UDC 004.054:004.056.53 **DOI:** https://doi.org/10.30837/0135-1710.2025.187.200

A. Abakumov, V. Kharchenko

COMBINED METHOD OF UAV CYBER ASSETS SECURITY ASSESSMENT BY USE OF PROCEDURES IMECA AND PENETRATION TESTING

Subject of the research is determined as methods and tools for security assessment of cyber assets of unmanned aerial vehicles (UAVs). The conclusion about a certain gap between theoretical risk assessment methods and practical penetration testing (PT) tools for UAV cyber assets was drawn based on an analysis of publications. Existing PT tools focus on attack reproduction, although they do not provide a methodology for the assessment of their impact in dynamic application environments. **Objective of the research** is to develop a combined method and elements of technology for reliable vulnerability detection with the possibility to verify the process and reason the selection of countermeasures. **Research tasks** include feasibility reasoning of combined use of various methods and tools for assessing UAV cybersecurity; development of models and an assessment method combining analytical and experimental procedures; practical execution of the method using a test environment. **Methods used:** Intrusion Modes and Criticality Analysis (IMECA) and PT. **Research results**: structure and sequence of combined cybersecurity assessment; functional IDEF0 model that ensures the completeness of the security assessment of UAV cyber assets and consists of the following stages: information gathering and vulnerability assessment, intrusion modes replication, IMECA-analysis (including preliminary and a posteriori IMECA-analysis), and countermeasure selection; deployed and tested test environment based on DVD simulator, capable of reproducing 80 % of priority intrusion modes. **Conclusions:** the combined method for security assessment of UAV cyber assets integrates IMECA procedures with PT practices, which allows to overcome the limitations of static risk assessment methods and isolated technical tests, creating a closed loop of verification and protection of on-board systems. Further research involves conducting a full-scale series of experiments for all identified intrusion modes, constructing a posteriori criticality matrices, and selecting countermeasures, as well as integration of the proposed method with the task of the functional safety assessment of unmanned systems.

Keywords: UAV cyber assets; IMECA-analysis; combined method; intrusion mode simulation; penetration testing.

1. Introduction

The rapid growth in the use of small unmanned aerial vehicles (UAVs), better known as "drones", can be observed in the following areas [1]:

- monitoring of hard-to-reach areas, real-time disaster relief;
- provision of services for smart cities;
- aerial photography, cinematography;
- precision agriculture (irrigation, phytopathology, soil mapping, farmer data analysis);
- traffic monitoring to obtain real-time information on road conditions;
- technical inspection and security monitoring of critical infrastructure facilities;
- reconnaissance, patrolling, logistics, demining, fire correction in combat conditions.

Since 2022, such UAVs have been actively used by the Armed Forces of Ukraine in countering Russia's full-scale aggression against Ukraine. Experience with the use of [2–6] UAVs has shown that high-tech devices can become targets of successful cyber attacks, not to mention civilian UAVs that are adapted for use in military operations. In combat zones, massive signal interference leads to significant UAV losses. For example, thousands of UAVs are shot down every month in Ukraine, mainly due to attacks that jam GPS navigation and control channels [7]. Zachary Kallenborn, a research associate at George Mason University, writes: "You can use them more aggressively because you don't care if they get lost" [2].

However, commercial UAVs require additional adaptation for military use, such as the use of special firmware that prevents detection by enemy aerial reconnaissance systems. In addition, it should be noted that software (SW) is constantly being updated, so outdated modified firmware becomes unusable in newer versions of UAVs.

These examples only emphasize the need for a systematic assessment of the security of cyber-physical components of UAVs [8], namely the analysis of potential threats and the identification of vulnerabilities (including zero-day vulnerabilities) before they are exploited by attackers, which could not only lead to the loss of the device itself during a mission, but also pose a threat to the lives of operators.

2. Analysis of recent studies and publications

An analysis of sources on the assessment of UAV cybersecurity (CS) and existing penetration testing (PT) methodologies adapted to the specifics of UAVs is provided based on a study of leading scientific databases, including Scopus, IEEE Xplore, and Google Scholar, published after 2020.

Table 1 provides the key ones, in the authors' opinion.

Table 1. *Classification of reviewed sources by research areas*

Research area	Sources
Threats, vulnerabilities of UAV components	[1, 5, 8–10]
Risk-oriented analysis and assessment of UAV vulnerabilities	[11–14]
UAV penetration testing	[15]

The paper [5] discusses numerous examples of malicious use of UAVs and analyzes possible attack vectors in civil and military scenarios. It shows that UAVs are vulnerable to a wide range of attacks and emphasizes the importance of implementing measures to detect and prevent them. [9] argues that UAV design problems are becoming increasingly apparent with the transition to mass military use, systematizes risks according to CIA aspects, and methods for analyzing vulnerabilities in UAV software.

The author of [10] presented a comprehensive classification of cyberattacks on UAVs, which can be used as a basis for threat modeling.

The work [11] considers the issue of assessing the design of multifunctional UAV fleets, identifies threats, vulnerabilities, and the potential consequences of cyberattacks, considering the characteristics of the interaction of system elements. The authors proposed a multi-level model of threats and attack scenarios, taking into account the functional distribution in the UAV infrastructure. A key methodological component of the study is the use of the Intrusion Modes and Effects Criticality (IMECA) method, which allows threats to be classified by level of criticality, the consequences of attacks to be modeled, and recommendations for improving system security to be formulated. [12] presents a model for the security of Internet of Drones (IoD) systems, focused on monitoring critical infrastructure. The authors analyzed so-called radio frequency vulnerabilities and applied IMECA to construct a risk matrix that considers the probability and criticality of intrusions.

Article [13] addresses the problem of the lack of a standardized method for assessing the overall security level of UAVs. The authors propose D3S (Drone Security Scoring System) – a methodology for assessing and assigning a security score to specific drone models based on the analysis of their components and resistance to attacks. In [14], the critical need for a structured methodology for assessing the security of UAVs is justified, given their integration into cyber-physical systems and the Internet of Things. The authors propose a systematic step-by-step approach that combines threat modeling, vulnerability analysis, assessment, and selection of appropriate countermeasures based on the assessment results.

Drone Attack Tool (DRAT) is a UAV PT framework proposed in [15] and designed to automate the process of finding vulnerabilities in commercial UAVs. The main goal of the tool is to reduce dependence on the operator's deep expertise and manual execution of complex attack scenarios by combining the necessary resources in a single graphical interface.

3. Research objectives and tasks

The analysis of sources indicates a gap between theoretical risk assessment methods and practical UAV penetration testing tools. Existing approaches to risk assessment (e.g., D3S) do not consider the actual exploitation of vulnerabilities in the dynamic conditions of UAV use. At the same time, existing PT tools (e.g., DRAT) focus on reproducing attacks but do not provide a methodology for assessing their impact.

Therefore, the purpose of the study is to develop a combined method and elements of technology for reliable vulnerability detection with the possibility of verifying the process and justifying the choice of countermeasures.

Research objectives:

- to justify the feasibility of the combined use of various methods and means of assessing the cybersecurity of UAVs;
- to develop an assessment method that includes analytical and experimental procedures;
- to test the method in practice using an appropriate test environment.

4. Materials and methods

One of the previous studies [16] analyzed several combinations of analytical and experimental methods for assessing security and cybersecurity (CS), considering such indicators as completeness, execution time, cost, and reliability of such assessment.

The analysis showed that the combination of the risk-oriented IMECA method [11, 12, 17] with PT [18, 19] best meets the requirements for CS analysis of unmanned intelligent systems (UIS).

Accordingly, the proposed combined method for assessing the security of UAV cyber assets using IMECA-analysis and PT procedures (hereinafter referred to as the combined method) can also be applied to assess the CS of unmanned aerial vehicles (UAVs). In the context of this study, UAV cyber assets are understood as a complex set of components that ensure the functioning of the system: a digital flight platform (including sensors and onboard software), a ground control station, as well as data and command transmission channels [20].

The essence of the combined method is to assess the security of UAV cyber assets by integrating IMECA-analysis procedures in preparatory and a posteriori forms with PT procedures to create an end-to-end cycle of verification of compliance with asset security requirements.

This approach determines its advantages, namely the reduction of residual vulnerability risks through improved test coverage and, as a result, the reduction of successful intrusion risks.

This work provides a detailed description of the processes of evaluating CS using the proposed method. To formalize and structurally describe the proposed method, the Integrated Definition for Function Modeling (IDEF0) methodology was chosen. This choice is due to the need to detail the processes of transforming input information (data on architecture, application scenarios, constraints) into results (risk assessments and a set of countermeasures) with a clear definition of control elements and necessary resources.

The hierarchical nature of IDEF0 provides the ability to step-by-step detail (decompose) complex assessment procedures, which allows maintaining the logical integrity of the method when integrating heterogeneous components: analytical IMECA-analysis and experimental PT.

4.1. General model of the combined method

The proposed combined method, presented in Figure 1 in the form of an IDEF0 context diagram, is based on a holistic process aimed at identifying, analyzing, confirming, and minimizing cyber risks.

At the entrance, information about the object of study is formed: the architecture and components of the UAV (I-ARCH), scenarios for its use (I-SCEN), as well as legal, operational, and technical restrictions (I-LIM).

The assessment process is implemented through a sequence of interrelated stages, which are provided by the corresponding set of tools (mechanisms) marked with red arrows in the diagram.

The process is strictly regulated by a set of control elements, which are shown in the diagram with blue arrows.

The result is a package of output data that includes a justified set of countermeasures (O-COUNTER), residual risk matrices (O-MATRIX), and a detailed report on the assessment of the impact on the UAV mission (O-IMPACT).

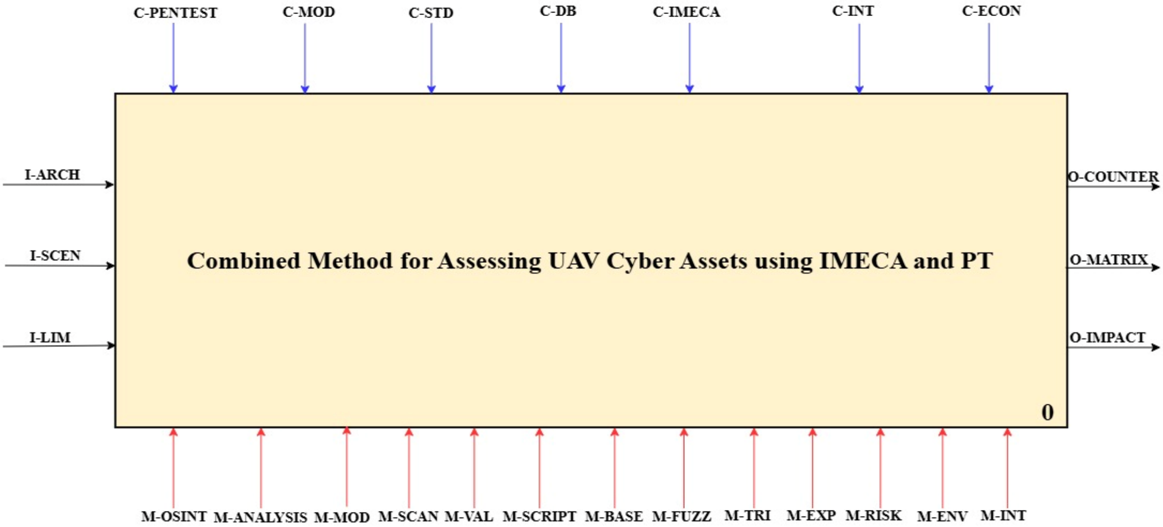


Fig. 1. Context diagram IDEF0 of the combined method (level A0)

4.2. Model decomposition and main stages of the combined method

Figure 2 shows the decomposed model of the combined method (level A1). It combines the classic stages of PT: information gathering and system analysis (1), assessment of known (2) and detection of unknown vulnerabilities (3), intrusion mode replication (5), as well as integrated IMECA-analysis in its preliminary (4) and a posterior (6) forms into a continuous process.

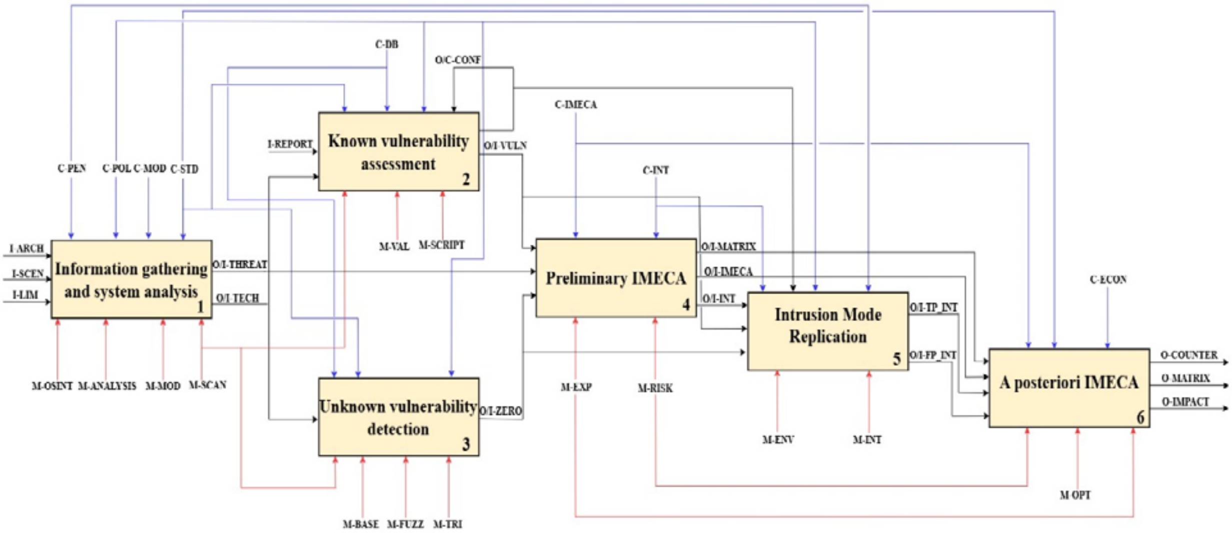


Fig. 2. Decomposed model of the combined method (level A1)

At the first stage of information gathering and system analysis, the research context is formed, and vulnerabilities and potential threats to the UAV under study are identified. Using OSINT tools (M-OSINT), automated scanners (M-SCAN), modeling tools (M-MOD), and analysis tools (M-ANALYSIS), a stack of UAV component technologies (O/I-TECH) and a list of potential threats (O/I-THREAT) are formed. The actions of researchers are guided by the C-PEN methodology, defined by C-MOD modeling frameworks, regulated by CS standards (C-STD), and governed by the terms of use of OSINT and automated scanning tools (C-POL), which impose additional technical and legal restrictions to avoid ethical violations. The further process branches into two parallel procedures: assessment of known vulnerabilities and detection of unknown vulnerabilities.

The goal of the second stage is to assess known vulnerabilities (O/I-VULN) by comparing UAV components with the vulnerability database (C-DB) and community reports (I-REPORT). At this stage, researchers actively use automated scanners (M-SCAN), vulnerability validation tools (M-VAL), and scripts to retrieve information from DBs (M-SCRIPT).

The functional purpose of the third stage is to identify zero-day vulnerabilities (O/I-ZERO) in UAV components that cannot be detected by automated means. Based on the input list of threats (O/I-THREAT) and the technology stack (O/I-TECH), researchers form a reference behavior model and analyze attack surfaces using basic and static analysis tools (M-BASE). Next, dynamic fuzzing (M-FUZZ) is performed to provoke failures, followed by triage and analysis of the root causes of anomalies (M-TRI) to confirm the criticality of the vulnerabilities found. The entire process is regulated by CS standards (C-STD) and terms of use (C-POL). Identified known and newly discovered vulnerabilities are consolidated and transferred to the preliminary IMECA-analysis input.

The purpose of the fourth stage is to analytically transform vulnerability data into an assessment of the risks to UAV missions. Based on the input lists of threats (O/I-THREAT), known vulnerabilities (O/I-VULN), and zero-day vulnerabilities (O/I-ZERO), attack vectors are mapped to intrusion modes. This process is regulated by the IMECA methodology and its assessment scales (C-IMECA), as well as intrusion models (C-INT). Using expert analysis (M-EXP) and risk assessment tools (M-RISK), a hypothesis about the level of danger is formed and a preliminary assessment of the probability, complexity of implementation, and severity of consequences is carried out. The result of this stage is the formation of preliminary criticality matrices (O-MATRIX) and prioritized attack scenarios (O/I-INT).

The fifth stage consists of practical verification of theoretical attack vectors in a controlled laboratory environment. Based on prioritized modes (O/I-INT), researchers reproduce scenarios using a specialized environment and equipment (M-ENV), including UAV simulator and PT operating systems, as well as appropriate intrusion tools (M-INT). The exploitation process is regulated by intrusion models (C-INT) and based on commonly accepted PT methodologies (C-PEN), such as PTES [21] or OSSTMM [22]. The result of this stage is an objective differentiation between successful confirmed intrusions (O/I-TP_INT) and refuted false positives (O/I-FP_INT).

The last stage consists of a final synthesis of the results and decisions on system protection. Based on empirical data on successful (O/I-TP_INT) and refuted (O/I-FP_INT) intrusions, as well as the initial matrix (O/I-MATRIX), the criticality of threats is reassessed. The key mechanism of this stage is optimization algorithms (M-OPT), which allow the selection of countermeasures to be automated. The process is managed taking into account cost-effectiveness criteria (C-ECON), which ensure that costs are minimized while achieving the required level of security. The result of the work is an updated criticality matrix (O-MATRIX), an impact assessment report (O-IMPACT), and a final set of recommended countermeasures (O-COUNTER), which guarantees an acceptable level of residual risk.

For a deeper understanding of the algorithm of actions when applying the combined method, a detailed description of each stage of the presented IDEF0 model is given below.

4.3. Details of the stages of the combined method

4.3.1. Information gathering and system analysis

Figure 3 shows the decomposition of the information gathering and system analysis stage. The model details the process by breaking it down into four functional blocks: passive reconnaissance (1), active reconnaissance (2), system components mapping (3), and identification of potential threats (4).

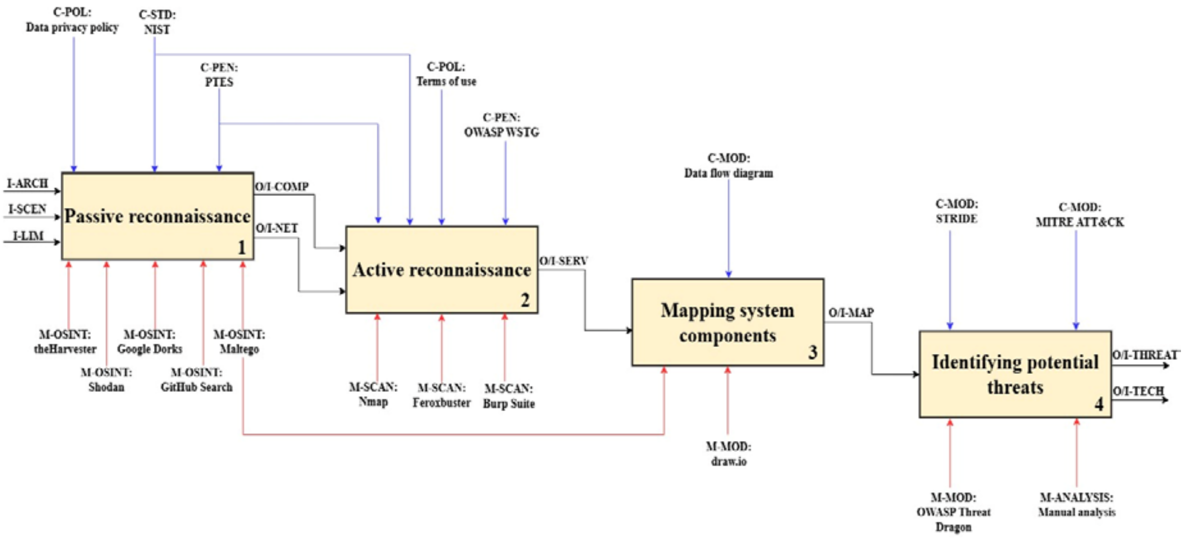


Fig. 3. Decomposed model of the information gathering and system analysis stage

Based on input data about the architecture (I-ARCH), usage scenarios (I-SCEN), and existing limitations (I-LIM), researchers use OSINT tools to form a preliminary network map (O/I-NET) and a list of UAV components (O/I-COMP). This includes searching for vulnerabilities via Shodan and theHarvester, analyzing data leaks using Google Dorks, researching code repositories via GitHub Search, and visualizing relationships in Maltego. Activities are strictly regulated by NIST standards [23] (C-STD) and PTES methodology (C-PEN), with the key restriction being the data privacy policy (C-POL), which excludes privacy violations.

The purpose of the active reconnaissance phase is to verify the collected data and identify entry points through direct interaction with UAV interfaces. The input data consists of identified components and a network map from the previous phase. Nmap is used to scan ports and services, and Feroxbuster and Burp Suite (M-SCAN) tools are used to analyze web interfaces and APIs. The process is governed by PTES [21] and OWASP Web Security Testing Guide (OWASP WSTG) [24] (C-PEN) methodologies. A critical aspect of management is compliance with the terms of use (C-POL), which define the permissible limits of interference to avoid destabilizing the operation of the UAV. The result is a confirmed list of active services (O/I-SERV).

The functional purpose of the system component mapping stage is to build a detailed model of UAV component interaction based on data about active services (O/I-SERV). Using the draw.io modeling tool (M-MOD), researchers systematize the information obtained in the form of a component map (O/I-MAP). The construction process is guided by the principles of creating data flow diagrams (C-MOD), which allows visualizing the vectors of information transfer between system modules and preparing the groundwork for threat modeling.

The final stage is aimed at identifying potential threats (O/I-THREAT) and forming a technology stack (O/I-TECH). Based on the component map (O/I-MAP), a security analysis is performed using the automated OWASP Threat Dragon tool (M-MOD) and manual analysis (M-ANALYSIS). The threat modeling process is regulated by the STRIDE methodology (for classifying attack types) and the MITRE ATT&CK knowledge base (C-MOD), which covers a wide range of known attacker tactics and techniques.

4.3.2. Assessment of known vulnerabilities

Figure 4 shows a model that details the process of assessing known vulnerabilities into three functional blocks: matching components with vulnerabilities DB (1), automated scanning (2), and scanning results validation (3).

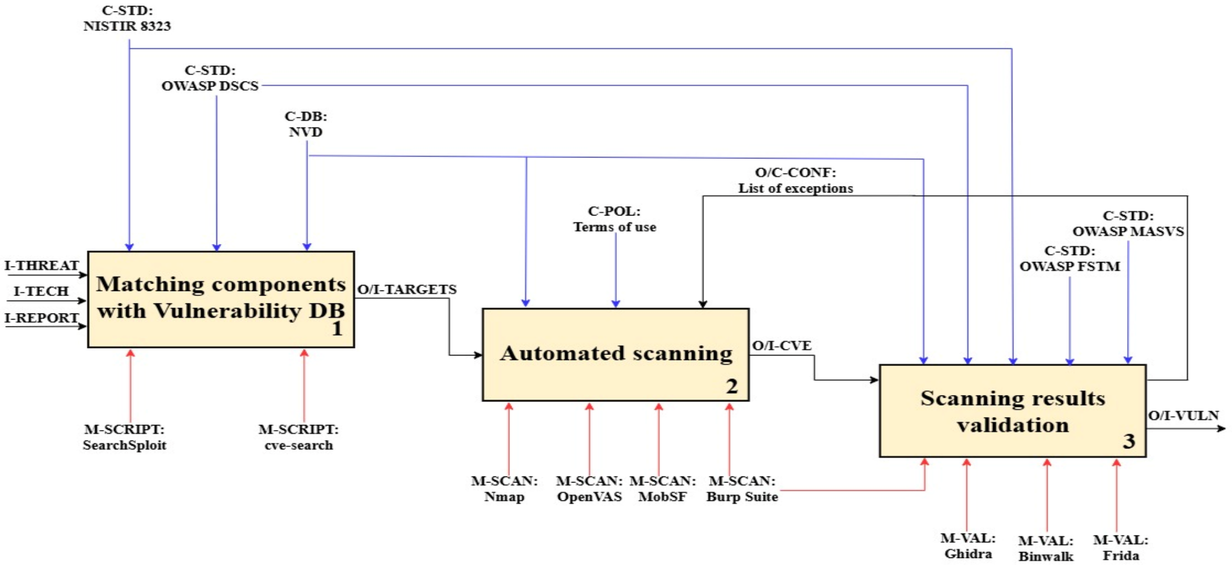


Fig. 4. Decomposed model of the known vulnerability assessment stage

The functional purpose of the first stage is to analytically identify potential vulnerabilities by correlating detected UAV components with known records in the database. Based on input data about threats (I-THREAT), technology stacks (I-TECH), and community reports (I-REPORT), researchers use exploit search tools and online database queries, such as SearchSploit and cve-search (M-SCRIPT). The search is regulated by the NISTIR 8323 standard (C-STD) and the recommendations of the specialized OWASP Drone Security Cheat Sheet (OWASP DSCS) reference guide. The result of the work is a list of potential targets (O/I-TARGETS) for further scanning verification.

The purpose of automated scanning is to actively check identified targets for vulnerabilities. Researchers use the M-SCAN suite of tools, which includes Nmap (port scanner), OpenVAS (vulnerability scanner), MobSF (mobile application analysis), and Burp Suite (web vulnerability proxy scanner). A critical aspect of management is strict adherence to terms of use (C-POL) to prevent system destabilization, as well as consideration of the list of exceptions (O/C-CONF). The result is a list of vulnerabilities and their CVE identifiers (O/I-CVE).

The final stage is aimed at validating the identified vulnerabilities to filter out false positives. For this purpose, reverse engineering (Ghidra), firmware analysis (Binwalk), and dynamic instrumentation (Frida) tools are used (M-VAL). The validation process is based on specialized standards for testing firmware, such as OWASP Firmware Security Testing Methodology (OWASP FSTM) and mobile applications – OWASP Mobile Application Security Verification Standard (OWASP MASVS), as well as the general standard NISTIR 8323. The result is a list of confirmed known vulnerabilities (O/I-VULN) and an updated list of exceptions (O/C-CONF), which is returned to the automatic scanning stage to improve its accuracy in subsequent iterations.

4.3.3. Detection of unknown vulnerabilities

The decomposition of the third stage of the combined method is shown in Figure 5. The model details the process of detecting unknown vulnerabilities into three functional blocks: attack surface analysis (1), fuzzing and anomaly detection (2), triage and root cause analysis (3).

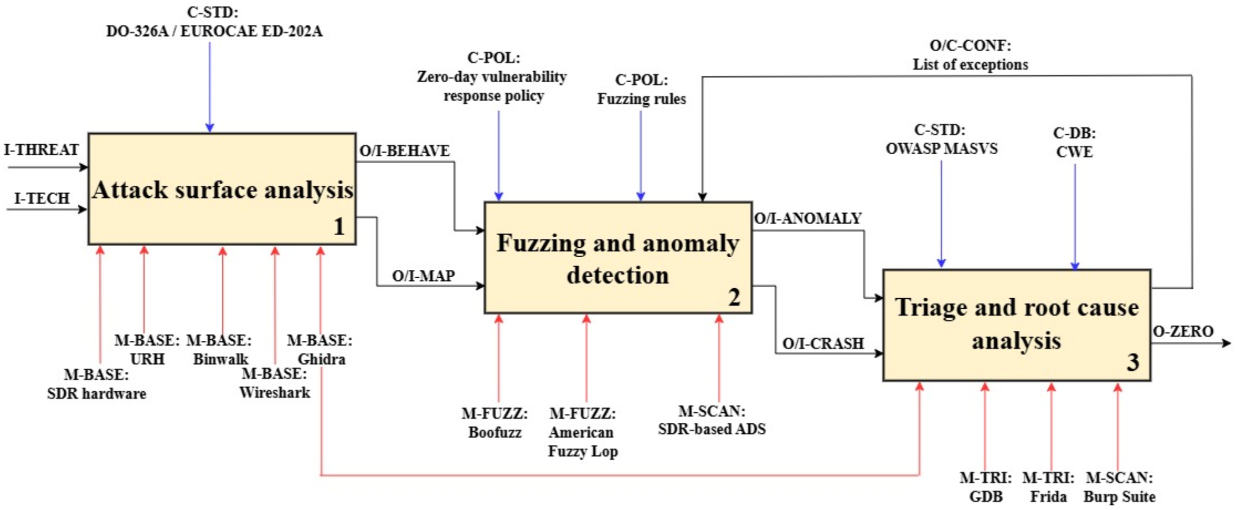


Fig. 5. Decomposed model of the stage of identifying unknown vulnerabilities

The purpose of the attack surface analysis stage is to create a model of normal UAV behavior and to map entry points in detail. Based on threat data (I-THREAT) and technology stack (I-TECH), a reference behavior profile (O/I-BEHAVE) and an attack surface map (O/I-MAP) are generated. Technical implementation is provided by the M-BASE suite of tools: SDR hardware is used for physical signal interception, which is then processed in URH and Wireshark for protocol analysis. Binwalk and Ghidra are used in parallel for static firmware analysis. The process is strictly regulated by DO-326A / EUROCAE ED-202A (C-STD) airworthiness safety standards, which define the requirements for security architecture.

The fuzzing and anomaly detection stage is a dynamic phase of active provocation of system malfunctions. Using a reference profile and attack map, as well as considering a list of exceptions from previous iterations (O/C-CONF), researchers apply fuzzing tools (M-FUZZ): the Boofuzz framework and the American Fuzzy Lop phaser to generate mutated data. Simultaneously with the attack, an SDR-based anomaly detection system (ADS) (M-SCAN) operates, performing external monitoring of the airwaves to record deviations. The process is managed in accordance with the zero-day vulnerability response policy and fuzzing rules (C-POL). The result is recorded reports of detected anomalies (O/I-ANOMALY) and critical failure logs (O/I-CRASH).

The final stage is aimed at verifying the anomalies found and determining the technical cause of the failure. Using M-TRI tools (GDB and Frida), researchers perform debugging and dynamic instrumentation of processes, and Burp Suite (M-SCAN) is used to analyze web vulnerabilities. The classification of detected defects is carried out based on CWE (C-DB) and in accordance with the OWASP MASVS standard (C-STD). Confirmed critical defects are recorded as zero-day vulnerabilities (O-ZERO), and false positives are added to the list of exceptions (O/C-CONF), which is returned to the fuzzing stage for testing optimization.

4.3.4. Preliminary IMECA-analysis

Figure 6 shows the decomposition of the fourth stage of the model – preparatory IMECA analysis, which consists of three functional blocks: identification of intrusion modes (1), assessment of intrusion parameters (2), and risk prioritization (3).

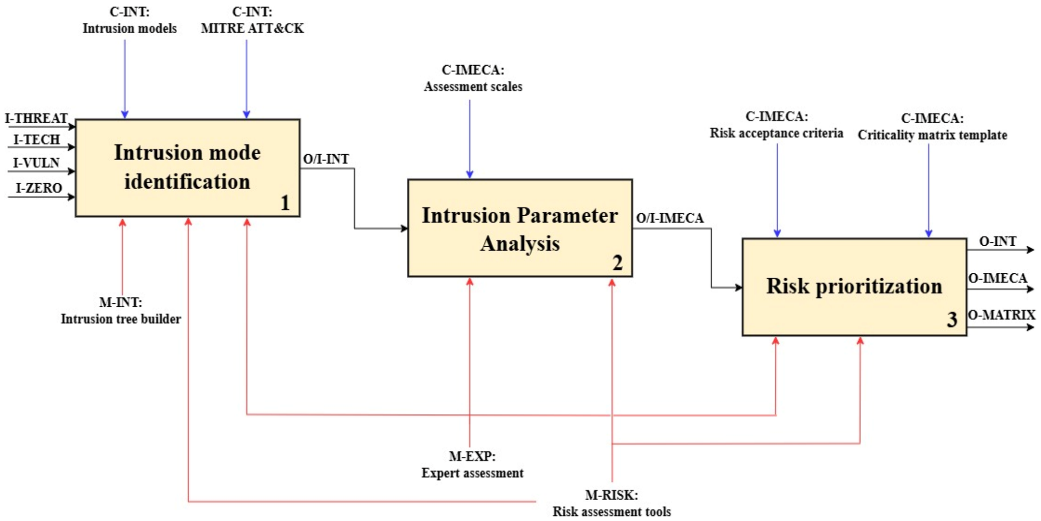


Fig. 6. Decomposed model of the preparatory IMECA-analysis stage

The purpose of intrusion mode identification is to synthesize technical data on vulnerabilities with abstract threat models to form specific intrusion scenarios. Based on input data about threats (I-THREAT), technology stack (I-TECH), known (I-VULN) and unknown (I-ZERO) vulnerabilities, experts transform vulnerability information into logical chains of attacker actions. This process is carried out using an intrusion tree constructor (M-INT) and expert assessment (M-EXP), guided by the MITRE ATT&CK tactics DB and intrusion models (C-INT). The result of this stage is a comprehensive list of identified intrusion modes (O/I-INT), which considers the specifics of combined attacks.

The next stage involves a preliminary quantitative and qualitative assessment of the identified intrusion modes. Experts (M-EXP) use approved assessment scales (C-IMECA) to determine key risk parameters: probability of occurrence, complexity of implementation, and severity of consequences. To reduce the subjectivity of expert judgments and automate calculations, risk assessment tools (M-RISK) are used, such as AXMEA [25]. The output of this stage is a structured table with preliminary assessments (O/I-IMECA).

The final stage is aimed at ranking threats to determine the focus of further experiments. Based on the completed table (O/I-IMECA) and using risk assessment tools (M-RISK), threats are visualized on a "probability-severity" plane according to the criticality matrix template (C-IMECA). The key control element is the risk acceptance criteria (C-IMECA), which define threshold values: scenarios that fall into the unacceptable risk zone are highlighted in a priority list (O-INT) for mandatory replication, and a criticality matrix (O-MATRIX) is formed.

4.3.5. Replication of intrusion modes

Figure 7 shows the decomposition of the fifth stage of the combined method. The model details the stage of replication of intrusion modes into three functional blocks: environment setup (1), operation (2), and post-operation (3).

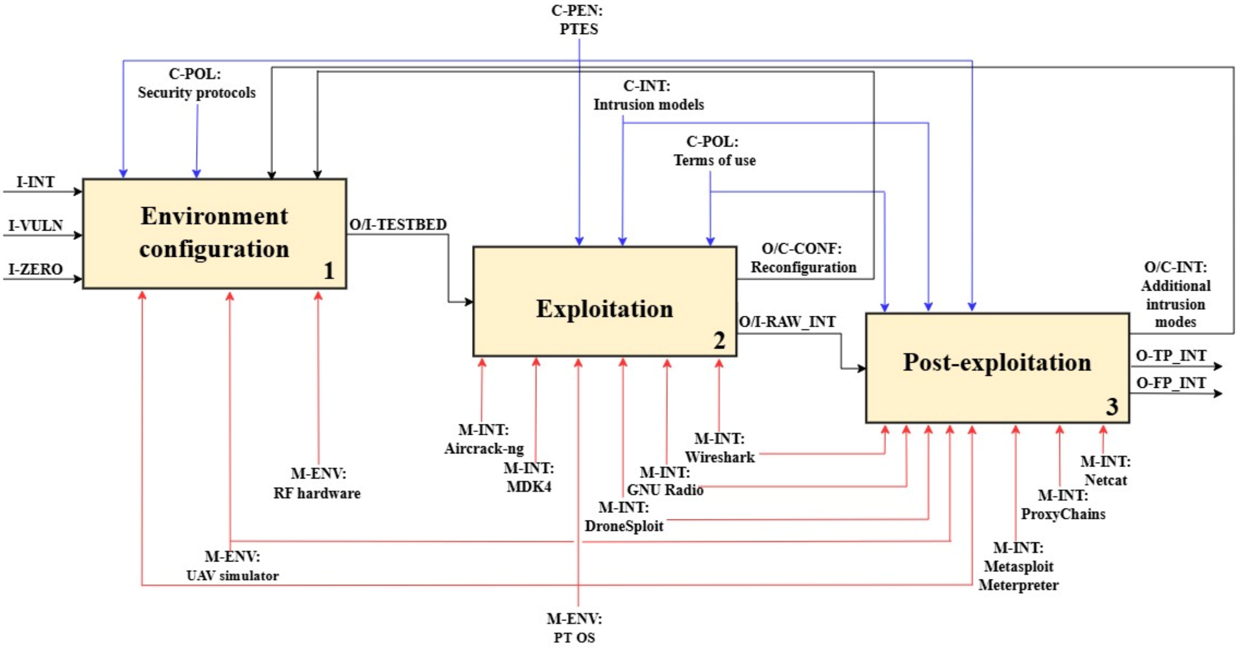


Fig. 7. Decomposed model of the replication stage of intrusion modes

The goal of the first stage is to prepare an isolated and controlled environment for the safe reproduction of intrusions. Based on prioritized modes (I-INT) and vulnerability data (I-VULN, I-ZERO), a test bed (O/I-TESTBED) is deployed. Technical implementation is provided by a set of M-ENV tools: deployment of a specialized OS (e.g., Kali Linux), configuration of a UAV simulator to create digital twins, and calibration of RF hardware. The process is strictly regulated by security protocols (C-POL) for test isolation and rules of use, and feedback from the next stage (O/C-CONF) allows for quick adjustments to the test bed configuration.

The operational stage is aimed at the direct implementation of intrusions on the prepared test bed. Researchers use a wide range of M-INT tools: Aircrack-ng and MDK4 are used for Wi-Fi attacks, the DroneSploit framework is used to exploit specific UAV vulnerabilities, and GNU Radio is used to work with radio waves. Traffic monitoring and analysis is performed using Wireshark. Actions are managed according to the PTES (C-PEN) methodology and approved intrusion models (C-INT). The result of this stage is the receipt of preliminary "raw" intrusion results (O/I-RAW_INT) or a request to reconfigure the environment (O/C-CONF) in case of failure.

The final stage focuses on securing the system, assessing the depth of penetration, and collecting evidence. Using M-INT tools, researchers establish persistent control over the device (via Metasploit Meterpreter and Netcat) and use ProxyChains to tunnel traffic. The process is governed by PTES rules and term of use (C-POL). If new attack vectors are discovered during the operation, they are returned to the beginning of the cycle as additional modes (O/C-INT). The result is verified data: confirmed successful intrusions (O-TP_INT) and refuted false hypotheses (O-FP_INT), which are transferred to the a posteriori IMECA-analysis.

4.3.6. A posteriori IMECA-analysis

Figure 8 shows the decomposition of the last stage of the combined method. The model details the posterior IMECA-analysis into three functional blocks: intrusion criticality reassessment (1), countermeasure selection (2), and residual risk assessment (3).

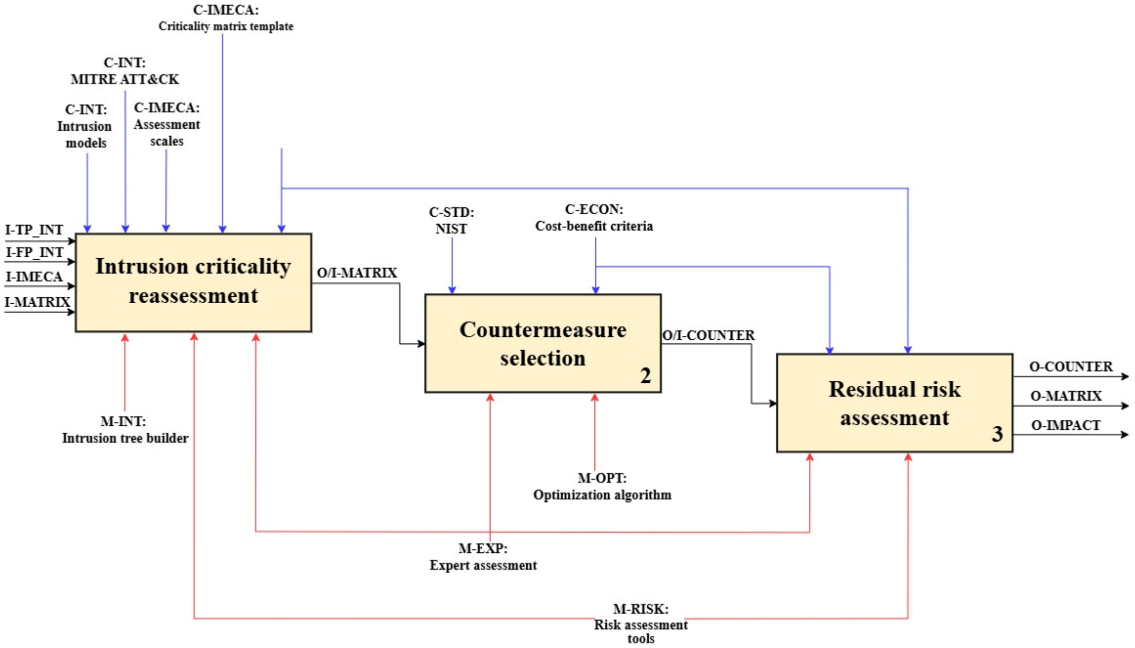

C-IMECA: Criticality matrix template
C-INT: MITRE ATT&CK
C-INT: Intrusion models
C-IMECA: Assessment scales
I-TP_INT
I-FP_INT
I-IMECA
I-MATRIX
Intrusion criticality reassessment
O/I-MATRIX
C-STD: NIST
C-ECON: Cost-benefit criteria
Countermeasure selection
2
O/I-COUNTER
Residual risk assessment
3
O-COUNTER
O-MATRIX
O-IMPACT
M-INT: Intrusion tree builder
M-OPT: Optimization algorithm
M-EXP: Expert assessment
M-RISK: Risk assessment tools

Fig. 8. Decomposed model of the a posteriori IMECA analysis stage

The goal of the first stage is to update risk assessments based on empirical data obtained during the replication of intrusion modes. Input data on confirmed (I-TP_INT) and false (I-FP_INT) attacks, together with initial tables (I-IMECA, I-MATRIX), are processed by experts (M-EXP) using intrusion tree builders (M-INT). This makes it possible to visualize verified compromise paths and adjust probability parameters to real values. The process is regulated by approved assessment scales, risk acceptance criteria (C-IMECA), and intrusion models (C-INT). The result is a validated criticality matrix (O/I-MATRIX) that reflects the actual state of system security.

The second stage involves the formation of a set of measures to neutralize critical risks. Using optimization algorithms (M-OPT) and expert assessment (M-EXP), researchers select countermeasures from security standards catalogs such as NIST (C-STD). The key constraint is the cost-benefit criteria (C-ECON), which ensure the implementation of the "minimum cost acceptable risk" principle. This allows us to weed out overly expensive solutions for protection against unlikely threats. The result is a pre-formed set of recommended countermeasures (O/I-COUNTER).

The final stage involves modeling the state of the system after the hypothetical implementation of the selected countermeasures. Risk assessment tools (M-RISK) and expert analysis (M-EXP) are used to calculate the residual risk for each scenario. If the risk level meets the acceptance criteria (C-IMECA) and is in the "green zone" of the matrix, the process ends with the formation of a final set of countermeasures (O-COUNTER), a residual risk matrix (O-MATRIX), and an impact assessment report (O-IMPACT).

5. Research results and their discussion

5.1. Analysis of preliminary results

The experimental study used the results of a preliminary study [19], in which IMECA tables of intrusion modes and criticality matrices were constructed based on the developed threat models for UAV application scenarios.

Analysis of the results showed that the most critical intrusion modes in UAV mission scenarios in terms of severity of consequences are: spoofing, jamming, man-in-the-middle and replay attacks, session hijacking, and optical blinding. Therefore, these intrusion modes were selected as priorities for further practical replication.

5.2. Building a test environment

Given the current martial law conditions in Ukraine, as well as the lack of safe areas for field testing and the instability of the power supply, it was decided to verify vulnerabilities in a simulated environment.

The Damn Vulnerable Drone (DVD) [26] specialized simulator was selected as the target system, which allows emulating UAV vulnerabilities. This tool was chosen because of its architectural advantages, which are based on the Software-in-the-Loop (SITL) principle, as this approach to simulation allows real UAV software to be run in a virtual environment that is as close as possible to its execution on physical equipment.

Advantages of using the simulator in the context of further research:

- The use of ArduPilot in the DVD simulator allows you to execute real binary firmware code, which ensures the sensitivity of UAV components to various commands and input data.
- Integration with Gazebo provides realistic physical simulation of flight and interaction with the environment, allowing for accurate analysis of possible consequences and intrusion scenarios.
- Although the proposed simulator does not reproduce the architecture of every real-world UAV model, the vulnerabilities injected into it are characteristic of many types of UAVs.

An analysis of the documentation and a review of the simulator's functionality confirmed the possibility of reproducing most of the above-mentioned intrusion modes:

- Despite the impossibility of physical RF spoofing, DVD allows logical spoofing by entering artificial GPS coordinates directly into the data stream, forcing the UAV to accept the false location as valid.
- Jamming can be implemented in DVD as a denial-of-service attack at the channel or application levels, resulting in loss of control, similar to the action of electronic warfare (EW).
- In the DVD simulator, the connection between the ground station and the UAV is emulated via a TCP/UDP connection, which is suitable for reproducing man-in-the-middle attacks and allows telemetry to be intercepted and flight commands to be modified in real time.
- The ability to capture traffic in the DVD environment allows for the replay of commands, verifying the absence of replay protection in the protocols used.
- The simulator is vulnerable to control session interception, especially in scenarios using unprotected protocols (such as Telnet, FTP) or through Wi-Fi session interception.

Three approaches were used in the process of deploying the test environment:

- Virtualization (Windows 11 + Hyper-V): An attempt to deploy via GPU Passthrough revealed a conflict between Nvidia drivers and the xRDP subsystem in the Kali Linux environment. As a result, only the Lite version of the simulator could be launched, which did not provide full functionality for replicating complex intrusion modes.
- ARM architecture (M1-based Macbook + Parallels): A fundamental incompatibility of a number of simulator components with the ARM architecture was discovered.
- Dedicated station (Bare Metal Kali Linux): The most effective solution was to deploy the simulator on a separate desktop PC running Kali Linux OS. This allowed us to avoid problems with hardware resource virtualization and gain access to the full version of the simulator. The specifications of the current test environment are shown in Table 2.

Limitations of the current configuration:

- Despite its successful deployment, this stand is characterized by low mobility and requires a continuous power supply, which limits the possibility of conducting experiments in the absence of electricity.
- The performance of the current CPU is quite low, especially when emulating complex intrusion modes while using attack and monitoring tools.

Table 2. *TTX of the test environment*

Component	Name
CPU	Intel Core i5-6700
GPU	Nvidia GeForce GTX 1660 Ti
RAM	16 Гб
Storage	SSD 256 Гб
PT OS	Kali Linux
UAV simulator	DVD based on ArduPilot/MAVLink architecture

Additional limitations of the test environment:

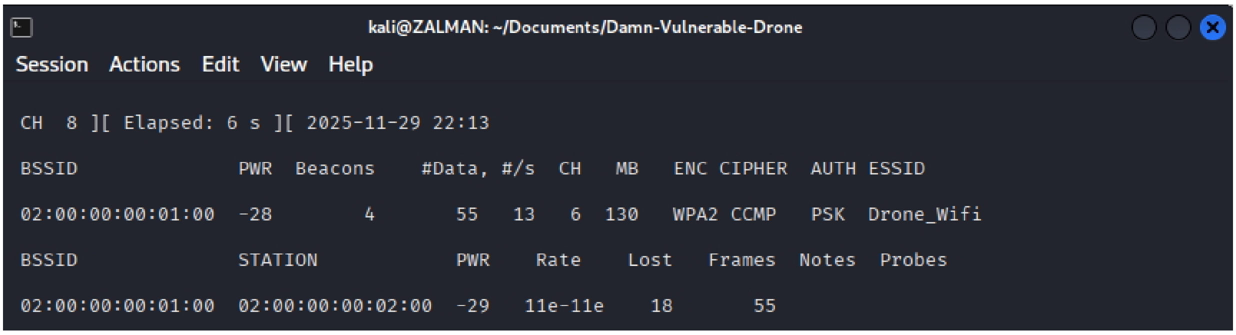
- Attacks on physical sensors, such as optical blinding of a camera with a laser, cannot be reproduced because the simulator's virtual camera receives images from a graphics engine and does not have a physical matrix sensitive to light saturation.
- The simulator does not reproduce the battery discharge process, so attacks aimed at preventing the transition to sleep mode or increasing the load on the CPU will not work.
- In the simulator, attacks on communication channel availability are implemented through packet injection or software connection termination. However, this does not take into account the physical aspects of electronic warfare (signal strength, weather conditions, terrain, and antenna characteristics).

These limitations narrow the scope of testing the combined method in the current iteration to the logical and network levels. Assessing physical resilience and protection against kinetic and/or energy attacks requires a transition to hybrid Hardware-In-The-Loop (HITL) modeling in subsequent stages of the study.

5.3. Practical testing of the test environment

To confirm the ability of the deployed test environment to replicate intrusion modes, an attack scenario on the UAV wireless control channel was implemented. The purpose of the experiment was to test the possibility of unauthorized access to the control network protected by the WPA2 protocol, which corresponds to the intrusion mode – "session interception".

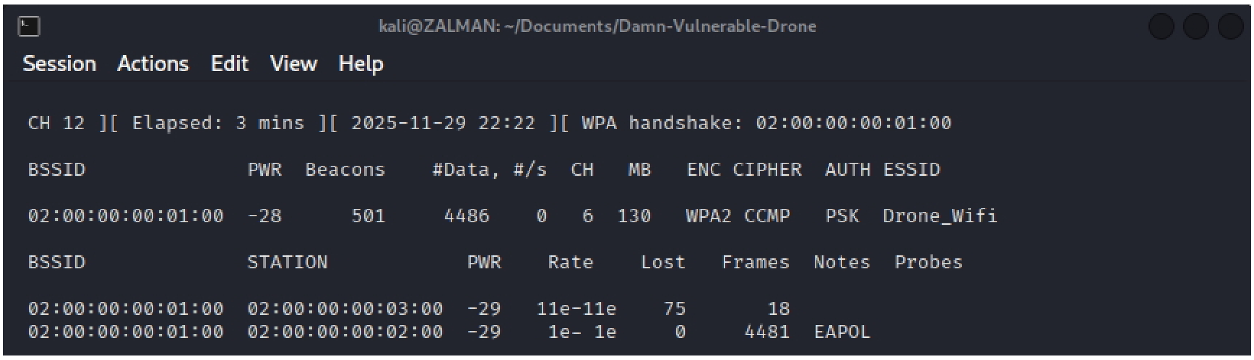
The use of the built-in airodump-ng utility allowed us to scan the airwaves and identify the target network (SSID), its BSSID (MAC address), operating channel, and encryption type (WPA2-PSK/CCMP). A ground station connected to the network was also identified.



```
CH  8 ][ Elapsed: 6 s ][ 2025-11-29 22:13

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

02:00:00:00:01:00  -28        4       55   13   6  130   WPA2 CCMP   PSK  Drone_Wifi

BSSID              STATION            PWR    Rate    Lost    Frames  Notes  Probes

02:00:00:00:01:00  02:00:00:00:02:00  -29    11e-11e    18       55
```

Fig. 9. Result of scanning with the airodump-ng utility

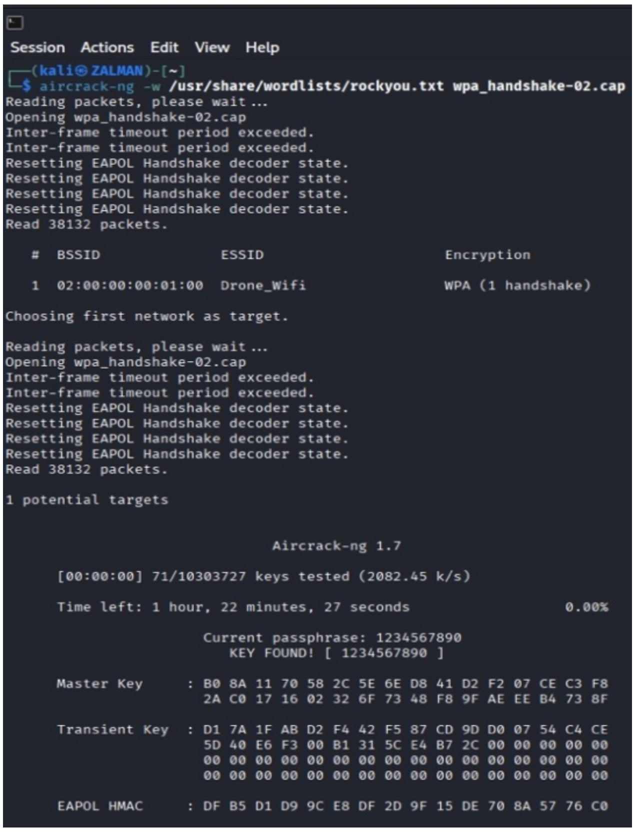
To obtain the cryptographic handshake required to crack the password, a deauthentication attack was initiated. Using the aireplay-ng tool, a series of deauthentication packets were sent to the access point and client addresses. This resulted in a forced disconnection. When the client attempted to automatically reconnect, the airodump-ng utility successfully intercepted and saved the WPA handshake to a *.cap file.


kali@ZALMAN: ~/Documents/Damn-Vulnerable-Drone
Session Actions Edit View Help

```
CH 12 ][ Elapsed: 3 mins ][ 2025-11-29 22:22 ][ WPA handshake: 02:00:00:00:01:00

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

02:00:00:00:01:00  -28      501     4486    0   6  130   WPA2 CCMP   PSK  Drone_Wifi

BSSID              STATION            PWR    Rate    Lost   Frames  Notes  Probes

02:00:00:00:01:00  02:00:00:00:03:00  -29   11e-11e    75       18
02:00:00:00:01:00  02:00:00:00:02:00  -29    1e- 1e     0     4481  EAPOL
```

Fig. 10. Interception of WPA handshake using the airodump-ng utility

The resulting password hash was subjected to a dictionary attack using the aircrack-ng tool version 1.7. Using the standard rockyou.txt password dictionary, the network's PSK key was successfully cracked.



```
┌──(kali㉿ZALMAN)-[~]
└─$ aircrack-ng -w /usr/share/wordlists/rockyou.txt wpa_handshake-02.cap
Reading packets, please wait...
Opening wpa_handshake-02.cap
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Read 38132 packets.

   #  BSSID              ESSID                     Encryption

   1  02:00:00:00:01:00  Drone_Wifi                WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening wpa_handshake-02.cap
Inter-frame timeout period exceeded.
Inter-frame timeout period exceeded.
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Resetting EAPOL Handshake decoder state.
Read 38132 packets.

1 potential targets


                               Aircrack-ng 1.7

      [00:00:00] 71/10303727 keys tested (2082.45 k/s)

      Time left: 1 hour, 22 minutes, 27 seconds                  0.00%

                     Current passphrase: 1234567890
                        KEY FOUND! [ 1234567890 ]

      Master Key     : B0 8A 11 70 58 2C 5E 6E D8 41 D2 F2 07 CE C3 F8
                       2A C0 17 16 02 32 6F 73 48 F8 9F AE EE B4 73 8F

      Transient Key  : D1 7A 1F AB D2 F4 42 F5 87 CD 9D D0 07 54 C4 CE
                       5D 40 E6 F3 00 B1 31 5C E4 B7 2C 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : DF B5 D1 D9 9C E8 DF 2D 9F 15 DE 70 8A 57 76 C0
```

Fig. 11. Result of a dictionary attack

As a result of the experiment, a valid password for accessing the UAV control wireless network was obtained. The attacker successfully connected to the network, obtaining an IP address in the same range as the flight controller. Compromising the network allows moving on to the post-exploitation stage, in particular: performing "man-in-the-middle" attacks to intercept telemetry, connect to open services (SSH/Telnet), or inject fake control commands. The experiment confirmed that the probability of implementing this intrusion mode is very high when using a weak password. This indicates the need to increase the criticality level of the intrusion mode in the matrix and justifies the need to implement complex password policies or switch to more secure communication protocols (e.g., WPA3) as a priority countermeasure.

6. Conclusions and prospects for further research

The paper presents and justifies a combined method for assessing the security of UAV cyber assets, which integrates IMECA analysis procedures with PT practice. This allows overcoming the limitations of static risk assessment methods and isolated technical tests, creating a closed cycle of system verification and protection.

Main results of the study:

- A functional model of a combined method (IDEF0) is proposed, which ensures the completeness of the security assessment of UAV cyber assets and consists of the following stages: information gathering and vulnerability assessment, intrusion mode replication, IMECA analysis (including preparatory and a posteriori IMECA analysis), and countermeasure selection.
- A test environment based on a DVD simulator has been deployed and verified. Analytical testing has confirmed the stand's ability to reproduce 80% of priority intrusion modes, making it an effective tool for secure research under existing constraints.
- Practical testing was carried out, during which an attack scenario on the wireless control channel was successfully implemented, confirming the possibility of gaining unauthorized access to the flight control system. This experiment proved the ability of the selected test environment to replicate intrusion modes.

Theoretical and experimental studies confirm the advantages of the proposed combined method compared to known analytical [11] and experimental [15] methods, which consist in improving the completeness and reliability of assessing the security of UAV cyber assets. This is achieved by adjusting the results of the preliminary IMECA analysis by reviewing the results of the PT and forming the final IMECA tables, which makes it possible to justify the choice of countermeasures and, consequently, to increase cyber and functional security as a whole.

Prospects for further research are related to conducting a full-scale series of experiments for all identified intrusion modes, constructing a posteriori criticality matrices and selecting countermeasures, as well as integrating the proposed method with the task of assessing the functional safety of unmanned systems [25].

For further research, it is recommended to switch to a mobile workstation (laptop) with a discrete Nvidia RTX series video card with CUDA driver support to ensure autonomy, increase productivity, and reduce the time required for experiments.

References

1. Tlili, F., Fourati, L. C., Ayed, S., Ouni, B. (2022), "Investigation on vulnerabilities, threats and attacks prohibiting UAVs charging and depleting UAVs batteries: Assessments & countermeasures". *Ad Hoc Networks*. Vol. 129, p. 102805. DOI: 10.1016/j.adhoc.2022.102805
2. Freedberg Jr, S. J. (2023), "Dumb and cheap: When facing electronic warfare in Ukraine, small drones' quantity is quality". *BreakingDefense.com*. Available at: https://breakingdefense.com/2023/06/dumb-and-cheap-when-facing-electronic-warfare-in-ukraine-small-drones-quantity-is-quality/ (Accessed: 30 November 2025).
3. Hartmann, K., Giles, K. (2016), "UAV exploitation: A new domain for cyber power". *2016 8th International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia, pp. 205–221. DOI: 10.1109/CYCON.2016.7529436
4. FP Explainers (2025), "Indian Army's 'Make in India' drones hacked in border areas: Report". *Firstpost.com*. Available at: https://www.firstpost.com/india/indian-army-make-in-india-drones-hacked-in-border-areas-report-13859474.html (Accessed: 30 November 2025).
5. Yaacoub, J.-P., Noura, H., Salman, O., Chehab, A. (2020), "Security analysis of drones systems: Attacks, limitations, and recommendations". *Internet of Things*. Vol. 11, p. 100218. DOI: 10.1016/j.iot.2020.100218
6. The New Geopolitics Research Network (2024), "Ukrainian Drones vs Russian Jamming". *NewGeopolitics.org*. Available at: https://www.newgeopolitics.org/2024/06/10/ukrainian-drones-vs-russian-jamming/ (Accessed: 30 November 2025).
7. Royal United Services Institute for Defence and Security Studies (2023), "Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine". *RUSI*. Available at: https://static.rusi.org/403-SR-Russian-Tactics-web-final.pdf (Accessed: 30 November 2025).
8. Mekdad, Y., Arış, A., Babun, L., El Fergougui, A., Conti, M., Lazzeretti, R., Uluagac, S. (2023), "A survey on security and privacy issues of UAVs". *Computer Networks*. Vol. 224, p. 109626. DOI: 10.1016/j.comnet.2023.109626
9. Yu, Z., Wang, Z., Yu, J., Liu, D., Song, H. H., Li, Z. (2024), "Cybersecurity of Unmanned Aerial Vehicles: A Survey". *IEEE Aerospace and Electronic Systems Magazine*. Vol. 39, No. 9, pp. 182–215. DOI: 10.1109/MAES.2023.3318226
10. Kong, P.-Y. (2021), "A Survey of Cyberattack Countermeasures for Unmanned Aerial Vehicles". *IEEE Access*. Vol. 9, pp. 148244–148263. DOI: 10.1109/ACCESS.2021.3124996
11. Zemlianko, H., Kharchenko, V. (2023), "Cybersecurity risk analysis of multifunctional UAV fleet systems: a conceptual model and IMECA-based technique". *Radioelectronic and Computer Systems*. No. 4, pp. 152–170. DOI: 10.32620/reks.2023.4.11
12. Torianyk, V., Kharchenko, V., Zemlianko, H. (2021), "IMECA based assessment of Internet of Drones systems cyber security considering radio frequency vulnerabilities". *Proc. 2nd Int. Workshop on Intelligent Information Technologies and Systems of Information Security (IntelITSIS'2021)*, Khmelnytskyi, Ukraine. Available at: https://ceur-ws.org/Vol-2853/paper50.pdf (Accessed: 30 November 2025).
13. Branco, B., Silva, J. S., Correia, M. (2024), "D3S: A Drone Security Scoring System". *Information*. Vol. 15, No. 12, p. 811. DOI: 10.3390/info15120811
14. Ficco, M., Granata, D., Palmieri, F., Rak, M. (2024), "A systematic approach for threat and vulnerability analysis of unmanned aerial vehicles". *Internet Things*. Vol. 26, p. 101180. DOI: 10.1016/j.iot.2024.101180
15. Veerappan, C. S., Keong, P. L. K., Balachandran, V., Fadilah, M. S. B. M. (2021), "DRAT: A Penetration Testing Framework for Drones". *2021 IEEE 16th Conference on Industrial Electronics and Applications (ICIEA)*, Chengdu, China, pp. 498–503. DOI: 10.1109/ICIEA51954.2021.9516363
16. Abakumov, A., Kharchenko, V. (2023), "Combining experimental and analytical methods for penetration testing of AI-powered robotic systems". *Proc. 7th Int. Conf. on Computational Linguistics and Intelligent*

Systems (COLINS 2023), Kharkiv, Ukraine. Vol. 3403, pp. 470–481. Available at: https://ceur-ws.org/Vol-3403/paper40.pdf (Accessed: 08 April 2025).

17. Veprytska, O., Kharchenko, V. (2023), "Extended IMECA Technique for Assessing Risks of Successful Cyberattacks". *2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Athens, Greece, pp. 1–7. DOI: 10.1109/DESSERT61349.2023.10416447
18. Abakumov, A., Kharchenko, V. (2022), "Combining IMECA analysis and penetration testing to assess the cybersecurity of industrial robotic systems". *2022 12th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Athens, Greece, pp. 1–6. DOI: 10.1109/DESSERT58054.2022.10018823
19. Abakumov, A., Kharchenko, V., Popov, P. (2025), "A Hybrid Cybersecurity Assessment Framework for Unmanned Aircraft Vehicles Based on IMECA and Penetration Testing". *2025 55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, Naples, Italy, pp. 7–14. DOI: 10.1109/DSN-W65791.2025.00032
20. Sanghavi, P., Kaur, H. (2023), "A Comprehensive Study on Cyber Security in Unmanned Aerial Vehicles". *2023 10th International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, pp. 804–809. Available at: https://ieeexplore.ieee.org/document/10112549 (Accessed: 09 December 2025).
21. The Penetration Testing Execution Standard (2017), "PTES Technical Guidelines". *Pentest-standard.org.* Available at: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines (Accessed: 30 November 2025).
22. Herzog, P. (2010), "OSSTMM 3: The Open-Source Security Testing Methodology Manual – Contemporary Security Testing and Analysis". *ISECOM.* Available at: https://www.isecom.org/OSSTMM.3.pdf (Accessed: 30 November 2025).
23. Scarfone, K., Souppaya, M., Cody, A., Orebaugh, A. (2008), "Technical Guide to Information Security Testing and Assessment: Recommendations of the National Institute of Standards and Technology". *NIST Special Publication 800-115*. Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf (Accessed: 30 November 2025).
24. OWASP (2024), "Web Security Testing Guide". *owasp.org.* Available at: https://owasp.org/www-project-web-security-testing-guide/ (Accessed: 30 November 2025).
25. Babeshko, I., Illiashenko, O., Kharchenko, V., Leontiev, K. (2022), "Towards Trustworthy Safety Assessment by Providing Expert and Tool-Based XMECA Techniques". *Mathematics*. Vol. 10, p. 2297. DOI: 10.3390/math10132297
26. Aleks, N. (2023), "Damn Vulnerable Drone (DVD)". *GitHub repository.* Available at: https://github.com/nicholasaleks/Damn-Vulnerable-Drone (Accessed: 29 November 2025).

Received (Надійшла) 01.12.2025
Accepted for publication (Прийнята до друку) 09.12.2025
Publication date (Дата публікації) 28.12.2025

About the Authors / Відомості про авторів

Abakumov Artem – National Aerospace University "Kharkiv Aviation Institute", Master of Science in Information measuring technologies, PhD Student at the Department of Computer Systems, Networks, and Cybersecurity, Kharkiv, Ukraine; e-mail: a.i.abakumov@csn.khai.edu; ORCID ID: https://orcid.org/0000-0002-7742-6515

Kharchenko Vyacheslav – Corr.-member of National Academy of Science, Doctor of Sciences (Engineering), Professor, National Aerospace University "Kharkiv Aviation Institute", Head at the Department of Computer Systems, Networks, and Cybersecurity, Kharkiv, Ukraine; e-mail: v.kharchenko@csn.khai.edu; ORCID ID: https://orcid.org/0000-0001-5352-077X

Абакумов Артем Ігорович – Національний аерокосмічний університет "Харківський авіаційний інститут", фахівець зі спеціальності "Інформаційні вимірювальні системи", аспірант кафедри комп’ютерних систем, мереж і кібербезпеки, Харків, Україна.

Харченко Вячеслав Сергійович – член-кореспондент Національної академії наук України, доктор технічних наук, професор, Національний аерокосмічний університет "Харківський авіаційний інститут", завідувач кафедри комп’ютерних систем, мереж і кібербезпеки, Харків, Україна.

КОМБІНОВАНИЙ МЕТОД ОЦІНЮВАННЯ БЕЗПЕКИ КІБЕРАКТИВІВ БпЛА З ВИКОРИСТАННЯМ ІМЕСА-ПРОЦЕДУР І ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

Предмет вивчення – методи й засоби оцінювання безпеки кіберактивів безпілотних літальних апаратів (БпЛА). На підставі аналізу публікацій зроблено висновок про певний розрив між теоретичними методами оцінювання ризиків і практичними інструментами тестування на проникнення (ТнП) кіберактивів БпЛА. Наявні інструменти ТнП призначені для відтворення атак, але не надають методології оцінювання їх впливу в динамічних умовах застосування. **Мета дослідження** – розробити комбінований метод і елементи технології достовірного виявлення вразливостей з можливістю верифікації процесу й обґрунтування вибору контрзаходів. **Завдання роботи:** обґрунтування доцільності комбінованого застосування різних методів і засобів оцінювання кібербезпеки БпЛА; розроблення моделей і методу оцінювання, який поєднує аналітичні та експерементальні процедури; практичне відпрацювання методу з використанням тестового середовища. **Упроваджені методи**: ризик-орієнтований аналіз режимів вторгнення, наслідків і критичності (IMECA-аналіз) і ТнП. **Результати дослідження**: обґрунтовано структуру й послідовність комбінованого оцінювання кібербезпеки; запропоновано функціональну IDEF0-модель, що забезпечує повноту оцінювання безпеки кіберактивів БпЛА й містить такі етапи: збір інформації та оцінювання вразливостей, реплікація режимів вторгнення, IMECA-аналіз (зокрема з підготовчим і апостеріорним IMECA-аналізом) і вибір контрзаходів; розгорнуто й апробовано тестове середовище на базі симулятора DVD, який здатний відтворювати 80 % пріоритетних режимів вторгнення. **Висновки:** комбінований метод оцінювання безпеки кіберактивів БпЛА інтегрує процедури IMECA з практикою ТнП, що дає змогу подолати обмеження статичних методів оцінювання ризиків та ізольованих технічних тестів, створюючи замкнутий цикл верифікації та захисту бортових систем. Подальші дослідження пов’язані з проведенням повномасштабної серії експериментів для всіх ідентифікованих режимів вторгнення, побудовою апостеріорних матриць критичності та вибору контрзаходів.

Ключові слова: кіберактиви БпЛА; IMECA-аналіз; комбінований метод; симуляції режимів вторгнення; тестування на проникнення.

Bibliographic descriptions / Бібліографічні описи

Abakumov, A., Kharchenko, V. (2025), "Combined method of uav cyber assets security assessment by use of procedures imeca and penetration testing", *Management Information Systems and Devises*, No. 4 (187), P. 200–219. DOI: https://doi.org/10.30837/0135-1710.2025.187.200

Абакумов А. І., Харченко В. С. Комбінований метод оцінювання безпеки кіберактивів БпЛА з використанням IMECA-процедур і тестування на проникнення. *Автоматизовані системи управління та прилади автоматики*. 2025. № 4 (187). С. 200–219.
DOI: https://doi.org/10.30837/0135-1710.2025.187.200