systems west information dated 05/28/1999 No. ND TZI 2.5-004-99: as of December 28 2012]. Available at: https://tzi.com.ua/downloads/2.5-004-99.pdf (accessed 03.09.2023). (In Ukrainian).

33. *Zakon Ukrayiny # 2952-IX vid 24.02.2023 «Pro natsional'nu bezpeku Ukrayiny». Verkhovna Rada Ukrayiny* [On the national security of Ukraine: Law of Ukraine dated 24.02.2023 No. 2952-IX. Verkhovna Rada of Ukraine]. Available at: https://zakon.rada.gov.ua/go/2469-19 (accessed 03.09.2023). (In Ukrainian).

34. Pevnev, V. Ya., Toryanyk, V. V., & Kharchenko, V. S. Kiberbezpeka bezprovodovykh smart-system: kanaly vtruchan′ ta radiochastotni vrazlyvosti [Cyber security of wireless smart systems: interference channels and radio frequency vulnerabilitis]. *Radioelektronni i komp'uterni sistemi – Radioelectronic and computer systems*, 2020, no. 4, pp. 79-92. DOI: 10.32620/reks.2020.4.07. (In Ukrainian).

35. Pevnev, V., Frolov, A., Tsuranov, M., & Zemlianko, H. Ensuring the Data Integrity in Infocommunication Systems. *International Journal of Computing*, 2022, vol. 21, no. 2, pp. 228-233. DOI: 10.47839/ijc.21.2.2591.

Received 17.07.2023, Accepted 20.11.2023

РИЗИК-ОРІЄНТОВАНИЙ АНАЛІЗ КІБЕРБЕЗПЕКИ СИСТЕМ БАГАТОФУНКЦІЙНИХ ФЛОТІВ БПЛА: КОНЦЕПТУАЛЬНА МОДЕЛЬ ТА IMECA-МЕТОДИКА

Георгій Землянко, Вячеслав Харченко

Предметом дослідження є забезпечення кібербезпеки систем багатофункційних флотів БПЛА (СБФ БПЛА). **Метою** дослідження є визначення та аналіз ризиків, пов'язаних з кібербезпекою багатофункційних флотів БПЛА, розробка моделей загроз, вразливостей та атак, проведення IMECA аналізу кібератак. **Завдання**: 1) провести аналіз загроз, які можуть впливати на безпеку багатофункційних флотів БПЛА; 2) визначити вразливості системи та їхні можливі наслідки в разі експлуатації; 3) розробити моделей: інфраструктури системи та загроз, вразливостей та атак, враховуючи особливості функціональності та зв'язку між елементами системи; 4) виконати ризик-орієнтований аналіз, визначаючи й категоризуючи потенційні загрози та їхні впливи. Були отримані наступні **результати**. 1. Описані та класифіковані загрози для кібербезпеки багатофункційних флотів БПЛА. 2. Виявлені та проаналізовані вразливості системи та їхні можливі наслідки. 3. Розроблені моделі загроз, вразливостей та кібератак, враховуючи специфіку функціонування флотів БПЛА. 4. Проведений ризик-орієнтований аналіз, визначено рівень загроз та розроблені рекомендації з підвищення кібербезпеки СБФ БПЛА відповідно до результатів, отриманих з використанням IMECA аналізу. **Висновки**. Дослідження підкреслюють важливість розробленої моделі та інструменту для виявлення та аналізу кіберзагроз для СБФ БПЛА. Це дозволяє підвищити рівень кібербезпеки та надійності системи і забезпечити своєчасну реакцію на кіберзагрози. **Напрями подальших досліджень:** розвиток моделі та методу для врахування специфіки кіберзагроз і технологічних особливостей інфраструктури СБФ; розроблення та впровадження проактивних засобів захисту в умовах комбінованих кібератак; розширення області застосування цих інструментів у різних галузях, зокрема, смарт-міст.

Ключові слова: кібербезпека; багатофункційні флоти БПЛА; загрози; вразливості; моделювання атак; ризик-орієнтований аналіз; безпека систем; IMECA.

Землянко Георгій Андрійович – аспірант, асистент каф. комп’ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Харченко Вячеслав Сергійович – д-р техн. наук, проф., зав. каф. комп’ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Heorhii Zemlianko – PhD student, Assistant at the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University “Kharkiv Aviation Institute”, Kharkiv, Ukraine,
e-mail: g.zemlynko@csn.khai.edu, ORCID: 0000-0003-4153-7608, Scopus Author ID: 57214232232.

Vyacheslav Kharchenko – Doctor of Technical Science, Professor, Head of the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University “Kharkiv Aviation Institute”, Kharkiv, Ukraine,
e-mail: v.kharchenko@csn.khai.edu, ORCID: 0000-0001-5352-077X, Scopus Author ID: 22034616000.