Date of publication DEC-31, 2025, date of current version SEP-20, 2025.
www.computingonline.net / computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.24.4.4346

UAV Cyber Resilience Assessment Method: Combining IMECA, Penetration Testing and State-space Markov Modeling

ARTEM ABAKUMOV[1], VYACHESLAV KHARCHENKO[1], YURII PONOCHOVNYI[2]
[1]National Aerospace University “KhAI”, Kharkiv, 61070, Ukraine (E-mail: a.i.abakumov@csn.khai.edu, v.kharchenko@csn.khai.edu)
[2]Poltava State Agrarian University, Poltava, 36000, Ukraine (E-mail: yuriy.ponochovnyy@pdau.edu.ua)

Corresponding author: Artem Abakumov (e-mail: a.i.abakumov@csn.khai.edu).

ABSTRACT The objective of this paper is to develop and justify a combined method for assessing the Cyber Resilience (CR) of Unmanned Aerial Vehicles (UAVs) under cyber attacks. The proposed approach, formalized in IDEF0 notation, integrates analytical IMECA-analysis and experimental Penetration Testing (PT) procedures with State-Space Markov Modeling (SSMM). This combination overcomes the limitations of static risk assessment methods by creating a closed cycle of system verification and protection. Based on the constructed SSMM, a sensitivity analysis was performed to identify key parameters. The study reveals that the system's response speed is the most critical factor for UAVs’ CR. It was established that an increase in operational recovery time leads to a 31.2% drop in the availability coefficient and nearly doubles the risk of compromise (+87.5%). Conversely, increasing the probability of successful recovery provides a significant increase in the probability of mission success (by 83.6%). Furthermore, the hypothesis regarding the effectiveness of frequent PT was refuted: changing the inspection interval showed a minor impact on availability (<2%), whereas excessive duration of PT procedures reduced system availability by 51.0%. These findings demonstrate the inefficiency of excessively long and frequent checks and suggest that the strategy should concentrate on the speed and automation of PT procedures rather than their frequency. Future research will focus on developing a multi-fragment SSMM to integrate PT processes with a UAV simulator and analyze the impact of combined intrusion modes.

KEYWORDS UAV, Cyber Resilience, State-Space Markov Modeling, IMECA, Penetration Testing.

I. INTRODUCTION

A rapid growth in the use of small unmanned aerial vehicles (UAVs), known as “drones”, is evident in various fields [1], including hard-to-reach areas monitoring, disaster prevention, services for smart cities, aerial photography and cinematography, advanced agriculture, traffic monitoring, critical infrastructure monitoring, and military missions (reconnaissance, patrolling, logistics).

Since 2022, small UAVs have played a vital role in the military operations of the Armed Forces of Ukraine amid full-scale aggression by the Russian Federation. Combat use [2-5] shows that even high-tech devices remain priority targets for cyber attacks and electronic warfare measures. This applies not only to specialized military UAVs, but also to commercial ones being militarized.

In war zones, massive signal jamming leads to significant UAV losses. According to [6], monthly UAV losses are measured in thousands, mainly due to successful attacks on the availability of navigation systems and control interception. As the experts point out in [2], the comparative affordability of these units changes the tactics of their use, allowing small UAVs to be utilized in an aggressive way.

Commercial UAVs require in-depth adaptation to military purposes. It includes firmware customization and integration to reduce UAV detectability by passive RF monitoring systems. It is also worth mentioning that vendor firmware is constantly being updated, so that outdated customed firmware becomes unusable in latest versions of UAVs [7].

These cases just emphasize the need for a systematic assessment of the small UAVs cyber assets security [8], specifically analyzing potential threats and exploring vulnerabilities (including zero-day vulnerabilities) before they are exploited by adversaries, which could not only result in the loss of the device itself during a flight mission, but also pose a threat to the lives and safety of operators.

During military implementation of such systematic analysis, it is necessary to consider a dynamic nature of UAV states and transitions between them. Modern approaches are likely to ignore the timeliness and stochastic essence of UAV operational cycles. This discrepancy between static analysis and actual system behavior makes it impossible to accurately assess operational reliability. Therefore, it is extremely important to apply approaches that consider UAVs as systems with multi-level degradation and recovery [9] to select and implement an effective set of countermeasures.

II. LITERATURE REVIEW

A. WORK RELATED

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

The authors [10] conducted a comparative analysis of dual-state and multi-state systems for UAV swarm modeling. Traditional binary models are insufficient, as they only consider “operational” and “faulty” states. Multi-state models allow for intermediate performance levels, which is critical for partially degraded systems. Quantitative experiments on UAV swarms up to 20 UAVs confirmed that multi-state models are more suitable for analyzing transitional operational states.

The [11] proposes an approach to UAV safety assessment where the device is considered as a unity of three entities: physical, informational, and controlled. The author has developed a continuous-time Markov model which, as opposed to simpler analogues, considers specific attack surfaces, such as attacks on control channels, GPS spoofing, and payload data interception. A critically important feature of this model is the consideration of combined attacks, which contributes to real-life military conditions modeling. The experiment showed a nonlinear relationship between ensuring security and countermeasures selection. Increasing the effectiveness of countermeasures for just one type of cyber attack only slightly improves overall reliability. But focusing on countering complex threats and preventing critical failure scenarios can really improve the level of protection.

In addition to well-known attack surfaces on communication and navigation channels, cutting-edge research focuses on vulnerabilities in intelligent UAV subsystems. In [12], a method was developed to ensure the robustness of adversarial attacks and fault injection detectors. This confirms the need to consider the resilience of AI components when building a comprehensive model of mission cyber resilience.

The authors [13] argue that traditional methods neglect the temporal correlation of system states, which reduces detection accuracy in dynamic flight conditions. Unlike discrete models, the use of continuous hidden Markov (CT-HMM) models avoids distortions caused by quantization of continuous observable quantities, which is critical for UAVs. To improve model accuracy in unstable communication channels, a method for estimating the signal-to-noise ratio based on spatial smoothing has been developed. The modeling results demonstrated that the integration of CT-HMMs significantly increases the probability of correct system state detection compared to methods without state prediction.

In [14], the concept of “UAV Fleet as a Dependable Service” for smart cities is proposed. The authors shift the focus from analyzing the reliability of individual devices to ensuring the dependability of service provision. The study specifies a taxonomy of UAV fleet failures caused by equipment faults and attacks on assets, treating cyber attacks as a critical factor in reliability analysis. The proposed methodology allows for the grounding of fleet parameters, considering operation modes and maintenance policies. The results demonstrate that applying these models allows for choosing appropriate parameters to ensure service delivery with a high probability.

Work [4] discusses numerous examples of UAV’s malicious use and analyzes possible attack surfaces in civil and military fields. It shows that UAVs are vulnerable to a wide range of cyber attacks and emphasizes the importance of implementing measures to detect and prevent them.

In [15], it is argued that UAV design problems are becoming increasingly apparent with the transition to mass military use, and risks are systematized according to CIA aspects and methods of analyzing vulnerabilities in UAV software.

The author of [16] presented a comprehensive classification of cyber attacks on UAVs, which can be used as a basis for threat modeling.

The paper [17] examines the issue of assessing the cybersecurity (CS) of multifunctional UAV fleets, identifies threats, vulnerabilities, and potential consequences of cyber attacks, considering the specifics of system element interaction. The authors proposed a multi-level model of threats and attack scenarios, considering the functional distribution in the UAV infrastructure. A key methodological component of the study is the use of the Intrusion Modes and Effects Criticality Analysis (IMECA) method, which allows threats to be classified according to their level of criticality, the consequences of attacks to be modeled, and countermeasures to be formulated to improve the CS of the system.

Study [18] addresses the problem of the lack of a standardized method for assessing the overall security level of UAVs. The authors propose Drone Security Scoring System (D3S) - a methodology for assessing and assigning a security score to specific UAVs based on an analysis of their components and resistance to attacks.

In [19], the critical need for a structured methodology for assessing the UAVs security is justified, given their integration into CPS and the IoT. The authors propose a step-by-step approach that combines threat modeling, vulnerability assessment, and selection of appropriate countermeasures based on the assessment results. Drone Attack Tool (DRAT) is a PT framework proposed in [20] and designed to automate the process of finding vulnerabilities in 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.

The literature review has revealed significant methodological gaps. The existing approaches to assessing UAV vulnerabilities (e.g., D3S) are primarily static and do not account for the dynamics of UAV transitions between states under the influence of cyber attacks. Conversely, the existing UAV-specific penetration testing (PT) tools (e.g., DRAT) mainly focus on exploiting vulnerabilities but do not provide metrics of their impact on UAV cyber resilience (CR) over time. The mathematical models considered can assess the UAVs' CR when states change, but don’t consider the implementation of PT measures and their indicators. Consequently, there is a need to develop a combined method that would integrate the practical results of PT (as a source of parameters), the analytical capabilities of IMECA (for criticality classification), and the predictive power of Markov models (for assessing mission success probability). This combination will enable a transition from stating the presence of vulnerabilities that can be exploited to quantitatively predicting the UAVs' CR in real operating conditions.

B. OBJECTIVES AND STRUCTURE

The objective of this paper is to develop a combined method for assessing the UAVs' CR under cyber attacks.

Research goals:

- Justifying the feasibility of using a variety of methods and tools to assess the UAVs’ CR (section III);
- Developing a model and assessment method that combines analytical and experimental procedures, as well as modeling system states using State-Space Markov Modeling (SSMM) (section IV);
- Modeling using SSMM and formulating conclusions on the selection of parameter values for protecting UAV assets (section V);
- Analysis of results and areas for further research (section VI).

III. METHODOLOGY OF RESEARCH

One of the previous research studies [21] analyzed a variety of combinations of analytical and experimental methods for assessing the security and cybersecurity (CS) of intelligent systems, considering such indicators as completeness, execution time, cost, and trustworthiness. The analysis showed that the combination of IMECA-analysis [17, 22] with PT best meets the requirements for assessing the UAVs’ CS. When we delved deeper while working under, we noticed that the limitation of this combination of methods remains the inability to fully model the dynamics of cyber attacks over time and the system's response to them. As noted in [11], assessing the security of UAV use requires consideration not only of the fact of an attack, but also of the intensity of its implementation. That is why it is necessary to expand the task to assessing CR, which characterizes the system's ability to continue performing its mission under destructive influences through degradation and recovery. To solve this problem, it is proposed to supplement the combined IMECA + PT method with a set of Markov models. Some modern approaches to autonomous penetration testing already use Markov processes for decision-making under uncertainty [23, 24]. This creates a natural compatibility between the results of PT and the mathematical evaluation model. SSMM makes it possible to determine the probability of the system being in different states, including states directly related to the consequences of intrusions. In addition, such a model allows investigating how PT quality affects the system's ability to tolerate intrusions and, consequently, the value of the system's availability function. Thus, the integration of Markov models allows the transformation of static vulnerability criticality assessments obtained from IMECA and empirical data on intrusion success into dynamic mission reliability indicators, which is a necessary condition for ensuring CR.

IV. COMBINED METHOD

A. HIGH-LEVEL IDEF0 MODEL

The Integration Definition for Function Modeling (IDEF0) functional modeling methodology was chosen to formalize and structurally describe the proposed combined method. This decision was motivated primarily by the need to accurately reflect the processes of transforming input information (UAV architecture, its application scenarios and limitations) into final CR metrics. The use of IDEF0 notation allows for a clear definition of functional blocks with the separation of control elements and implementation mechanisms.

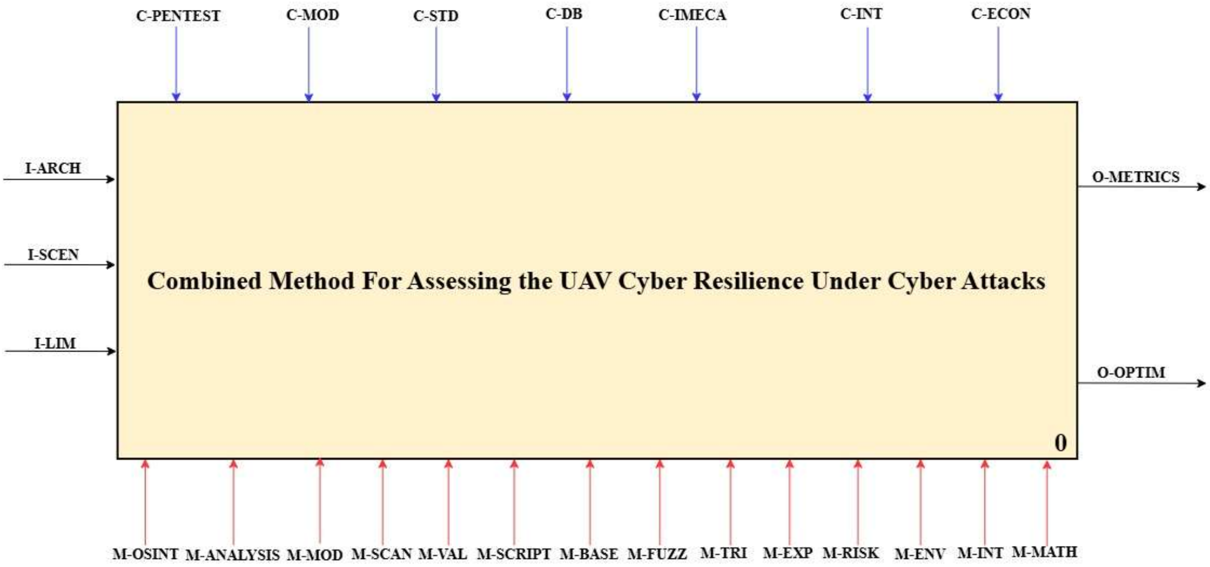

Figure 1. IDEF0 model of UAV CR assessment method (Level A0)

A fundamental advantage is the hierarchical nature of the notation, which provides the capability to decompose complex evaluation procedures incrementally. This enables the logical integrity of the method to be preserved when integrating disparate components.

The proposed combined method, presented in Figure 1 as an IDEF0 context diagram (Level A0), is based on a holistic process aimed at identifying vulnerabilities, analyzing and confirming them, selecting countermeasures, and quantitatively assessing the UAVs' CR. At the input stage, information about the object of study is generated: the UAV architecture (I-ARCH), scenarios of its use (I-SCEN), as well as legal, operational, and technical limitations (I-LIM). The assessment is implemented through a sequence of interrelated stages, which are provided by the necessary set of 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 by blue arrows. The result is calculated CR metrics (O-METRICS), as well as substantiated recommendations for fine-tuning parameters to maximize CR level (O-OPTIM).

B. DECOMPOSED IDEF0 MODEL

Figure 2 shows a decomposed model of the combined method (Level A1), which combines the following stages: information gathering and system analysis (1), known (2) and zero-day (3) vulnerabilities, intrusion modes replication (5), IMECA-analysis in its preliminary (4) and a posteriori (6) forms, and MSSM (7) into a single continuous process.

At the initial stage of information gathering and system analysis, the research context is formed, and vulnerabilities and potential threats to the UAV are identified. A stack of UAV technologies (O/I-TECH) and a list of potential threats (O/I-THREAT) are formed using OSINT tools (M-OSINT), automated scanners (M-SCAN), modeling (M-MOD) and analysis (M-ANALYSIS) tools. The researchers' steps are guided by the PT methodology (C-PEN), defined by modeling frameworks (C-MOD) and regulated by CS standards (C-STD), and governed by policy on the use of OSINT and automated scanning tools (C-POL), which impose additional technical and legal restrictions to avoid ethical violations. The following process branches into two parallel blocks: known and zero-day vulnerabilities assessment. The purpose of the second stage is to assess known vulnerabilities (O/I-VULN) by comparing UAV technologies used with vulnerability DBs (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) that cannot be detected by any automated means. Based on the input list of threats (O/I-THREAT) and the technology stack (O/I-TECH), researchers develop a benchmark behavior model and analyze attack surfaces using basic and static analysis tools (M-BASE). Then, 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 found vulnerabilities. The entire process is regulated by CS standards (C-STD) and interaction policies (C-POL).

The goal of the fourth stage is to analytically transform vulnerability data into an assessment of the risks to UAV missions. Based on input lists of threats (O/I-THREAT), known (O/I-VULN) and zero-day (O/I-ZERO) vulnerabilities data, attack surfaces are mapped to intrusion modes. This process is regulated by the IMECA methodology and its assessment scales (C-IMECA), as well.

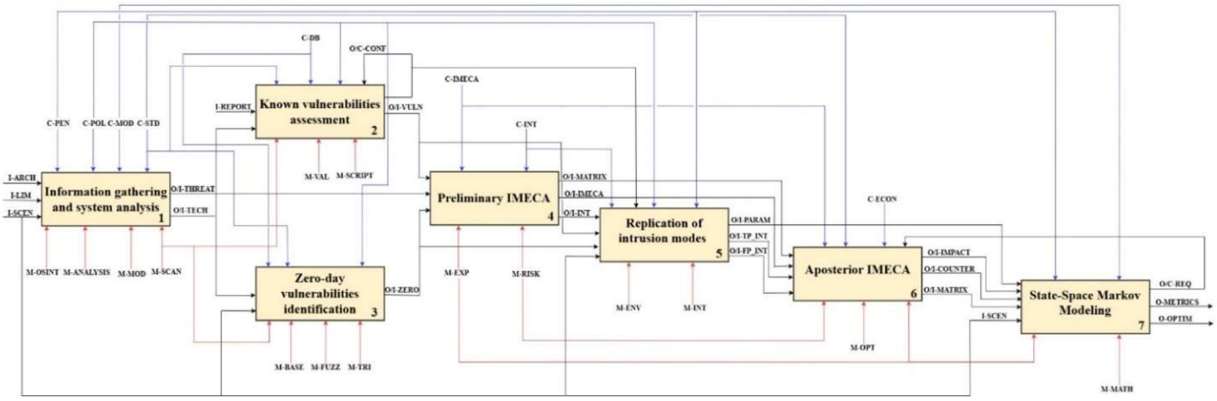

Figure 2. IDEF0 model of UAV CR assessment method (Level A1)

as intrusion models (C-INT). With the expert analysis (M-EXP) and risk assessment tools (M-RISK), a hypothesis about the level of threat 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 intrusion modes (O/I-INT).

The fifth stage consists of intrusion modes practical replication and is one of the key stages of the PT methodology deeply integrated into the proposed method. In addition to confirming the existence of vulnerabilities, a critically important function of this stage is the collection of time metrics for further modeling. The modeling process is strictly confined to an isolated sandbox environment (M-ENV) to prevent any impact on a real UAV. The active phase of the intrusion is removed using a cleanup procedure. This involves terminating attack scripts, removing test artifacts and returning the UAV to its original state. The output consists of a set of empirical parameters (O/I-PARAM): the time and frequency of security checks, the intensity of successful attacks, the average recovery time after attacks, etc. A differentiation is also made between successful confirmed intrusions (O/I-TP_INT) and rejected false positives (O/I-FP_INT) of threats based on empirical data. The result is an updated criticality matrix (O/I-MATRIX), an impact assessment report (O/I-IMPACT), and a set of recommended countermeasures (O/I-COUNTER). This data, along with the parameters from the previous stage, is transferred to the next block.

At the sixth stage, the results are synthesized based on empirical data about 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 then reassessed. The key mechanism in this stage is optimization algorithms (M-OPT), which automate the selection of countermeasures. The process is managed considering cost-effectiveness criteria (C-ECON) to minimize costs while achieving the required security level. The outcome includes an updated criticality matrix (O-MATRIX), an impact assessment report (O-IMPACT), and a set of recommended countermeasures (O-COUNTER) that ensure an acceptable level of residual risk.

The seventh stage is the final step of the method. The SSMM is constructed based on UAV application scenarios (I-SCEN), a set of empirical parameters (O/I-PARAM), and a criticality matrix from a posteriori IMECA analysis. The key implementation mechanism (M-MATH) is the mathematical apparatus of Markov processes with discrete states and uninterrupted time, implemented in a specialized software environment. The output consists of calculated CR metrics (O-METRICS), as well as substantiated recommendations for adjusting parameters of the system (O-OPTIM) to achieve the target level of CR. In addition, feedback is generated in the form of refined security architecture requirements (O/C-REQ).

V. MARKOV MODEL DEVELOPMENT AND RESEARCH

A logical continuation of structural modeling is the transition to the practical implementation of the final stage of the proposed methodology. For this purpose, a UAV SSMM operation under cyber attacks has been developed. This approach allows not only to evaluate the integral indicators of CR, but also to investigate their sensitivity to changes in the temporal characteristics of attacks and recovery and considers PT parameters.

A. STATE-SPACE MARKOV MODEL FORMALIZATION

In the context of this study, UAVs' CR is understood as the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises of systems that use or depend on cyber resources [25]. The UAVs' SSMM, which consists of four states S_0-S_3 (Figure 3), is described by probabilistic transitions between states:

- Anticipate. Proactive detection of vulnerabilities at the S_0 (Ready) stage. In the model, this is implemented by transitioning to state S_3 (PT) with intensity λ_{PT}. This helps identify and address potential threats before the mission starts, decreasing the chances of a successful future attack.
- Withstand. The ability of the system to function effectively, determined by the intensity of mission requests λ_{op} and the intensity of their execution μ_{op}. It

is necessary to successfully complete the mission (transition from Mission Execution (S_1) to safe state S_0) before the cyber attack is implemented. Mathematically, this is expressed in the maximization of μ_{op} while reducing the intensity of successful attacks λ_a that transfer the system to state S_2 (Compromised).

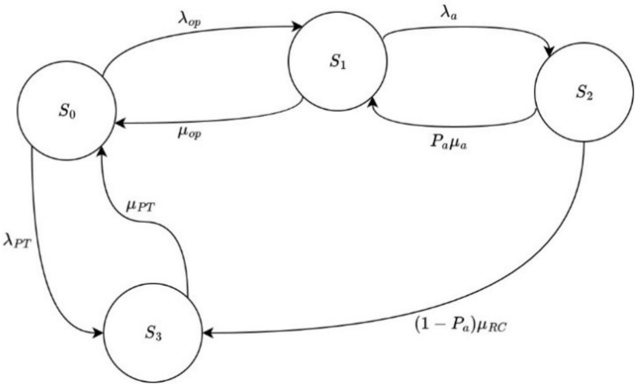

Figure 3. UAV SSMM considering PT parameters

- Recover. The ability of the system to recover from a S_2. The model provides for two levels of response: (1) Rapid return to task execution through transition $S_2 \rightarrow S_1$ thanks to automatic self-recovery mechanisms. The intensity of this transition is $P_a\mu_a$; (2) If operational recovery fails, a transition $S_2 \rightarrow S_3$ occurs with a resulting intensity of $(1-P_a)\mu_{RC}$.
- Adapt. Analysis of incident causes, implementation of corrective measures and modification of protection configuration while in state S3. Returning to the S0 state with intensity μ_{PT} ensures that the UAV is patched and its protection parameters are adapted to new attack surfaces before the next mission.

B. ASSUMPTIONS AND LIMITATIONS

The developed SSMM model is predicated upon several fundamental assumptions inherent within the SSMM. Firstly, the model presumes the Markov property, which denotes that the future state of the system depends solely upon its current state, without accounting for the historical record of preceding intrusions or failures. Secondly, only the mission execution state is deemed perilous. The authors acknowledge that the state of availability and the state of being on a PT are also potentially vulnerable, yet this is not presently incorporated within the model. Thirdly, the transition intensity is assumed to be constant throughout the simulation period. These assumptions influence the interpretation of the calculated CR indicators. The availability function ($A_{g)}$ reflects the behavior of the system in a steady state, averaged overtime. In actual combat conditions (for instance, during a series of coordinated serial attacks), instantaneous availability may deviate from this average baseline. To surmount these limitations, future research will concentrate on developing a multi-fragment SSMM. This approach will permit the relaxation of the stationarity assumption by modeling transitions between distinct operational contexts.

C. JUSTIFICATION OF THE PARAMETER VALUES CHOICE

To continue the experiment and study the developed SSMM, it is necessary to determine the numerical values of the parameters - the transition intensities. As the statistical DB of real incidents and field test results is still being formed at this stage of the research, the selection of input parameter values was made based on a review of publications [11, 14, 26, 27] and expert assessment. This approach enables simulation of the system's behavior across a wide range of scenarios: from the most favorable to the most critical. All model parameters are classified into four groups depending on the nature of their origin and the possibility of controlling them:

- Operational. This group of parameters is determined by operational and tactical requirements for UAV use and does not depend on the cyber protection subsystem. Time between mission requests (T_{op}) and its execution time (τ_{op}) determine the intensity of UAV use. This parameter depends on the complexity of the navigation algorithm, such as chaotic agent navigation used for achieving uniform area exploration [28], which may extend the exposure time to threats but ensure better operational results. The range of values is selected to cover different mission modes: from high-intensity short-term flights (e.g., reconnaissance) to long-term shifts in areas with low combat intensity. The corresponding intensities are calculated as mission request intensity ($\lambda_{op} = 1/T_{op}$) and mission execution intensity ($\mu_{op} = 1/\tau_{op}$).
- Pentesting. These are parameters that are determined during intrusion modes replication and IMECA-analyses: PT frequency (T_{PT}) and its duration (τ_{PT}). Varying these parameters allows us to find a balance between CS checks and mission availability. The values are chosen to explore the impact of both frequent short checks and infrequent but thorough security audits. The detailed mapping of these empirical metrics to the model's transition intensities is presented in Table 1.

Table 1. Mapping of empirical PT metrics to SSMM parameters

Empirical parameters	Measurement procedure	SSMM parameters	Formula
TTR	Time recorded from the moment of successful exploitation of vulnerability to the restoration of normal UAV operation.	τ_a	$\mu_a = 1/\tau_a$
TMR	The time required for a complete reset, reflashing, or hard reset of the UAV in case the automatic means have failed.	T_{RC}	$\mu_{RC} = 1/T_{RC}$
MTBI	The scheduled time interval between consecutive intrusion iterations initiated by PT experts to simulate specific threat density.	T_a	$\lambda_a = 1/T_a$
PT duration	The actual time spent by PT experts on completing a full checks cycle.	τ_{PT}	$\mu_{PT} = 1/\tau_{PT}$
PT frequency	The frequency of PT cycle launches.	T_{PT}	$\lambda_{PT} = 1/T_{PT}$

- Threat. This group characterizes the variability of the external environment. Since it is difficult to accurately predict these values in combat conditions, several parameters have been selected for modeling that simulate different threat levels: time between attacks (T_a) characterizes the density of cyber influence (from massive attacks once per minute in electronic warfare conditions to isolated incidents once every N minutes). Consequently, the intensity of cyberattacks represents the rate of intrusion attempts derived from the empirical Mean Time Between Intrusions (MTBI) (Table 1), serving as the transition rate governing the system's shift from a normal operation state to a state under attack.
- Recovery. Probability of successful recovery (P_a) is a key indicator of the effectiveness of protective measures, the variation of which allows assessing the survivability of a system with both low and high levels of CR. The operational recovery time (τ_a) and emergency recovery time (T_{RC}) determine the system's restoration capabilities. These values directly correspond to the Time to Recover (TTR) and Time for Manual Restoration (TMR) metrics measured during the PT stage (Table 1), defining the respective recovery intensities varying from seconds (automatic restart of processes) to minutes (complete reboot or firmware re-flashing).

To address the transition from empirical data (O/I-PARAM) to mathematical modeling, a mapping scheme was established. This scheme linked specific PT metrics with SSMM parameters, which are summarized in Table 1.

C. MODELING

A simulation model was constructed for modeling purposes, the structure of which is shown in Figure 4. The simulation was performed in MATLAB using the Simulink package.

The graphical diagram shows the four states of the system (graph nodes) and the possible transitions between them (directed arcs). An important feature of the diagram is that the weights of the arcs correspond to the calculated numerical values of the transition intensities for the base scenario:

- Node 1 (Green) corresponds to state S_0 (Ready);
- Node 2 (Yellow) corresponds to state S_1 (Mission execution);
- Node 3 (Red) corresponds to state S_2 (Compromised);
- Node 4 (Purple) corresponds to state S_3 (PT).

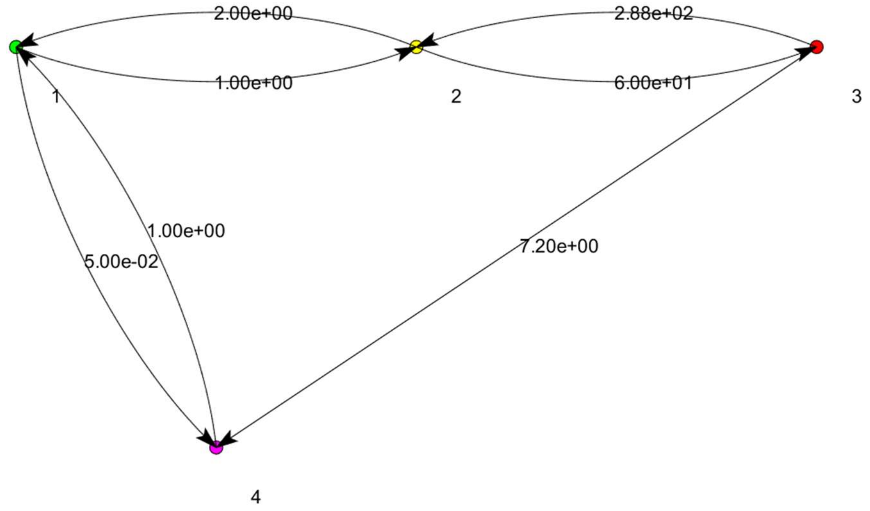

Figure 4. Simulation of UAV SSMM considering PT parameters

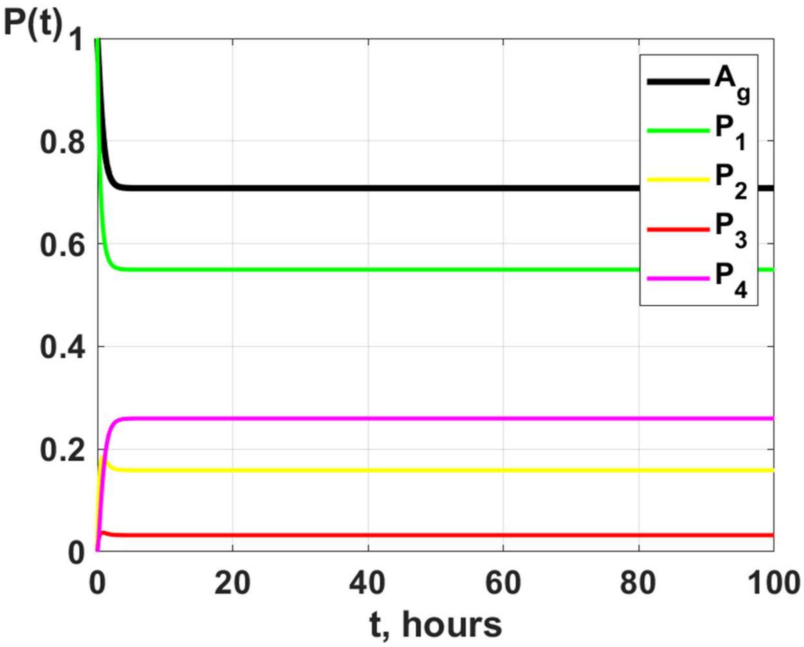

Figure 5. Probability chart of UAV being in S_0-S_3 states

For initial modeling and comprehensive model verification processes, a carefully selected set of base values was systematically formed and documented, as clearly shown in the detailed Table 2.

Figure 5 presents a comprehensive graph that illustrates the probability of the UAV being in operational states S0-S3 as a direct function of time $P_i(t)$ for the established base set of parameters.

Explanation of symbols in Figure 5:

- A_g (black line) corresponds to the availability function and is mathematically defined as the sum of probability P_1 and P_2 ($A_g = P_1+P_2$);
- P_1 (green line) corresponds to the probability of being in state S_0 (Ready), indicating the UAV is fully operational and waiting for mission assignment;
- P_2 (yellow line) corresponds to the probability of being in state S_1 (Mission execution), representing the likelihood that the UAV is actively performing its operational tasks;
- P_3 (red line) corresponds to the probability of being in state S_2 (Compromised), which indicates the UAV has been cyber attacked, affecting normal operations.
- P_4 (purple line) corresponds to the probability of being in state S_3 (PT), representing the phase where the UAV undergoes testing and preventive procedures.

Since in the probability model P_1- P_4 quickly transition to a steady state within the first 5 hours of simulation time, we will now examine the comprehensive effect of systematic changes in individual input parameters on the values of steady-state probabilities of UAV states and its availability function $A_g(t)$. This analysis will provide crucial insights into parameter sensitivity and system behavior under varying operational conditions.

Figures 6-8 show histograms of the distribution of stationary probabilities of parameter states that have the most significant impact on UAV CR metrics.

Table 2. Sensitivity analysis of UAV CR metrics to the variations in the input parameters

Group	Parameters	Values	Impact					Sensitivity
			A_g	P_1	P_2	P_3	P_4	
Operational	T_{op}	1→20 h	+31.6%	+67.4%	-91.8%	-90.6%	-75.0%	High
	τ_{op}	0.5→10 h	-15.9%	-33.9%	+45.9%	+46.9%	+37.7%	Medium
Threat	T_a	1→20 min	+33.2%	+15.8%	+93.1%	-90.6%	-79.2%	High
Recovery	τ_a	5→120 s	-31.2%	-14.8%	-88.1%	+87.5%	+74.2%	Critical
	τ_{RC}	5→20 min	+16.9%	+6.2%	+54.7%	+59.4%	-53.5%	Medium
	P_a	0.4→0.9	+28.5%	+12.4%	+83.6%	-15.6%	-75.8%	Critical
Pentesting	T_{PT}	20→50 h	+1.7%	+1.8%	+1.3%	≈ 0%	-5.0%	Low
	τ_{PT}	1→5 h	-51.0%	-50.8%	-50.9%	-50.0%	+145%	Critical

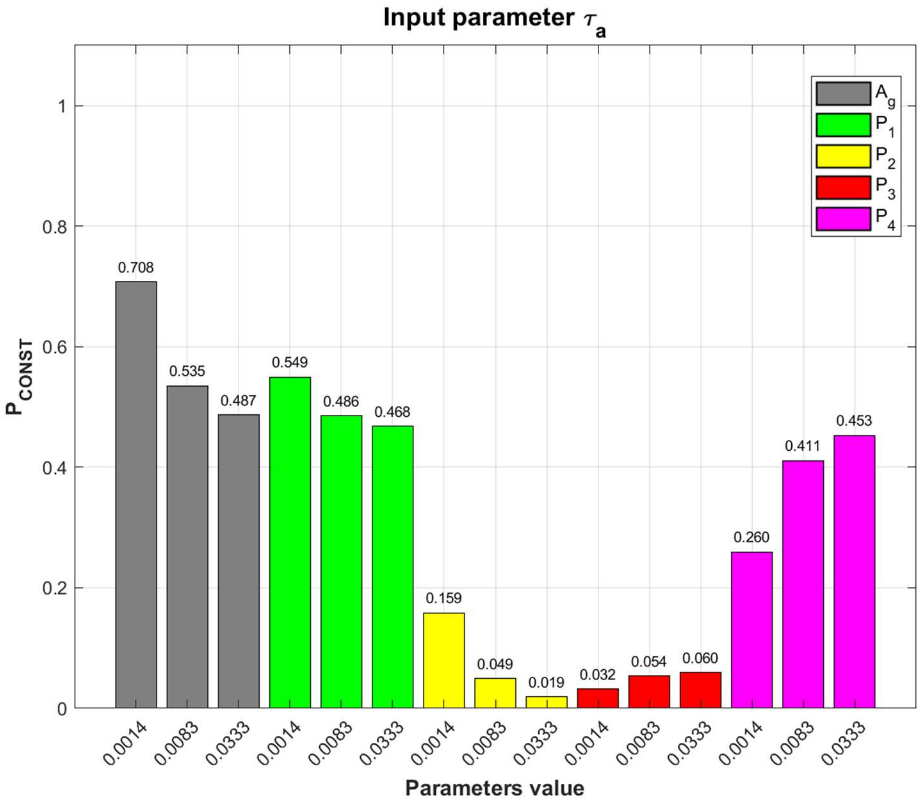

Figure 6. Histogram of the distribution of stationary probabilities of states when the operational recovery time changes τ_a

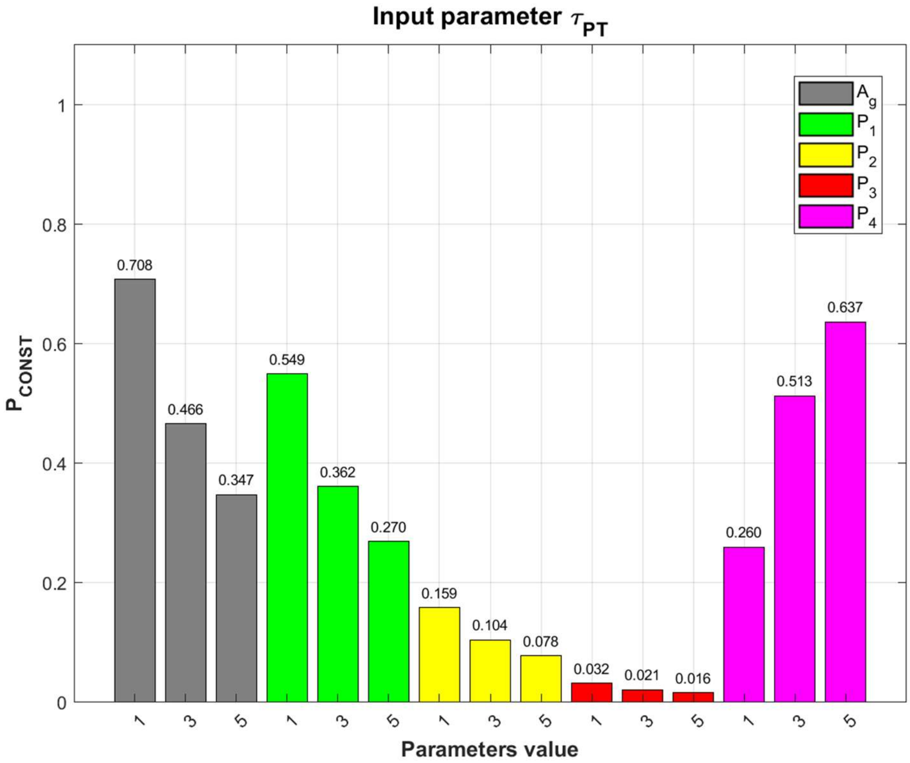

Figure 7. Histogram of the distribution of stationary probabilities of states when changing the duration of PT τ_{PT}

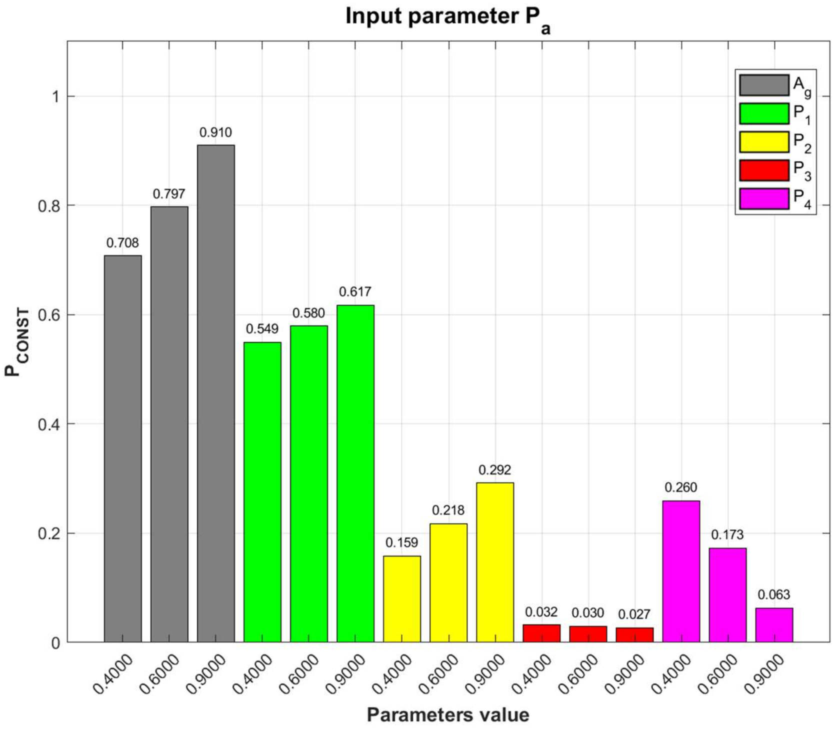

Figure 8. Histogram of the distribution of stationary probabilities of states when the probability of successful recovery changes P_a

Based on the modelling results, an analysis of the sensitivity of key system metrics to variations in input parameters was performed. The results are classified according to four levels of impact (Critical, High, Medium, Low), as shown in Table 2. The time characteristics of recovery and PT processes have the most significant impact:

- Even a slight increase in operational recovery time (τ_a) leads to a 31.2% drop in A_g availability and nearly doubles the risk of compromise. This indicates that response speed is more important than passive protection (Figure 6). This necessitates further research into this relationship.
- PT duration (τPT) demonstrates the highest negative impact among all parameters (A_g drop of 51.0%). Excessive PT duration effectively paralyzes the system, rendering it unfits for mission execution (Figure 7).
- Increasing the probability of automatic recovery (P_a) provides a 28.5% increase in availability but increases the probability of successful mission completion by 83.6%, allowing the system to function effectively even under intense attacks (Figure 8).

Factors with a high impact include parameters that determine the defense and operation strategy. T_a attack interval and the T_{op} mission interval are strong external levers.

- Increasing the interval between missions (T_{op}) has a positive effect on overall reliability (A_g increases by 31.6%) and reduces risks, but this comes at the cost of drastically reduced mission success probability (P_2 drops by 91.8%).
- Increasing the interval between attacks (T_a) increases system availability by 33.2%. At the same time, there is an almost twofold increase in the probability of successful mission completion and a tenfold decrease in the risk of compromise, confirming the critical dependence of mission success on the density of the enemy's cyber influence.

The analysis revealed nonlinear effects for the parameters of average impact:

- Mission duration (τ_{op}) has a predictable negative impact: extending the time of operations in enemy territory increases the window of opportunity for attack, leading to a 15.9% decrease in availability and a 46.9% increase in the probability of compromise.
- Recovery time (τ_{RC}) showed an unexpected positive effect. Modeling shows that longer deep recovery reduces the frequency of repeated transitions to the PT state, which cumulatively compensates for lost time.

A significant scientific finding is the establishment of the system's low sensitivity to the frequency of penetration tests (T_{PT}). Altering this parameter improves preparedness by a mere 1.7%.

VI. CONCLUSION

The paper presents and justifies a combined method for assessing the UAVs' CR, which combines analytical and experimental procedures, as well as modeling the dynamics of SSMM. This allows overcoming the limitations of static risk assessment methods and isolated penetration tests, creating a closed cycle of system verification and protection. A combined method has been developed and formalized in IDEF0 notation.

Based on the constructed SSMM, a sensitivity analysis was performed, which revealed that the most critical parameter of cyber resilience is the response speed of the system.

It was established that an increase in the operational recovery time leads to a 31.2% drop in the availability coefficient and almost doubles the risks of compromise (+87.5%). Therefore, a critical design guideline is to prioritize automatic recovery mechanisms that ensure an operational recovery time (τ_a) of under 60 seconds. The priority of automation of recovery processes over the frequency of checks was quantitatively confirmed. Modeling showed that increasing the probability of successful recovery provides a significant increase in the probability of mission success (by 83.6%). Consequently, for high-intensity scenarios, the target probability of auto-recovery P_a should be at least 0.9, which sets a benchmark for architectural resilience regardless of the fluctuating intrusion success rate. At the same time, the hypothesis about the effectiveness of frequent PT has been refuted: changing the inspection interval has a minor impact on availability (<2%), while excessive duration of PT procedures can reduce system availability by 51.0%. This refutes the necessity for excessively long and frequent checks and suggests that the strategy should concentrate not on check frequency, but on its speed and the automation of PT procedures. Specifically, it is recommended to limit the duration of field PT sessions (τ_{PT}) to a minor fraction (e.g., <15%) of the average mission cycle to avoid critical availability drops.

Thus, the use of the mathematical apparatus of Markov processes harmoniously complements the IMECA and PT methods since it allows the study of the system's behavior in dynamic mode, the influence of PT processes on the final measures of availability, and the justification of requirements for these processes.

Prospects for further research are aimed at developing a multi-fragment SSMM, which ensures the integration of PT processes and considers the factor of combined intrusion modes, as well as uses time parameters of the frequency and duration of PT procedures with a UAV simulator.

References

[1] F. Tlili, L. C. Fourati, S. Ayed, and B. Ouni, "Investigation on vulnerabilities, threats and attacks prohibiting UAVs charging and depleting UAVs batteries: Assessments & countermeasures," *Ad Hoc Networks*, vol. 129, p. 102805, 2022. https://doi.org/10.1016/j.adhoc.2022.102805.

[2] S. J. Freedberg Jr., "Dumb and cheap: When facing electronic warfare in Ukraine, small drones' quantity is quality," *BreakingDefense.com*, 2023. [Online]. Available at: https://breakingdefense.com/2023/06/dumb-and-cheap-when-facing-electronic-warfare-in-ukraine-small-drones-quantity-is-quality/.

[3] K. Hartmann and K. Giles, "UAV exploitation: A new domain for cyber power," *Proceedings of the 2016 8th International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia, 2016, pp. 205–221. https://doi.org/10.1109/CYCON.2016.7529436.

[4] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations," *Internet of Things*, vol. 11, p. 100218, 2020. https://doi.org/10.1016/j.iot.2020.100218.

[5] The New Geopolitics Research Network, "Ukrainian Drones vs Russian Jamming," *NewGeopolitics.org*, 2024. [Online]. Available at: https://www.newgeopolitics.org/2024/06/10/ukrainian-drones-vs-russian-jamming/.

[6] Royal United Services Institute for Defence and Security Studies, "Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine," *RUSI*, 2023. [Online]. Available at: https://static.rusi.org/403-SR-Russian-Tactics-web-final.pdf.

[7] Mezha, "DJI Mavic 3 was discontinued: What will happen next and are there Ukrainian analogues," *Mezha.ua*, 2023. [Online]. Available at: https://oboronka.mezha.ua/en/dji-mavic-3-znyali-z-virobnictva-shcho-bude-dali-ta-chi-ye-ukrajinski-analogi-302336/. (in Ukrainian)

[8] Y. Mekdad *et al.*, "A survey on security and privacy issues of UAVs," *Computer Networks*, vol. 224, no. 109626, 2023. https://doi.org/10.1016/j.comnet.2023.109626DOI: 10.1016/j.comnet.2023.109626.

[9] H. Dui, C. Zhang, G. Bai, and L. Chen, "Mission reliability modeling of UAV swarm and its structure optimization based on importance measure," *Reliability Engineering & System Safety*, vol. 215, p. 107879, 2021. https://doi.org/10.1016/j.ress.2021.107879.

[10] E. Zaitseva *et al.*, "Comparative reliability analysis of unmanned aerial vehicle swarm based on mathematical models of binary-state and multi-state systems," *Electronics*, vol. 13, no. 22, p. 4509, 2024. https://doi.org/10.3390/electronics13224509.

[11] I. Kliushnikov, "Assessment of the safety of using unmanned aerial vehicles using Markov models," *Systems of Arms and Military Equipment*, no. 4(76), pp. 51–57, 2023. https://doi.org/10.30748/soivt.2023.76.05.

[12] V. Moskalenko, A. Korobov, and Y. Moskalenko, "Object detection with affordable robustness for UAV aerial imagery: model and providing method," *Radioelectronic and Computer Systems*, no. 3, pp. 55–66, 2024. https://doi.org/10.32620/reks.2024.3.04.

[13] Y. Feng, W. Xu, Z. Zhang, and F. Wang, "Continuous hidden Markov model based spectrum sensing with estimated SNR for cognitive UAV networks," *Sensors*, vol. 22, no. 7, p. 2620, 2022. https://doi.org/10.3390/s22072620.

[14] V. Kharchenko, I. Kliushnikov, A. Rucinski, H. Fesenko, and O. Illiashenko, "UAV fleet as a dependable service for smart cities: Model-based assessment and application," *Smart Cities*, vol. 5, no. 3, pp. 1151–1178, 2022. https://doi.org/10.3390/smartcities5030058.

[15] Z. Yu, Z. Wang, J. Yu, D. Liu, H. H. Song, and Z. Li, "Cybersecurity of unmanned aerial vehicles: A survey," *IEEE Aerospace and Electronic Systems Magazine*, vol. 39, no. 9, pp. 182–215, 2024. https://doi.org/10.1109/MAES.2023.3318226.

[16] P.-Y. Kong, "A survey of cyberattack countermeasures for unmanned aerial vehicles," *IEEE Access*, vol. 9, pp. 148244–148263, 2021. https://doi.org/10.1109/ACCESS.2021.3124996.

[17] H. Zemlianko and V. Kharchenko, "Cybersecurity risk analysis of multifunctional UAV fleet systems: a conceptual model and IMECA-based technique," *Radioelectronic and Computer Systems*, no. 4, pp. 152–170, 2023. https://doi.org/10.32620/reks.2023.4.11.

[18] B. Branco, J. S. Silva, and M. Correia, "D3S: A drone security scoring system," *Information*, vol. 15, no. 12, p. 811, 2024. https://doi.org/10.3390/info15120811.

[19] M. Ficco, D. Granata, F. Palmieri, and M. Rak, "A systematic approach for threat and vulnerability analysis of unmanned aerial vehicles," *Internet of Things*, vol. 26, p. 101180, 2024. https://doi.org/10.1016/j.iot.2024.101180.

[20] C. S. Veerappan, P. L. K. Keong, V. Balachandran, and M. S. B. M. Fadilah, “DRAT: A penetration testing framework for drones,” *Proceedings of the 2021 IEEE 16th Conference on Industrial Electronics and Applications (ICIEA)*, Chengdu, China, 2021, pp. 498–503. https://doi.org/10.1109/ICIEA51954.2021.9516363.

[21] A. Abakumov and V. Kharchenko, “Combining experimental and analytical methods for penetration testing of AI-powered robotic systems,” *Proceedings of the 7th Int. Conf. on Computational Linguistics and Intelligent Systems (COLINS 2023)*, Kharkiv, Ukraine, 2023, vol. 3403, pp. 470–481. [Online]. Available: https://ceur-ws.org/Vol-3403/paper40.pdf.

[22] A. Zimba, “A Bayesian attack-network modeling approach to mitigating malware-based banking cyberattacks,” *International Journal of Computer Network and Information Security (IJCNIS)*, Vol.14, No.1, pp.25-39, 2022. https://doi.org/10.5815/ijcnis.2022.01.03.

[23] T. Almutiri, F. Nadeem, “Markov models applications in natural language processing: A survey,” *International Journal of Information Technology and Computer Science (IJITCS)*, vol. 14, no. 2, pp. 1-16, 2022. https://doi.org/10.5815/ijitcs.2022.02.01.

[24] M. Kozlovska and A. Piskozub, “Hybridizing large language models and Markov processes: A new paradigm for autonomous penetration testing,” *Automatic Control and Programming Systems*, vol. 10, no. 2, pp. 146–150, 2025. https://doi.org/10.23939/acps2025.02.146.

[25] R. Ross et al., “Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems,” *National Institute of Standards and Technology*, Gaithersburg, MD, NIST Special Publication (SP) 800-160 Vol. 2 Rev. 1, 2021. https://doi.org/10.6028/NIST.SP.800-160v2r1.

[26] V. Salauyou, “Description styles of fault-tolerant finite state machines for unmanned aerial vehicles,” *Radioelectronic and Computer Systems*, no. 1, pp. 196–206, 2024. https://doi.org/10.32620/reks.2024.1.15.

[27] O. Fedorovich, D. Krytskyi, M. Lukhanin, O. Prokhorov, and Y. Leshchenko, “Modeling of strike drone missions for conducting wave attacks in conditions of enemy anti-drone actions,” *Radioelectronic and Computer Systems*, no. 1, pp. 29–43, 2025. https://doi.org/10.32620/reks.2025.1.02.

[28] P. Artemiou, L. Moysis, I. Kafetzis, N. G. Bardis, M. Lawnik, and C. Volos, “Chaotic agent navigation: Achieving uniform exploration through area segmentation,” *Proceedings of the 2022 12th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Athens, Greece, 2022, pp. 1–7. https://doi.org/10.1109/DESSERT58054.2022.10018663.

ARTEM ABAKUMOV, graduated National Technical University “Kharkiv Polytechnic Institute” (2014), Master’s Degree in “Information Measuring Systems”. PhD student of the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University “KhAI”, Kharkiv, Ukraine.

Scientific interests: UAVs cybersecurity, penetration testing, vulnerability assessment.

Prof. VYACHESLAV KHARCHENKO, graduated Kharkiv Higher Military Engineering College of Rocket Troops, Dr. of Sciences in Engineering (1995), Corr. Member of National Academy of Science of Ukraine (2025). Head of the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University “KhAI”, Kharkiv, Ukraine.

Scientific interests: Dependable and resilient computing, safety and cybersecurity of I&C systems and critical infrastructures; Intelligent UXV systems for dangerous spaces; Explainable AI as a Service, AI vs AI scenarios.

Prof. YURII PONOCHOVNYI, graduated National Aerospace University “KhAI”, Dr. of Sciences in Engineering (2021). Professor of the Department of Information Systems and Technologies, Poltava State Agrarian University, Poltava, Ukraine. Scientific interests: Information systems and technologies, reliability and safety assessment, cybersecurity of critical systems.