Міністерство освіти і науки України
Національний аерокосмічний університет
ім. М. Є. Жуковського «Харківський авіаційний інститут»

Кваліфікаційна наукова
праця на правах рукопису

ЗЕМЛЯНКО ГЕОРГІЙ АНДРІЙОВИЧ

УДК 004.056.5:004.896.22:629.7.033.2.001.2

ДИСЕРТАЦІЯ

МЕТОДИ ТА ЗАСОБИ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СИСТЕМИ БАГАТОФУНКЦІЙНИХ ФЛОТІВ БЕЗПІЛОТНИХ АПАРАТІВ В УМОВАХ КОМБІНОВАНИХ КІБЕРАТАК

Спеціальність 125 Кібербезпека
Галузь знань 12 Інформаційні технології

Подається на здобуття наукового ступеня доктора філософії

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

_____ Землянко Г. А.
підпис

Науковий керівник Харченко В’ячеслав Сергійович,
доктор технічних наук, професор

Харків – 2024

АНОТАЦІЯ

Землянко Георгія Андрійовича. Методи та засоби для забезпечення кібербезпеки системи багатофункційних флотів безпілотних апаратів в умовах комбінованих кібератак. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 125 – Кібербезпека. – Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, 2024.

Мета дисертаційної роботи полягає в підвищенні рівня кібербезпеки систем багатофункційних флотів безпілотних апаратів за допомогою розроблення та впровадження ризик-орієнтованих методів та засобів оцінювання та вибору контрзаходів, враховуючи комбіновані кібератаки.

У рамках загальної задачі розглядається розроблення моделей, методів та засобів для аналізу та забезпечення кібербезпеки систем багатофункційних флотів безпілотних апаратів в умовах різноманітних атак.

Часткові задачі включають аналіз технологій та методів оцінювання кібербезпеки, розроблення концептуальних та математичних моделей системи, розроблення методів аналізу кіберзагроз та критичності атак, удосконалення методів вибору контрзаходів, розроблення алгоритмів та програмних засобів для вибору контрзаходів.

Серед нових наукових результатів слід відзначити вперше запропоновані моделі кіберфізичної системи багатофункційних флотів безпілотних апаратів, що охоплюють різні мобільні підсистеми та інформаційну інфраструктуру. Також удосконалено метод аналізу кіберзагроз та впроваджено ефективний метод вибору контрзаходів.

На практичному рівні розроблено алгоритми та програмні засоби для розширеного аналізу кібербезпеки системи багатофункційних флотів безпілотних апаратів. Структура системи та інформаційна технологія для прийняття рішень щодо ризик-орієнтованого оцінювання та вибору контрзаходів також розроблені.

Результати дослідження впроваджено в навчальний процес кафедри, а також в науково-дослідні проекти на замовлення МОН України (№ ДР 0121U112172, № ДР 0121U113842, № ДР 0117U05349, № ДР 0118U003822). Зокрема, запропоновані методи та засоби використовуються в рамках проєктів ФЛІНТ та ГРАНІТ.

Ключові слова: кібербезпека, безпілотний апарат, рій БПЛА, захист інформації, аналіз вразливостей, кібератаки, контрзаходи, ризики, інтерактивні алгоритми, кіберфізична система, багатофункційний флот БПЛА, критична інфраструктура, оцінювання безпеки, інтернет речей, моніторинг, захист зображення, загрози, захист конфіденційності, IMECA-аналіз, комбіновані атаки, експертна оцінка, ієрархічна модель.

Список публікацій здобувача за темою дисертації

1. Anatoly, P., Zemlianko, H., Kharchenko, V. (2020). Prototyping and Rapid Development of IoT Systems in Context of Edge Computing. In: Nechyporuk, M., Pavlikov, V., Kritskiy, D. (eds) Integrated Computer Technologies in Mechanical Engineering. *Advances in Intelligent Systems and Computing*, vol 1113. Springer, Cham. https://doi.org/10.1007/978-3-030-37618-5_23.

2. Assoc. Prof., Dr A. P. Plakhteyev, MSc student H. Zemlianko (KhAI). Section 31. Prototyping and rapid development of IoT systems. //Drozd A. et al. Internet of Things for Industry and Human Application //Volumes 1–3. Volume 2. Modelling and Development. – 2019.

3. Torianyk V., Kharchenko V., Zemlianko H. IMECA based assessment of internet of drones systems cyber security considering radio frequency vulnerabilities //IntelITSIS //CEUR Workshop Proceedings. – 2021. – С. 460-470.

4. Pevnev, V., Tsuranov, M., Zemlianko, H., Amelina, O. (2021). Conceptual Model of Information Security. In: Nechyporuk, M., Pavlikov, V., Kritskiy, D. (eds) Integrated Computer Technologies in Mechanical Engineering - 2020. ICTM 2020. *Lecture Notes in Networks and Systems*, vol 188. Springer, Cham. https://doi.org/10.1007/978-3-030-66717-7_14.

5. Pevnev, V., Plakhteev, A., Tsuranov, M., Zemlianko, H., Leichenko, K. (2022). “Smart City” Technology: Conception, Security Issues and Cases. In: Nechyporuk, M., Pavlikov, V., Kritskiy, D. (eds) Integrated Computer Technologies in Mechanical Engineering - 2021. ICTM 2021. *Lecture Notes in Networks and Systems*, vol 367. Springer, Cham. https://doi.org/10.1007/978-3-030-94259-5_19.

6. Pevnev, V., Frolov, A., Tsuranov, M., & Zemlianko, H. (2022). Ensuring the Data Integrity in Infocommunication Systems. *International Journal of Computing*, *21*(2), 228-233. https://doi.org/10.47839/ijc.21.2.2591.

7. Zemlianko H., Kharchenko V. Cybersecurity risk analysis of multifunctional UAV fleet systems: a conceptual model and IMECA-based technique. *Radioelectronic and Computer Systems*. 2023. № 4. С. 152–170. URL: https://doi.org/10.32620/reks. 2023.4.11.

8. Zemlianko H., Kharchenko V. Cyber Security Systems of Highly Functional Uav Fleets for Monitoring Critical Infrastructure: Analysis of Disruptions, Attacks and Counterapproaches. *Èlektronnoe modelirovanie*. 2024. Т. 46, № 1. С. 41–54. URL: https://doi.org/10.15407/emodel.46.01.041.

9. Землянко Г.А., Харченко В.С. IMECA-аналіз кібербезпеки систем багатофункціональних флотів БПЛА при комбінованих атаках: базові моделі та вибір контрзаходів. *Measuring and computing devices in technological processes*. 2023. № 4. С. 225–233. URL: https://doi.org/10.31891/2219-9365-2023-76-30.

10. Землянко Г.А., Пєвнєв В.Я., Ніколас Бардис, Харченко В. С., Розділ 9. Розробка моделі загроз для безпілотних літальних апарптів. 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. 159–177. ISBN 978-617-8335-01-4. URL:https://dspace. library.khai.edu/xmlui/handle/123456789/5307.

11. Оцінка кібербезпеки Інтернету систем дронів з урахуванням радіочастотної вразливості на основі. // Теоретичне обгрунтування методології, структури, моделі, методи оцінювання надійності і живучості інтелектуальних

систем моніторингу потенційно небезпечних і військових об'єктів з використанням багатоцільових флотів БПЛА : звіт про НДР (проміж.) : Д503-1/2021-Ф / М-во освіти і науки України, Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харків. авіац. ін-т" ; керівник Харченко В. С. ; викон.: Морозова О. І. [та інш.]. - Харків, 2021. - 230 с. - № ДР 0121U112172.

12. Методи контролю та оцінювання інформаційної безпеки комп’ютерних мереж з використанням пентестингу. // Розроблення засобів тестування та верифікації вбудованих і розподілених гарантоздатних ІТ-систем та інфраструктур : звіт про НДР (проміж.) / М-во освіти і науки України, Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харків. авіац. ін-т" ; керівник Харченко В. С. ; викон.: Фесенко Г. В. [та інш.]. - Харків, 2021. - 197 с. - № ДР 0121U113842.

13. Розроблення програмно-апаратних засобів для систем розумного міста. // Розробка моделей та засобів кібербезпеки інформаційних і комунікаційних систем. Впровадження запропонованих принципів, моделей та методів оцінювання та розробки гарантоздатних комп'ютерних систем, мереж та ІТ-інфраструктур : звіт про НДР (заключ.) / М-во освіти і науки України, Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харків. авіац. ін-т" ; керівник Харченко В. С. ; викон.: Лисенко І. В. [та інш.]. - Харків, 2020. - 245 с. - № ДР 0117U05349 - Інв. № 0221U000032.

14. Методи і засоби побудови енергоефективних засобів побудови смарт-систем з використанням IoT і Edge комп’ютингу. // Розроблення методів формування вимог, аналізу, оцінювання та зменшення витрат ресурсів протягом життєвого циклу програмного забезпечення, мобільних пристроїв, хмарних обчислень : звіт про НДР (заключ.) : Д503-1/2018-Ф . Т. 1 / М-во освіти і науки України, Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харків. авіац. ін-т" ; керівник Харченко В. С. ; викон.: Колісник М. О. [та інш.]. - Харків, 2020. - 232 с. - № ДР 0118U003822 - Інв. № 0221U000030.

15. Heorhii Zemlianko, Kyrylo Leichenko, "Smart City" technology: conception, security issues and cases. Book of abstracts of the International Workshop on Reliability Engineering and Computational Intelligence 2020 (RECI 2020), Zilina,

Slovakia, 27-29 October 2020. P. 41. URL: https://ki.fri.uniza.sk/RECI2020/Abstracts%20of%20RECI%202020.pdf

16. Землянко Г.А. Implementation of smart grid technologies in the power system of Ukraine. Матеріали III НТК «Інформаційна, функційна і кібербезпека» (СКІФіК-2023), 30 лист.– 1 груд. 2023 р. Харків, Україна. Харків: НАКУ «ХАІ», 2023. С. 105–106.

17. Землянко Г.А. Ensuring cybersecurity of the cyber physical system of combined fleets of unmanned aerial, ground and sea vehicles. Всеукраїнська науково-технічна конференція «Інтегровані комп'ютерні технології в машинобудуванні» ІКТМ 2023, Харьків, 2023.

ANNOTATION

Zemlyanko Heorhii Andriiovych. Methods and means to ensure cybersecurity of multi-functional fleets of UAV under conditions of combined cyber attacks. - Qualification scientific work on the rights of a manuscript.

Dissertation for the degree of Doctor of Philosophy in the speciality 125 - Cybersecurity. - National Aerospace University "Kharkiv Aviation Institute", Kharkiv, 2024.

The dissertation aims to enhance the cybersecurity of multi-functional fleets of unmanned aerial vehicles (UAVs) by developing and implementing methods and tools for risk-oriented assessment and selection of countermeasures, taking into account combined cyberattacks.

The overarching objective involves the development of models, methods, and tools for the analysis and cybersecurity of multi-functional fleets of UAVs under conditions of both individual and combined attacks. The specific tasks include:

1. Analysis of functions, technologies, and methods for evaluating and ensuring the cybersecurity of UAV systems, with a justification of the research's purpose, tasks, and methodology.

2. Development of conceptual and mathematical models for the cyber-physical system of multi-functional fleets of UAVs as the object of cybersecurity assessment.

3. Formulation of a method for analyzing cyber threats, consequences, and the criticality of individual and combined attacks on the assets of the cyber-physical system.

4. Refinement of the method for selecting a set of countermeasures to ensure the cybersecurity of the cyber-physical system, considering various components of cybersecurity and addressing both individual and combined cyberattacks.

5. Development of algorithms, software tools, and information technology for conducting analysis and selecting countermeasures to ensure the cybersecurity of multi-functional fleets of UAVs.

6. Implementation of the proposed methods and tools in state and international research projects and educational programs, as well as in substantiating security requirements for UAV systems.

Novel scientific results include:

1. Introduction of models for the cyber-physical system of multi-functional fleets of UAVs, providing a theoretical-multiset representation of software and hardware components at different hierarchy levels, intruders, threats, vulnerabilities, and attacks.

2. Enhancement of the IMECA analysis method, detailing the impact on various security properties and subsystems, along with the development of models for combined sequential-parallel cyberattacks by different perpetrators and means.

3. Improvement of the method for selecting countermeasures by forming a set of countermeasures considering the influence on different cybersecurity components under conditions of individual and combined cyberattacks, using directed search procedures for coverage options.

The proposed methods and tools have been implemented in the educational process of the department, contributing to the training of bachelor's, master's, and doctoral students specializing in Cybersecurity and Information Protection. Moreover, they have been applied in scientific research projects commissioned by the Ministry of Education and Science of Ukraine, including the FLINT project led by Dr. Harchenko V.S. and the GRANIT project led by Dr. Sklyar V.V.

Keywords: cyber security, unmanned aerial vehicle, UAV swarm, information protection, vulnerability analysis, cyber attacks, countermeasures, risks, interactive algorithms, cyber physical system, multifunctional UAV fleet, critical infrastructure, security assessment, Internet of Things, monitoring, image protection, threats, privacy protection, IMECA - analysis, combined attacks, expert assessment, hierarchical model.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

БПЛА	—	Безпілотний літальний апарат
БА	—	Безпілотні апарати
БНА	—	Безпілотні сухопутні апарати
БПА	—	Безпілотні підводні апарати
БНК	—	Безпілотні надводні кораблі
БСМ	—	Бездротова сенсорна мережа
ІБ	—	Інформаційна безпека
ЛСМ	—	Літаюча сенсорна мережа
МСЕ	—	Міжнародний союз електрозв'язку
НДР	—	Науково-дослідна робота
ПК	—	Персональний комп'ютер
ПЗ	—	Програмне забезпечення
КЗ	—	Канал зв’язку
КІ	—	Критична інфраструктура
КБ	—	Кібербезпека
КЦДС	—	Конфіденціальність, цілісність, доступність та спостереженість
СБФ БПЛА	—	Система багатофункцыйних флотыв БПЛА
CIA	—	Confidentiality, Integrity, and Availability
DDoS	—	Distributed Denial of Service
DSN	—	Distributed Sensor Networks
FANET	—	Flying Ad-Hoc Network
RF	—	Radio Frequency
UAV	—	Unmanned Aerial Vehicle
UAS	—	Unmanned Aerial System
WSN	—	Wireless Sensor Network

ВСТУП

Обґрунтування вибору теми дослідження. В останні роки застосування безпілотних апаратів значно зростає в різних сферах, включаючи морську, повітряну та наземну. Системи багатофункційних флотів безпілотних апаратів (СБФ БА) використовуються для виконання різноманітних завдань, таких як навігація, збір та аналіз даних, відстеження, моніторинг і навіть виконання військових операцій. Однак зі зростанням їх використання збільшується ймовірність кібератак, спрямованих на ці системи.

Розвиток технологій та зростаюча кількість загроз кібербезпеці вимагає пошуку нових методів і засобів для захисту систем БА від кібератак. Особливу увагу слід приділити системам багатофункційних флотів БА, оскільки вони можуть бути особливо вразливі через велику кількість взаємодіючих елементів і компонентів. Таким чином, проведення досліджень в галузі забезпечення кібербезпеки цих систем є актуальним та важливим завданням, яке потребує подальшого вивчення.

Об'єкт дослідження – процеси забезпечення кібербезпеки системи багатофункційних флотів безпілотних апаратів.

Предмет дослідження – моделі, методи та засоби інформаційної технології забезпечення кібербезпеки системи багатофункційних флотів безпілотних апаратів.

Мета і завдання дослідження. Метою дослідження є підвищення кібербезпеки систем багатофункційних флотів безпілотних апаратів шляхом розроблення і впровадження методів і засобів її ризик-орієнтованого оцінювання та вибору контрзаходів з урахуванням комбінованих кібератак.

Для досягнення мети дослідження необхідно вирішити наступні завдання:

– аналіз типів і функцій безпілотних апаратів (літальних, наземних, морських), методів і засобів оцінювання та забезпечення кібербезпеки систем на їх основі;

– розроблення концептуальної та математичних моделей кіберфізичної системи багатофункційних флотів безпілотних апаратів як об’єкта оцінювання кібербезпеки;.

– розроблення методу аналізу кіберзагроз, наслідків та критичності одиничних і комбінованих атак на активи кіберфізичної системи багатофункційних флотів БПЛА;

– удосконалення методу вибору сукупності контрзаходів для забезпечення кібербезпеки кіберфізичної системи багатофункційних флотів БПЛА;

– розроблення алгоритмів, програмних засобів та інформаційної технології для проведення аналізу і вибору контрзаходів для забезпечення кібербезпеки системи багатофункційних флотів БПЛА;

– впровадження запропонованих методів і засобів в державних та міжнародних науково-дослідних проектах і навчальному процесі, а також при обґрунтуванні вимог до безпеки систем БПЛА.

Методи дослідження. У дисертаційній роботі використовувались методи математичного моделювання, теорії ймовірності та теоретико-множинні моделі, IMECA-таблиці, матриці критичності та дослідженні методу вибору контрзаходів за критеріями, критерії мінімізації та максимізації, алгоритми пошуку оптимальних підмножин контрзаходів.

Наукова новизна отриманих результатів:

– **вперше запропоновано** *моделі* кіберфізичної системи багатофункційних флотів безпілотних апаратів як об’єкта оцінювання кібербезпеки, які, на відміну від відомих, описують концептуальну схему, що об’єднує комплекс мобільних підсистем, а саме безпілотних літальних, наземних і безекіпажних апаратів та інформаційну інфраструктуру, надають теоретико-множинне представлення програмно-апаратних компонентів на різних рівнях ієрархії, порушників, загроз, вразливостей і атак та їх онтологічних зв’язків, і забезпечують повноту аналізу такої системи в умовах зовнішніх впливів, а також надають можливості формування множини контрзаходів для захисту фізичних і кіберактивів;

– **удосконалено** *метод* (IMECA) аналізу кіберзагроз, наслідків та критичності атак на активи кіберфізичної системи багатофункційних флотів безпілотних літальних апаратів шляхом деталізованого опису впливу на різні властивості безпеки (конфіденційність, цілісність, доступність, спостережність) і різні підсистеми, а також розроблення моделей і послідовностей комбінованих послідовно-паралельних кібератак різними порушниками і засобами, що надає змогу підвищити достовірність оцінювання кібербезпеки та обґрунтувати стратегії захисту та вибір контрзаходів для забезпечення прийнятного ризику;

– **удосконалено** *метод* вибору контрзаходів для забезпечення кібербезпеки кіберфізичної системи багатофункційних флотів безпілотних літальних апаратів завдяки формуванню множини контрзаходів з врахуванням впливу на різні складові кібербезпеки, в умовах одиничних та комбінованих кібератак, з використанням процедур спрямованого пошуку варіантів покриття, що забезпечує прийнятний ризик при мінімальних витратах або мінімальний ризик при обмежених витратах.

Особистий внесок здобувача полягає у розробці методів, моделей та інструментальних засобів, які забезпечують вирішення поставлених задач, описаних вище. Всі основні результати отримані автором особисто та опубліковано у роботах (див. Додаток А).

У працях, які опубліковані у співавторстві, автору належать: модель кіберфізичної системи багатофункційних флотів безпілотних апаратів, як об’єкта оцінювання кібербезпеки; метод (IMECA) аналізу кіберзагроз, наслідків та критичності атак на активи кіберфізичної системи багатофункційних флотів безпілотних літальних апаратів; модель комбінованих послідовно-паралельних кібератак різними порушниками і засобами; метод вибору контрзаходів для забезпечення кібербезпеки кіберфізичної системи багатофункційних флотів безпілотних літальних апаратів.

Абробація матеріалів дисертації. Основні положення та ідеї дисертаційної роботи доповідалися та обговорювалися на конференціях: “International Workshop

on Intelligent Information Technologies & Systems of Information Security” (м. Хмельницький, 2021 р.); "Integrated Computer Technologies in Mechanical Engineering" (м. Харків, 2020, 2021, 2023); "International Workshop on Reliability Engineering and Computational Intelligence 2020 (RECI 2020)" (City Zilina, Slovakia, 2020); Матеріали ІІІ НТК “Інформаційна, функціональна та кібербезпека” (СКІФіК-2023)” (Харків, Україна, 2023 р.).

Зв’язок з науковими програмами, планами, темами. Дисертаційна робота виконана у Національному аерокосмічному університеті ім. М.Є. Жуковського «Харківський авіаційний інститут» відповідності з державними програмами та планами НДР:

– при виконанні міжнародного проекту Internet of Things: Emerging Curriculum for Industry and Human Applications (ALIOT, №573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP) впродовж 2016-2019 рр., за програмою ЄС ERASMUS +;

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

– при виконанні держбюджетної науково-дослідницької роботи «Методи, моделі та інформаційні технології підвищення надійності та безпечності складних ІТ-систем на етапах розроблення та впровадження» ДР № 0121U113842 впродовж 2021-2023 рр.;

– при виконанні держбюджетної науково-дослідницької роботи «Методи, програмно-апаратні засоби та інформаційні технології розроблення і модернізації гарантоздатних комп'ютерних систем, мереж та ІТ-інфраструктур» ДР № 0117U05349 впродовж 2018-2020 рр.;

– при виконанні держбюджетної науково-дослідницької роботи «Методологія сталого розвитку та інформаційні технології зеленого комп'ютингу та комунікацій» ДР № 0118U003822 впродовж 2018-2020 рр.

Роль автора у зазначених НДР в яких автор був безпосереднім виконавцем, полягає у розробці та підвищені показників кібербезпеки та точності оцінювання ризиків для безпілотних мобільних і стаціонарних систем та критичної інфраструктури.

Практичне значення отриманих результатів. Практичні результати полягають у доведенні теоретичних положень дисертаційної роботи до конкретних алгоритмів, інструментальних засобів та рекомендацій по підвищенню кібербезпеки СБФ БПЛА. Результати дисертаційної роботи впроваджено у додатку Є:

– у навчальному процесі кафедри комп'ютерних систем, мереж і кібербезпеки ХАІ за спеціальністю 125 – Кібербезпека і захист інформації;

– при виконанні держбюджетної науково-дослідницької роботи ДР № 0121U112172 впродовж 2021 -2023 рр., ДР № 0121U113842 впродовж 2021 -2023 рр., ДР № 0117U05349 впродовж 2018-2020 рр., ДР № 0118U003822 впродовж 2018-2020 рр., а також у міжнародному проєкті ALIOT, №573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP, 2016-2020 рр.;

– при обґрунтуванні вимог та аналізі кібербезпеки комп’ютерних мереж і мобільних систем (компанія CD-Link).

Структура та обсяг дисертації. Дисертація складається із вступу, чотирьох розділів, висновку, списку виконаних джерел і додатків. Загальний обсяг дисертації складає 242 сторінки, з яких анотація на 7 сторінках, зміст на 3 сторінках, перелік умовних позначень на 1 сторінці, основний текст на 166 сторінках, список використаних джерел із 152 найменувань на 19 сторінках, додатки на 45 сторінках. Робота містить 39 таблиць та 33 рисунків.

Публікації. За темою дисертаційної роботи було опубліковано 13 наукових праць, серед яких: 2 статті у наукових фахових виданнях України категорії Б; 3 статті у англомовних журналах категорії А, що індексовані у базі даних Scopus (квартіль Q3); 2 колективні монографії; 6 публікацій в працях міжнародної конференції, матеріали якої включено у базу даних Scopus.

РОЗДІЛ 1. АНАЛІЗ ФУНКЦІЙ, ТЕХНОЛОГІЙ ТА МЕТОДІВ ДЛЯ ОЦІНЮВАННЯ ТА ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СИСТЕМ БЕЗПІЛОТНИХ АПАРАТІВ. ПОСТАНОВКА ЗАВДАННЯ ДОСЛІДЖЕНЬ

1.1 Аналіз технологій розробки та використання систем безпілотних апаратів

Останніми роками успішні застосування безпілотних апаратів у бойових умовах, космосі, глибинному морі та інших небезпечних та віддалених середовищах привернули значний науковий інтерес. Автономія була визначена в багатьох дослідженнях, але визначення, запропоноване робочою групою ALFUS (рівні автономії для безпілотних систем) Інституту національних стандартів і технологій (NIST), є найбільш комплексним і стандартизованим [1]. З цього визначення можна зробити висновок, що "автономність" - це здатність безпілотної системи бути незалежною від оператора і керуватися самостійно. Отже, можна визначити безпілотні апарати як машини, які можуть функціонувати без людського впливу або нагляду.

Технологія безпілотних апаратів відзначає значний розвиток. Сучасні автомобілі мають напівавтономні функції, такі як автопаркування та адаптивний круїз-контроль. БПЛА, популярні військове застосування протягом десятиліть, свідчать про стрімкий прогрес у цій галузі [2]. У перспективі очікується інтеграція безпілотних сухопутних апаратів (БНА), безпілотних підводних апаратів (БПА), безпілотних надводних кораблів (БНК) та робототехніки в повсякденне життя.

Безпілотні апарати, які відіграють важливу роль у безпеці людей, обороні, логістиці та громадському сервісі, повинні емулювати прийняття рішень людини, особливо під час кібератак чи відмови обладнання.

Безпілотні апарати перейшли від дистанційного керування до складних наземних (БНА), повітряних (БПЛА) та морських (БПА та БНК) систем. Ці транспортні засоби працюють автономно, покладаючись на впізнавання середовища або програмування [3,4].

Спочатку розроблені для військових застосувань, таких як розмінування та спостереження, БНА тепер розширюються на цивільні сфери, такі як постачання та сільське господарство [5,6]. БПЛА відзначаються у спостереженні та зборі даних, досліджуючи небезпечні або недоступні області з високою швидкістю та розвиненими візуальними та комунікаційними можливостями [7-9]. Цивільне використання БПЛА охоплює доставку, повітряну фотографію, сільське господарство та моніторинг погоди [10-12].

Безпілотні морські апарати, що об'єднують в собі БПА та БНК, відіграють важливу роль у морських операціях, включаючи контроль над мінами, морську безпеку та блокадні місії [10], досліджують недоступні підводні області за допомогою камер, гідролокаторів та роботизованих рук для збору зразків. Вони виконують різноманітні завдання у військовій та цивільній сферах, такі як морські дослідження, розмінування та розвідка [12,13].

Активно вивчається нова гетерогенна система нагляду, що виходить за межі однієї платформи і співпрацює з безпілотними повітряними апаратами, наземними, надводними та підводними апаратами [14,15,16]. З однієї платформи поля бою в галузях суші, моря, повітря, космосу, електромагнітики та мереж стають все більше взаємопов'язаними, перетворюючись на багатоплатформний бій у різних середовищах [17].

Останнім часом активно проводяться дослідження, використання співпраці між безпілотними транспортними засобами, такими як комбінації БПЛА-БНА та БПЛА-БНК або БНК-БПА [18,19,20].

Однак цей технологічний стрибок також викликає нагальну проблему - кібербезпека. Оскільки ці безпілотні апарати все більше інтегруються в критичні операції, вразливість перед кіберзагрозами стає більш очевидною.

Зазначений у тексті розвиток безпілотних апаратів свідчить про необхідність удосконалення кібербезпеки в цій сфері. Для дисертаційного дослідження важливим стане аналіз існуючих БПЛА, їхніх особливостей та вже застосованих методів захисту. Подальша робота буде зосереджена на ретельному аналізі уразливостей цих систем і розробці ефективних заходівдля підвищення

кіберзахисту, спрямованих на збереження цілісності, безпеки та безперебійності їхньої роботи.

1.1.1 Призначення та класифікація безпілотних апаратів. Особливості функціонування безпілотних апаратів

Наразі безпілотні апарати виконують широкий спектр завдань, таких як спостереження, ударні операції, транспортування вантажів та радіоелектронне заваджання. Більшість безпілотних апаратів використовуються для ведення спостережень та розвідки в реальному часі, надання цільових вказівок для інших засобів ураження, транспортування вантажів, ретрансляції даних та інших функцій [21, 22, 23, 28, 29, 30, 31].

Терористи й особи, що порушують закон, використовують безпілотні апарати для таких завдань [21, 24, 25, 29, 31]:

– спостереження за об'єктами з охоронним периметром;

– вбивство окремих важливих осіб;

– випуск саморобних засобів ураження;

– пошкодження будівель, культурних об'єктів, інфраструктури та транспортних засобів;

– транспортування заборонених предметів або їхнє випускання на охоронений території;

– перешкоджання повітряному рухові у аеропортах.

Переваги безпілотних апаратів, що ускладнюють їх виявлення та протидію, включають [21, 22, 26, 27, 30, 31]:

– можливість безпечного віддаленого виконання завдань без присутності оператора та отримання оперативної інформації про процес у реальному часі;

– широкий спектр малогабаритних цільових навантажень, таких як радіолокаційні станції (РЛС), засоби радіоелектронної розвідки (РЕР), збройові системи зі спрямованим ураженням та інші;

– можливість тривалого перебування в зонах бойових дій та самостійного придушення ворожих засобів ППО;

– низька помітність безпілотних апаратів в радіолокаційному та оптичному діапазонах завдяки їх невеликим габаритам порівняно з пілотованим транспортом та використанню пластикових та композитних матеріалів у конструкції;

– здатність до маневрів з високими навантаженнями на малих відстанях (до 50 м) та низьких швидкостях (10-30 м/с), що ускладнює ураження ворожих засобів ППО;

– малий розмір, що знижує ймовірність поразки снарядами зенітної артилерії та ускладнює роботу радіопідривників зенітних керованих ракет;

– скритність застосування, забезпечена тихими двигунами та польотом у режимі "радіомовчання" до входу в зону бойового застосування.

Характеристики безпілотних апаратів виявляють додаткові переваги їх структури та експлуатації [22, 28, 30, 31]. Ці переваги включають:

- застосування класичної динамічної схеми для стабільності та простоти управління;

- можливість використання електричних двигунів, що відрізняються простотою експлуатації;

- використання нетрадиційних джерел енергії, таких як сонячні батареї або кріогенне паливо, що дозволяє працювати без обмеження часу;

- зниження витрат на пересування та тимчасове базування компактних підрозділів безпілотних апаратів, ремонт та обслуговування в полевих умовах;

- економічна вигода у розробці та експлуатації порівняно з пілотованим транспортом, при збереженні високих витрат на пілотів, транспорт наземного, морського та повітряного базування.

Перспективи підвищення їхньої ефективності полягають у груповому застосуванні малих та доступних апаратів, що утворюють флот, і спільно виконують завдання, якщо чітко розподілити їх функції [22, 26, 27, 28, 31].

Основні недоліки безпілотних апаратів включають [22, 27, 29, 30, 31]:

– обмеження застосування в залежності від часу та погодних умов для певних категорій;

– низький рівень інтелектуальності у автономному режимі;

– низька скритність каналів радіоуправління (КРУ) та передачі даних;

– низька надійність конструкції;

– вразливість КРУ та каналу супутникової навігації до радіоелектронних перешкод;

– обмежена дальність дистанційного керування з ПУ без додаткових засобів ретрансляції;

– обмеження за масою та складом корисного навантаження.

Якщо розглядати більш детальніше, на прикладі БПЛА, то традиційно використовує обмежений набір обладнання, включаючи навігаційну систему (автономну або засновану на сигналах СРНС) [22], систему зв'язку, яка забезпечує керування з ПУ та передачу телеметричних даних, і цільове навантаження, таке як апаратуру розвідки або засоби ураження.

БПЛА, в порівнянні з пілотованими літаками, обмежені в швидкій реакції на непередбачені обставини під час польоту, діагностиці несправностей та ручному керуванні. Їх висока вразливість до бойових умов та обмежена "інтелектуальність" в автономному режимі створюють виклики, такі як відсутність ключових людських якостей, що впливає на ефективність їх використання в бойових умовах [22].

Під час аналізу БПЛА, як один із видів безпілотних апаратів, було виявлено класифікацію за їх масогабаритними параметрами, швидкістю, призначенням та застосуванням. Існує декілька класифікацій для розмірів та швидкості БПЛА, зокрема американська [32], західноєвропейська [33] та російська [34]. У цій дослідженій роботі [35] представлено гармонізовану класифікацію в Додатку Б, яка об'єднує підходи західноєвропейської та російської систем класифікації.

У таблиці А.5, що додається, подано огляд глобальних вимог і правил, які застосовуються до експлуатації БПЛА [36, 37]. Ця таблиця включає інформацію

про обов'язкові стандарти безпеки, вимоги до сертифікації, експлуатаційні правила, а також вимоги до документації та звітності, пов'язані з експлуатацією БПЛА.

У роботі [26] запропоновано класифікацію безпілотних літальних апаратів (БПЛА) залежно від їх функціональної швидкості польоту, що вкладається в такі категорії:

– малошвидкісні БПЛА зі швидкістю польоту до 200 км/год (максимальна швидкість в межах 250 км/год);

– середньошвидкісні БПЛА зі швидкістями польоту від 150 до 400 км/год (максимальна швидкість в межах 450 км/год);

– швидкісні БПЛА зі швидкістями польоту від 350 до 800 км/год (максимальна швидкість в межах 900-980 км/год).

Виокремлюються такі категорії БПЛА [26, 27, 31]:

1. Багаторазове застосування: розвідувальні, розвідувально-ударні, транспортні, носії засобів озброєння, розширюють функціональні можливості носія, перехоплювачі.

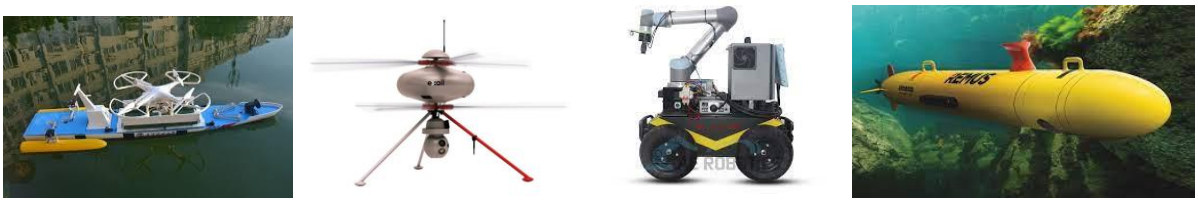
2. Одноразове застосування: хибні цілі, барражують «БПЛА-камікадзе», розвідувально-ударні «БПЛА-камікадзе», перехоплювачі.

Відповідно до кількості одночасно застосовуваних безпілотних апаратів слід розрізняти [26, 28, 29, 31]: поодинокого застосування та групового застосування.

Основна мета безпілотних апаратів — виконання завдань у різних сферах, від військових до комерційних [30, 31, 38]. Військове використання БПЛА вже розповсюджене серед 11 держав, включаючи США, Китай, Росію, та Ізраїль, а також в Україні [30, 39]. Ці застосування обговорюються у різних галузях оборони: ВМС, армія та повітряні сили, які зображені на рисунку 1.1 (а): електронна розвідка, розвідка, заглушення та знищення радіолокаційної системи, передача радіосигналів, спостереження за флотами противника, спостереження за діяльністю противника, моніторинг та контролювання об’єкту, знищення нерозірваних бомб, приманка ракетами, шляхом викиду штучних сигнатур.

Після виникнення безпілотних апаратів у військовій сфері та їх стрімкого розвитку вони швидко знайшли застосування у цивільних галузях [28, 29, 40]. Зокрема, цивільні безпілотні апарати зараз використовуються у географічних дослідженнях, сільському господарстві, пошуково-рятувальних операціях, метеорологічних вимірюваннях, пожежогасінні, виявленні пожеж у лісовому господарстві, нагляді за нелегальним імпортом, моніторингу забруднення та вивченні стану земель, перевірці трубопроводів та електромереж, пошуку нафти та газу, доставці посилок, міському плануванні та виявленні рухомого транспорту на землі [30, 31, 36], як на рисунку 1.1 (б).

а) Використання військових безпілотних апаратів



б) Використання цивільних безпілотних апаратів

Рисунок 1.1 – Використання безпілотних апаратів у різних галузях

Проведений аналіз [21-31] вказує на особливу складність протидії малим безпілотним апаратам — зокрема, малогабаритним і повільним. Додаткові труднощі у виявленні та захисті виникають через:

– застосування високоманеврених (наприклад, «змійка») та «рваних» (з періодичним зависанням або різким зниженням швидкості) режимів руху;

– використання пластикових та композитних матеріалів у конструкції, які слабко відображають електромагнітне випромінювання (EMI);

– використання зв'язку через існуючі мережі мобільних операторів та точок доступу Wi-Fi, замість виділених каналів управління.

Наприкла, малі БПЛА класифікуються як (див. Таблицю А.4):

– нано БПЛА - масою < 0,25 кг, тривалість польоту < 1 год, висота польоту до 300 м, радіус дії до 1 км;

– мікро БПЛА - масою до 5 кг, тривалість польоту близько 1 год, висота польоту до 3 км, радіус дії до 10 км;

– міні БПЛА - масою до 25 кг, тривалість польоту < 4 год, висота польоту до 3 км, радіус дії до 40 км.

Використання малих безпілотних апаратів широко розповсюджене в тактиці військових і терористичних операцій, поділяються на розвідувальні та ударні (останні лише одноразового застосування) з масою корисного навантаження до 20 кг.

Терористичні групи та протизаконні особи використовують такі апарати для різних цілей, таких як [22, 23, 28, 30, 31, 41]:

– обліт об'єктів з метою спостереження;

– точкове виконання атак на ключових осіб;

– засипання території саморобними засобами ураження;

– нанесення збитків спорудам, культурним об'єктам, інфраструктурі та транспортним засобам;

– транспортування заборонених предметів або їх скидання на охоронювану територію;

– перешкоджання повітряному руху в аеропортах;

– передача повідомлень у радіочутливих областях.

Функціональна структура безпілотних апаратів представлена на рисунку 1.2 і включає шість взаємозалежних систем: модулі збору даних, AHRS, NAV, управління, реєстрації даних і телеметрії [30, 31, 40]. Модуль зв'язку охоплює всі вхідні/вихідні сигнали, інтегруючись у всі модулі функціональної структури безпілотних апаратів.

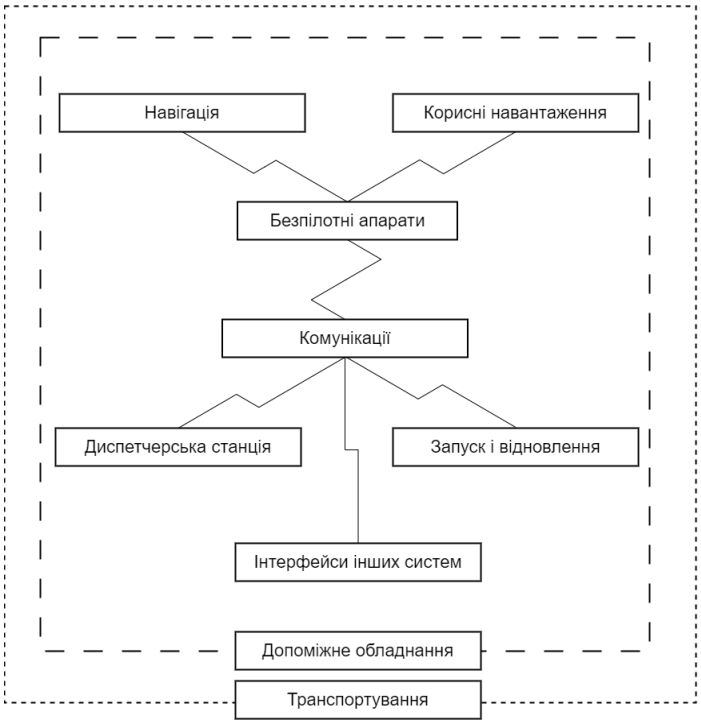


Рисунок 1.2 – Функціональна структура системи безпілотних апаратів

Компоненти безпілотної системи використовують бездротові канали зв’язку (КЗ) для взаємодії, а наземні станції управління (GCS) поділяються на локальні і штабні варіанти. Переносні пункти управління, такі як КПК, смартфони та захищені ноутбуки, належать до підкласу локальних пунктів.

Існує значна різниця між різними КЗ з точки зору безпеки [30, 31, 36, 42]. Зв'язок між супутником і безпілотний апарат – це радіозв'язок LOS, у той час як зв'язки, наприклад, БПЛА-БПЛА, КПК-БПЛА і локальної ГКС-БПЛА можуть використовувати радіо чи GPRS/EDGE.

Дослідження показують, що мережі Wi-Fi уразливі до атак, що можуть бути використані для злому мереж безпілотних апаратів [30, 31, 43]. Різні КЗ, такі як супутник і штабна ГКС, можуть мати певні загрози, але можуть бути менш вразливими завдяки існуючим заходам безпеки [44, 45]. Урахування вимог до безпеки для кожного КЗ є ключовим.

Залежно від завдань, на безпілотні апарати можуть встановлюватися різноманітні системи та пристрої [23], такі як засоби розвідки, радіоелектронні перешкоди, засоби управління озброєнням, автономна апаратура польоту та інше.

1.1.2 Сучасні мережеві технології для безпілотних апаратів

Сучасні мережеві технології в Інтернет речах (IoT) та технології розумного міста дозволяють організувати надійну та безпечну інфраструктуру зв'язку для забезпечення ефективного функціонування. В даний час існують різні мережеві технології, які широко застосовуються у розгортанні розумних міст, і серед них виділяються 5G, Wi-Fi 6 та оптоволоконні мережі [46, 47].

Вибір мереж для розумних міст обумовлюється їх високим рівнем безпеки, який є критичним аспектом, враховуючи обробку значної кількості даних та взаємодію із пристроями IoT. Концепція розумного міста, як запропоновано в [47], акцентує увагу на розвитку технологій, виокремлюючи роль інфраструктури зв'язку, де 5G та Wi-Fi 6 використовуються для бездротового сегмента, а оптоволоконне застосовується для провідного [47].

У контексті розумних міст безпілотні апарати відіграють ключову роль у наданні цінної інформації та підтримці безпеки в різних підсистемах, таких як моніторинг транспорту та дорожнього руху, забезпечення безпеки міста через аерофотозйомку та відеоспостереження, а також виявлення та запобігання надзвичайним ситуаціям [48, 49].

Wi-Fi – один із найпоширеніших типів безпроводових мереж, базований на стандарті IEEE 802.11. Використовується для передачі великих обсягів даних на великі відстані з високою швидкістю. Дозволяє безпілотним апаратам передавати відео, зображення та дані сенсорів, а також забезпечує реальний час для відеозв'язку між оператором та апаратом [46, 47].

Bluetooth – ще один поширений тип безпроводових мереж для підключення безпілотних апаратів до інших пристроїв, таких як смартфони чи планшети. Забезпечує надійний зв'язок на короткій відстані для передачі даних, команд та звукового сигналу [48, 49].

Zigbee – технологія для комунікації між безпілотними апаратами, працює на низькій потужності та дозволяє підключати багато апаратів до однієї мережі.

Ефективно використовується в місцях з великою кількістю апаратів, таких як фабрики чи склади [46, 47].

LTE (Long-Term Evolution) – стандарт мобільного зв'язку для передачі даних на великі відстані з високою швидкістю. Використовується для забезпечення зв'язку між безпілотним апаратом та оператором через мобільну мережу, передаючи великі обсяги важливих даних [46, 47].

NB-IoT (Narrowband Internet of Things) – стандарт мережі Інтернет речей для зв'язку з низькою швидкістю передачі даних. Використовується в апаратах з низьким споживанням енергії та довгим терміном служби батареї для передачі даних сенсорів та вимірювань [48, 49].

Один із ключових проривів XXI століття - це розробка та широке використання безпілотних літальних мереж. Раніше літаючі мережі існували як цільові мережі, що літають, або FANET. Останнє десятиліття було присвячене численним дослідженням у цій сфері вітчизняними та зарубіжними вченими [50-59]. Ці дослідження стосувалися загальних принципів FANET [59, 60], використання безпілотних літальних апаратів для пошуку мети [50], спеціалізованого використання сенсорів у військових цілях [54], маршрутизації мереж FANET [61], поведінки головних вузлів у тривимірному просторі [62, 63] та використання БПЛА для позиціонування [52]. Однак, робота [54] відображає вдосконалювання бездротової сенсорної мережі у військових операціях за допомогою спеціалізованих БПЛА.

Польоти за межами прямої видимості відкривають великий потенціал для БПЛА, але їх реалізації стискається с такими перешкодами [60].

1. Регулювання: авіаційне регулювання не враховує особливості польотів БПЛА, що ускладнює їх економічне використання або робить його неможливим.

2. Інфраструктура:

– засоби керування польотами: мобільні мережі, супутникове зв’язку, прямий канал;

– системи управління трафіком;

– віддалена ідентифікація;

– станції зарядки, розвантаження, зльоту та посадки.

3. Технології БПЛА:

– ефективні джерела енергії;

– сенсори для автономного польоту і ухилення від зіткнення;

– оптимізація гвинтів та двигунів для зниження шуму і підвищення стійкості;

– системи безпеки під час непередбачуваних ситуацій.

Згідно проведеним аналізам вчених, де для будування літаючої мережі використовували флоти БПЛА загального користування [65-74], було виявлено, що такий підхід розглядає створення нового класу мереж, які частина мережі зв'язку за межами видимості та реалізують концепцію Інтернету речей.

В контексті розвитку літаючої сенсорної мережі, взаємодія наземного та літаючого сегментів створює нові можливості для вдосконалення наземного сегмента через застосування БПЛА у системі VANET (Vehicular Ad Hoc Networks). Основний акцент з використання літаючих сенсорних мереж полягає в тому, що треба спрямувати та вдосконалити характеристики наземного сегмента, як станцій та центрів зв’язку через інтеграцію можливостей літаючого сегмента. Дана проблематика враховує чотири основних факти:

1. Регулювання у сфері пілотованої авіації, хоча й сприяє обмеженому використанню БПЛА, залишає частину питань у "сірій" зоні [64].

2. Понад 60% потенціалу БПЛА використовується у польотах поза прямою видимістю, що вимагає координації польоту та отримання дозволів на використання повітряного простору [74].

3. Розвиток бортових технологій та прогрес у регулюванні сприяють зростанню інвестицій у цю сферу [75].

4. Українські виробники БПЛА мають світовий потенціал, однак через численні обмеження часто спрямовуються на зарубіжні ринки [76].

1.1.3 Групове застосування безпілотних апаратів

Застосування безпілотних апаратів в різних сферах, таких як наземне, повітряне та морське середовище, широко розповсюджене. Наземні апарати використовуються для розвідки, моніторингу дорожнього руху, безпеки, навігації та автоматизації сільськогосподарських робіт і будівельних процесів. У повітряній сфері вони використовуються для зондування атмосфери, моніторингу погодних умов, аерофотозйомки, пошуково-рятувальних операцій та військових цілей. У морському середовищі вони використовуються для моніторингу морських біоресурсів, дослідження дна, контролю за дотриманням міжнародних морських норм, пошуково-рятувальних операцій та навігаційної підтримки для суден. Використання таких апаратів сприяє підвищенню ефективності та безпеки, зменшенню витрат і ризиків для людей, а також забезпечує доступ до інформації та можливостей, раніше недоступних через обмеження часу, простору або складності у віддалених чи небезпечних умовах.

Групове застосування безпілотних літальних апаратів (БПЛА) розглядається на прикладі їх формування в польоті, де вони можуть бути координовані або співпрацювати між собою з метою виконання повітряних завдань [61]. Координація передбачає взаємозв'язок між завданнями та синхронізацію в їх виконанні, тоді як співпраця вимагає міцної просторово-часової координації між різними БПЛА [71]. Утворення флоту може приймати різні геометрії формувань у повітрі, наприклад, V- або ромбовидні, з керівником, який визначає траєкторію, а його послідовники забезпечують відстань між собою, дотримуючись геометрії формування.

Групове застосування БПЛА включає розподіл робочих завдань на всю команду, зменшуючи витрати на місію за рахунок менших апаратів та забезпечуючи більшу відмовостійкість і гнучкість, завдяки можливості реконфігурації у разі відмови окремих транспортних засобів [35]. Однак недоліки утворення флоту полягають у вразливості до апаратних збоїв у відносно малих просторах з високою швидкістю, що може призвести до втрати синхронізації з командою та загрозити загальній комунікації [71]. Таким чином, групове

застосування БПЛА є ефективною стратегією для підвищення їхньої продуктивності та ефективності виконання завдань, забезпечуючи більшу надійність та гнучкість у різних умовах використання.

Дослідження з вдосконалення технології використання груп БПЛА проводяться за допомогою математичних моделей та натурних макетів, включаючи натурні експерименти [77] в модельних умовах [78] та реальних бойових сценаріях [79, 80]. Групи БПЛА за принципом побудови бойового порядку можуть бути [23,24]:

– упорядкованими (зграя, рій): бойовий порядок формується за допомогою алгоритму управління групою всередині групи або за командами з наземного/повітряного пункту управління;

– невпорядкованими: бойовий порядок визначається послідовністю старту БПЛА та індивідуальними алгоритмами функціонування та програмою польоту кожного апарату.

Упорядковані групи можуть бути [23,24]:

– автономними – після старту реалізують свій (заданий при старті або формований у процесі польоту) алгоритм функціонування

– пов'язаними – після старту реалізується алгоритм, який формується та контролюється ззовні – з наземного/повітряного ПУ.

За бойовим складом групи БПЛА можуть бути [23,24]:

– однорідними: до складу групи входять БПЛА одного типу та однакового функціонального призначення;

– неоднорідними: до складу групи входять БПЛА різного типу та функціонального призначення.

За бойовою спеціалізацією групи БПЛА можуть бути [23,24]:

– цільовими: ударні, розвідувальні, винищувальні тощо;

– багатоцільовими: розвідувально-ударними, винищувально-ударними.

Основними об'єктами для реалізації технології групового застосування можуть бути (за хронологією та доцільністю розвитку) [23,24]:

– малорозмірні БПЛА різного призначення: розвідувальні, ударні, постановники перешкод, що імітують тощо;

– ударні авіаційні засоби типу плануючих авіаційних бомб та крилатих ракет;

– перспективні автономні БПЛА різного призначення.

За рахунок високої автономії та різноманітності безпілотних апаратів, включаючи БПЛА, їхній функціональний потенціал значно зростає, що призводить до складнішого функціонування. Прогнозується розвиток автономних груп з різноманітними цілями, включаючи можливе поєднання з пілотованими апаратами. Однак обмеження управління людиною, зумовлене фізіологічними обмеженнями, такими як обмежена кількість контрольованих параметрів та швидкість реакції, є значною проблемою. Це може призвести до виключення людини з інтермедіарних етапів управління групою безпілотних апаратів, зберігаючи лише функцію прийняття рішень та формування програм автономних дій для виконання оперативних завдань.

У науковій літературі представлені різні стратегії управління формуванням флоту, наприкладі БПЛА [39, 40, 81]. Зокрема:

– Стратегія лідера-послідовника (Leader-follower) є широко використовуваною для систем з кількома БПЛА, де товариші по команді слідують за лідером [78]. Лідер приймає рішення щодо траєкторії місії, а інші апарати підпорядковані йому. Проте головною проблемою є ризик для всієї місії у випадку втрати або недоліку функціонування лідера.

– Віртуальний лідер передбачає заміну реального лідера на віртуального, де всі апарати отримують траєкторію, аналогічну траєкторії віртуального лідера. Це зменшує автономність, але збільшує ризик зіткнень між БПЛА [82, 83].

– Поведінковий підхід (децентралізований) передбачає дотримання кожним апаратом певних правил для виконання групової поведінки. Ці правила, натхнені правилами Рейнольдса щодо колективного переміщення тварин [23, 84, 35, 25], включають уникнення зіткнень, узгодження швидкості та центрування флоту. Така

структура є самоорганізованою, оскільки кожен апарат повинен дотримуватися правил і знати об’єктивну траєкторію.

1.1.4 Висновки стосовно фізичних і кіберактивів безпілотних апаратів

На основі проведеного аналізу технологій розробки та використання систем безпілотних апаратів визначено ряд ключових висновків, які стосуються їх фізичних та кіберзагроз.

1. По-перше, визначено, що функціонування безпілотних апаратів тісно пов'язане із сучасними мережевими технологіями, що відкриває нові можливості для їх групового використання. Враховуючи це, висвітлено необхідність удосконалення методів захисту від кіберзагроз, оскільки групове застосування може збільшити ризики з боку кібератак.

2. По-друге, зазначено, що потенціал та загрози, пов'язані з фізичними та кіберактивами безпілотних апаратів, потребують детального вивчення та оцінки. Виділено важливість розробки та вдосконалення математичних моделей та методів оцінювання кібербезпеки для забезпечення ефективності та надійності цих систем.

3. По-третє, робота вказує на необхідність обґрунтування та вибору показників оцінки кібербезпеки флотів безпілотних апаратів. Це робить акцент на важливості розроблення систематизованих та стандартизованих методів оцінки, які враховують усі аспекти фізичних та кіберактивів.

1.2 Аналіз БПЛА, як об’єктів кібербезпеки

Технології спрямовані на подолання бар'єрів та збереження життя. Беспілотні літальні апарати (БПЛА) відіграють ключову роль у цьому. Вони використовуються для виконання завдань, які можуть загрожувати здоров'ю та життю людини. Також їх використання розширює можливості виконання складних та важкодоступних операцій, які виходять за межі людських можливостей. БПЛА

все частіше використовуються не як окремі одиниці, а як частина організованих груп, які можна назвати флотами [64].

В літературі можна знайти багато академічних досліджень з цією метою. Наприклад, Аріансья і співавт. (2018) [74] представляють контроль та забезпечення безпеки критичної інфраструктури; Фалорка, і співавт.(2021) [75] розглядають візуальний огляд будинків і споруд; Мадемліс і співавт.(2019) [76] обговорюють використання БПЛА в кіно- та рекламній індустрії. Міроненко Микита Ігорович у своїй дисертації розглядає моделі та методи інформаційної технології машинного навчання для автономного БПЛА, спрямованого на відеомоніторинг місцевості [85]. Монографія Бондара та інших авторів розглядає застосування безпілотних авіаційних систем у цивільному захисті [86]. Дисертація Бережного Андрія Олександровича аналізує методи та інформаційні технології, які застосовуються для автоматизованого планування маршрутів польотів БПЛА з метою підвищення ефективності пошуку об'єктів [87]. У монографії "Internet of Drones: AI Applications for Smart Solutions" автори обговорюють застосування штучного інтелекту для створення інноваційних рішень у галузі БПЛА та їх інтеграції до "Інтернету речей" [88]. Робота Hu F. "UAV Swarm Networks: Models Protocols and Systems" охоплює моделі, протоколи та системи управління зграй БПЛА, що є актуальною темою у сучасних дослідженнях [89]. У роботі "Internet of Drones" автори Krishnan S. та Murugappan M. досліджують актуальні аспекти застосування концепції Інтернету речей (IoT) у галузі безпілотних літальних апаратів (БПЛА). Вони звертають увагу на різні аспекти інтеграції БПЛА в Інтернеті речей, включаючи проблеми пов'язані з мережевою архітектурою, протоколами передачі даних, безпекою та управлінням ресурсами [90].

1.2.1 Потенціал та загрози БПЛА

Зі збільшенням використання БПЛА зростає занепокоєння питаннями їхньої безпеки та захисту. Потенційні ризики включають зіткнення, втручання в роботу інших повітряних засобів та кібератаки, які можуть призвести до витоку даних або

несанкціонованого управління БПЛА. Ці питання спровокували сплеск наукових досліджень з безпеки та захисту БПЛА.

Флот БПЛА - це група безпілотних літальних апаратів або літаючих роботів, які працюють над повідомленням для досягнення певної мети [64]. Флоти БПЛА мають кілька переваг перед одиночними БПЛА. Вся система є гнучкою, тому вихід з ладу або втрата одного БПЛА не впливає на працездатність всієї системи. Гнучкість флоту БПЛА значно підвищується завдяки динамічній адаптації різних стилів і стандартів конфігурації. Зв'язок відіграє важливу роль в управлінні та координації флоту БПЛА. Архітектура зв'язку описує, як відбувається обмін даними між БПЛА або між БПЛА і центральним центром управління. З розвитком технологій флоту БПЛА однією з головних проблем є відстеження безпілотників у відкритому просторі і моніторинг їх стану в просторовому і часовому аспектах.

У світі передової робототехніки очікується, що це дозволить подолати обмеження одиночних роботів і дасть можливість великим групам працювати разом. Це надихається поведінкою тварин, де створення і результат об'єднують зусилля для досягнення складних цілей. Залежно від парадигми застосування, повноцінний і легко масштабований флот БПЛА - це сукупність БПЛА, кількість яких може бути збільшена або зменшена [42]. Вартість виробництва безпілотних літальних апаратів дешевшає, БПЛА стають все більш доступними, а використання цієї технології продовжує розвиватися, що створює різні дослідницькі виклики БПЛА використовуватися в різних сферах, включаючи сільське господарство, військові рятувальні операції, управління ланцюгами поставок, управління запасами, аварійно-рятувальні операції та спостереження [91,92].

Однією з перших робіт у галузі безпеки БПЛА було опубліковано в [93,44]. У ній представлено огляд викликів та проблем у забезпеченні безпеки БПЛА, включаючи потребу у захищеному зв'язку, зберіганні даних та прийнятті критичних рішень щодо місії.

В [45] були виділені проблеми безпеки та конфіденційності у зв'язку БПЛА в літаючих безладних мережах, представлений широкий огляд існуючих механізмів безпеки, включаючи автентифікацію, конфіденційність, цілісність та доступність

даних, та виявлено обмеження цих механізмів. Аналогічно, автори [94] представили огляд існуючих досліджень з безпеки БПЛА, включаючи різні види атак, уразливості та методи захисту. Вони наголосили на важливості забезпечення безпеки БПЛА від кібератак, таких як перешкоди, прослуховування та підробка.

В останні роки дослідники активно вивчають питання безпеки БПЛА у хмарних середовищах. У [95,96] обговорюються проблеми та загрози безпеці для БПЛА у хмарних середовищах, представлено огляд сучасних рішень для вирішення цих проблем та виявлено перспективи майбутніх досліджень.

Під час стихійних лих, таких як повені, пожежі, землетруси і похорони, доступ до районів ускладняється, а рятувальні операції затримуються [97,98]. Застосування БПЛА у рятувальних операціях може ефективно прискорити їх проведення, надаючи можливість проведення оцінки масштабних катастроф та пошуку вцілілих. Флот БПЛА може стати важливим інструментом для встановлення тимчасових зв'язкових каналів у постраждалих районах [99].

Дистанційне керування флотами БПЛА зазвичай реалізується через наземні станції, які можуть бути реалізовані за допомогою смартфонів, підключених до мобільних мереж. З точки зору безпеки, варто враховувати, що флоти БПЛА стають об'єктом потенційних кібератак, що може призвести до серйозних наслідків, включаючи збитки [46]. Виявлення та запобігання таким атакам є критичним для забезпечення безпеки та ефективності флотів БПЛА.

Нові технології, такі як БПЛА, мають свої переваги, такі як екологічне усвідомлення, висока продуктивність та підтримка моніторингу і безпеки, але вони також супроводжуються недоліками, такими як енергетичні витрати, обмеження дальності польоту і труднощі в управлінні [47].

1.2.2 Визначення загроз для безпеки каналів управління БПЛА

Українське законодавство регулює використання БПЛА через низку нормативних актів, які встановлюють вимоги до кваліфікації операторів, обмеження місць польотів, технічного стану БПЛА та умов їх використання [100].

Нормативним документом, який регулює цю сферу, є "Про затвердження Змін до Правил інженерно-авіаційного забезпечення державної авіації України" [101], який містить загальні вимоги та процедури отримання дозволів на застосування БПЛА.

У додаток до основного нормативного акта, існують стандарти та закони, які можуть використовуватися під час застосування БПЛА, такі як "Про затвердження Правил технічної експлуатації безпілотних авіаційних комплексів І класу державної авіації України" [101], "Техніка авіаційна державної авіації. Апарати літальні безпілотні. Основні терміни та визначення понять. Класифікація" [102] та інші правові норми, що регулюють використання повітряного простору безпілотними повітряними суднами [103, 104, 105, 106].

Використання БПЛА в Україні підкоряється міжнародним стандартам та рекомендаціям, таким як Міжнародні стандарти цивільної авіації (ICAO) [107] і рекомендації Європейського агентства авіаційної безпеки (EASA) [108].

На даний момент в Україні відсутні будь-які вимоги або стандарти щодо систем управління середніми та важкими БПЛА. У зв'язку з цим, для синтезу системи управління застосовується система стандартів НАТО, а їх схема визначена в цій роботі [109].

БПЛА складається з трьох основних елементів: системи польоту, цільового навантаження та системи управління. Аналізуючи здатність зовнішніх факторів до взаємодії з іншими компонентами через бездротову лінію зв'язку, приділено увагу можливості впливу на систему управління і цільове навантаження.

Оцінюючи схему зв'язку системи управління, можна виділити три вектори впливу: центр управління, сам БПЛА та радіоканал. Вплив на центр управління може здійснюватися з боку зовнішніх мереж передавання даних через обхід захисту та шкідливі дії, такі як впровадження програмних закладок або переспрямування трафіку.

Переваги цього підходу полягають у повному контролі над БПЛА оператором та можливості впливу на компоненти системи управління. Однак, недоліками є потреба у висококваліфікованих фахівцях для втручання в

управління, необхідність конфіденційної інформації та несправедливість результатів через багато факторів, які впливають на цю взаємодію.

Другим аспектом взаємодії в центрі управління безпілотними літальними апаратами (БПЛА) є можливість надсилання оператору неправдивої інформації щодо стану БПЛА та його положення у просторі через канали передачі даних та команд. Ця атака може включати підміну трафіку, спрямованого на вхідні пристрої управління, надсилання неправдивої телеметрії та даних про стан БПЛА з метою впливу на рішення оператора та викликання певних реакцій.

Переваги цього підходу включають його відносно просту реалізацію, здатність спровокувати оператора на певні дії, необхідні для атаки, і можливість спричинити збій у виконанні польотних завдань. Однак існують певні недоліки, такі як обмеженість в зоні радіовидимості антен апаратури, неповний контроль над БПЛА, залежність від досвіду оператора та складність реалізації атаки через аналіз протоколів зв'язку. Крім того, захист каналів передачі даних може знизити ефективність таких атак.

У контексті того, що системи управління БПЛА були спроектовані з фокусом на їхню надійність та продуктивність, питання безпеки управління БПЛА залишалося на другому плані. Проте, зі зростанням застосування БПЛА та їх використання для незаконних цілей, питання безпеки управління набуває важливості.

В результаті проведеного аналізу було виявлено перелік векторів впливу на систему управління БПЛА, які можуть стати об'єктом зловмисних дій. Цей перелік представлений в таблиці 1.1. До основних векторів впливу на систему управління БПЛА відносяться перешкоджання зв'язку між земною станцією та БПЛА, вплив на датчики апарату з метою їх збоїв або випадкових вимірювань, введення шумів в систему передачі даних, а також атаки на програмне забезпечення БПЛА.

Таблиця № 1.1 – Вектори впливу на систему управління БПЛА

Вектор впливу	Переваги	Недоліки
1	2	3
Впливи на центр управління БПЛА з боку зовнішніх мереж.	1 Повний контроль над БПЛА з функціоналом оператора. 2. Імовірнісна можливість впливу на інші підпорядковані центру управління польотом БПЛА складові частини системи управління.	1. Складна реалізація, автоматизація. 2. Необхідна велика кількість знань конфіденційного характеру. 3. Необхідний доступ до зовнішніх мереж передачі даних, які мають з'єднання з мережами технічного обслуговування БПЛА. 4.Результат взаємодії не визначений, тому що на нього впливає багато ймовірнісних чинників.
Нав'язування оператору БПЛА неправдивої інформації через апаратуру приймання передачі команд і відправки телеметрії	1. Порівняно нескладна реалізація. 2. Можливість спровокувати оператора на дії, необхідні атакуючому. 3. Існує ймовірність здійснити збій польотного завдання.	1 Необхідно перебувати в прямій радіовидимості антен апаратури приймання-передавання даних центру управління польотів. 2 Немає повного контролю над БПЛА. 3. Реалізація впливу і його наслідки сильно залежать від досвіду оператора. 4. Необхідне знання використовуваних протоколів зв'язку. 5. У разі застосування в каналі СКЗІ (імітовставка або шифрування), вплив стає неможливим.
Вплив на приймально-передавальний тракт системи управління БПЛА	1.Повний контроль над БПЛА з функціоналом оператора.	1. Необхідне знання використовуваних протоколів зв'язку. 2. У разі застосування в каналі СКЗІ (імітовставка або шифрування), вплив стає неможливим. 3. Деякі системи зв'язку можуть бути несприйнятливими до цього виду атаки.

Продовження таблиці 1.1.

1	2	3
Вплив на цільове навантаження	1. Може призвести до зриву польотного завдання.	1. Не може або дуже рідко може призвести до захоплення управління БПЛА. 2 У разі застосування в каналі СКЗІ, вплив стає неможливим.
Вплив на систему просторового позиціонування БПЛА	1 Може призвести до часткового або повного захоплення управління. 2.Легка реалізація. 3.Вплив погано виявляється з боку оператора. 4. Для протидії необхідна розробка нових захищених виробів.	1.Потрібна попередня розвідка апаратури просторового позиціонування. 2. Необхідно мати велику кількість різного обладнання.
Вплив на радіоканал	1.Можливість здійснення повного контролю над БПЛА. 2. можливість здійснення спостереження за дією БПЛА без відома оператора. 3.Контроль усіх показників телеметрії БПЛА.	1.Складна реалізація, автоматизація; 2. у разі застосування в каналі СКЗІ (імітовставка або шифрування), вплив стає неможливим. 3. необхідні знання використовуваних протоколів зв'язку і системи управління БПЛА.

1.3 Аналіз математичних моделей та методів оцінювання та забезпечення кібербезпеки БПЛА

Математична модель в інформаційній безпеці — це опис сценаріїв у вигляді послідовності дій порушників та відповідних заходів у відповідь. Наближення таких моделей описують процеси взаємодії порушника із системою захисту та можливі результати дій [110].

Методи оцінки та забезпечення кібербезпеки БПЛА включають різноманітні теоретичні підходи, призначені для аналізу уразливостей та розробки відповідних заходів захисту.

1.3.1 Методи оцінювання та забезпечування кібербезпеки БПЛА та флотів

У процесі проектування складних систем, таких як комплексні та інтегровані засоби кіберзахисту СБФ БПЛА, у більшості випадків вдаються до моделювання основних процесів, що відбуваються всередині інформаційної системи та на стику «середовище – система» [111]. Крім того, моделі можуть використовуватися для проведення моніторингу та аудиту безпеки на етапах експлуатації та супроводу систем. Основу моделей оцінки та забезпечення безпеки інформації становлять такі теорії:

- формально-евристичний підхід;
- теорія ймовірностей та випадкових процесів;
- еволюційне моделювання;
- теорія графів, автоматів та мереж Петрі;
- теорія нечітких множин;
- ентропійний підхід.

Формально-евристичний підхід передбачає застосування формальних моделей та евристичних методів з метою оцінки рівня безпеки. Його переваги включають відносну простоту та застосовність до різних типів систем, проте він часто обмежений точністю моделей і може упустити деякі загрози через недостатній облік контексту [111].

Теорія ймовірностей і випадкових процесів використовується для аналізу ймовірностей виникнення кібератак та ефективності заходів захисту. Її переваги включають математичну точність та здатність враховувати випадкові фактори. Однак вона може вимагати великого обсягу даних для досягнення достовірних результатів і не завжди може враховувати складні взаємодії в системі [112].

Еволюційне моделювання дозволяє аналізувати динаміку розвитку кіберзагроз та ефективність адаптації систем захисту. Його переваги включають здатність враховувати умови середовища, що змінюються, і противників. Однак, складність моделей та обчислювальні витрати можуть бути значними [112].

Теорія графів, автоматів та мереж Петрі дозволяє моделювати структуру системи та її поведінку в контексті кібератак. Переваги включають інтуїтивну наочність та здатність аналізувати потенційні вразливості. Однак вона може зіткнутися з обмеженнями в адаптації до складних і динамічних систем[111].

Теорія нечітких множин застосовується для врахування невизначеності та розмитості в даних про кіберзагрози та рішення щодо забезпечення безпеки. Її переваги включають здатність враховувати нечіткість у реальних ситуаціях. Проте, інтерпретація та застосування нечітких правил можуть бути суб'єктивними та вимагати великого обсягу експертних знань [112].

Ентропійний підхід використовується для аналізу невизначеності у системах та оцінки їх складності. Його переваги включають здатність оцінювати рівень хаосу та випадковості в системі. Однак він може бути обмежений в адаптації до конкретних контекстів і вимагати точного визначення параметрів [111].

Відмінності більшості моделей полягають у тому, які параметри вони використовують як вхідні, а які представляють у вигляді вихідних після проведення розрахунків. Крім того, останнім часом широкого поширення набувають методи моделювання, засновані на неформальній теорії систем: методи структурування, методи оцінювання та методи пошуку оптимальних рішень [111,112].

Отже, хоча перераховані вище методи мають свої переваги, жоден з них не забезпечує повноцінний захист від кіберзагроз для систем безпілотних літальних апаратів. Тому подальшим кроком у розвитку досліджень є розробка та покращення методів забезпечення кібербезпеки з метою забезпечення більш ефективного захисту для систем безпілотних літальних апаратів.

1.3.2 Обґрунтування та вибір показників оцінки кібербезпеки флотів БПЛА

Обґрунтування та вибір показників оцінки кібербезпеки флотів безпілотних літальних апаратів (БПЛА) є ключовим етапом в забезпеченні ефективної захисту від потенційних кібератак. У даній роботі, враховуючи специфіку сучасних кіберзагроз та потреби в адаптованих методиках оцінки, були обрані наступні показники: ймовірність, тяжкість, вартість та ризик.

Показник ймовірності відображає можливість виникнення кібератаки на флот БПЛА. Враховуючи широкий спектр потенційних загроз, оцінка ймовірності дозволяє визначити, наскільки великою є ймовірність реалізації конкретного виду атаки та її можливі наслідки для безпеки системи.

Тяжкість кібератаки визначає масштаб та наслідки інциденту для флоту БПЛА. Цей показник включає в себе оцінку ступеня пошкодження, можливості відновлення та вплив на операційну діяльність. Врахування тяжкості кібератаки дозволяє здійснювати прогнозування втрат та приймати ефективні заходи протидії.

Вартість кібербезпеки відображає фінансові та ресурсні затрати, пов'язані з захистом флоту БПЛА від кібератак. Цей показник включає в себе витрати на розробку та впровадження заходів безпеки, витрати на відновлення систем та можливі втрати від перерв у роботі.

Ризик є комплексним показником, який враховує ймовірність та тяжкість кібератаки разом із вартістю заходів безпеки. Цей показник дозволяє оцінити загальний рівень загрози для флоту БПЛА та визначити стратегії мінімізації ризиків.

Обрані показники відображають комплексний підхід до оцінки кібербезпеки флотів БПЛА, забезпечуючи аналітичну основу для прийняття обгрунтованих рішень щодо захисту від потенційних кіберзагроз. Врахування ймовірності, тяжкості, вартості та ризику дозволить ефективно управляти кібербезпекою та забезпечити безпеку та надійність флотів БПЛА.

1.4 Постановка науково-прикладної задачі та обґрунтування методики дослідження

Результати проведеного аналізу нормативної бази, моделей, методів оцінювання та забезпечення кібербезпеки системи багатофункційних флотів безпілотних апаратів показали, що необхідно розвивати моделі, методи та інструментальні засоби підвищення кібербезпеки такого роду систем.

1.4.1 Загальна та часткові задачі дослідження

Таким чином, загальним науковим завданням дисертаційного дослідження є розроблення моделей, методів і засобів аналізу та забезпечення кібербезпеки систем багатофункційних флотів БПЛА в умовах одиничних і комбінованих атак.

Існують БПЛА та системи БФ БПЛА.

Необхідно розробити математичні моделі та методи оцінювання і забезпечення кібербезпеки систем багатофункційних флотів БПЛА.

Рішення загального завдання включає ряд часткових наукових і прикладних завдань, які необхідно вирішити, а саме:

1. Аналіз функцій, технологій та методів для оцінювання та забезпечення кібербезпеки систем безпілотних апаратів. Обґрунтування мети, задач та методики досліджень.

2. Розроблення концептуальної та математичних моделей кіберфізичної системи багатофункційних флотів безпілотних апаратів як об’єкта оцінювання кібербезпеки.

3. Розроблення методу аналізу кіберзагроз, наслідків та критичності одиничних і комбінованих атак на активи кіберфізичної системи багатофункційних флотів безпілотних апаратів.

4. Удосконалення метод вибору сукупності контрзаходів для забезпечення кібербезпеки кіберфізичної системи багатофункційних флотів безпілотних апаратів.

5. Розроблення алгоритмів, програмних засобів та інформаційної технології для проведення аналізу кібербезпеки системи багатофункційних флотів безпілотних апаратів.

6. Впровадження запропонованих методів і засобів в державних та міжнародних науково-дослідних проектах і навчальному процесі кафедри, а також при обґрунтуванні вимог до безпеки систем безпілотних апаратів.

1.4.2 Етапи та методика дослідження

Сформулюємо основні етапи і методику досліджень, результати яких викладені в розділах 2, 3 та 4. Методика досліджень ґрунтується на застосуванні системного підходу до постановки та рішення загальної і часткових завдань дисертаційного дослідження, вибору математичного апарату, використовуваних моделей та методів дослідження, а також програмних засобів для реалізації інформаційної технології.

Методика досліджень розробляється виходячи з вимог до логіки та послідовності рішення поставлених завдань і адекватності обраного математичного апарату та складається з ряду основних етапів. На рис. 1.3 наведена запропонована в дисертаційній роботі методика досліджень, означені основні етапи, показані взаємозв’язки з отриманими результатами.

На першому етапі необхідно провести аналіз існуючої нормативної бази регламентуючих документів щодо кібербезпеки БПЛА, загальні положення щодо захисту інформації в системах від несанкціонованого доступу, критерій оцінки захищеності інформації в системах від несанкціонованого доступу, визначити особливості побудови і функціонування такого роду систем. Особлива увага приділяється аналізу моделей, методів, процедур і підходів до оцінювання і забезпечення кібербезпеки СБФ БПЛА та самих БПЛА у системі.

На другому етапі розроблюється комплекс моделей оцінювання кібербезпеки, які включають в себе концептуально-ієрархічну модель структури СБФ БПЛА та теоретико-множинні моделі, які враховують в себе поведінки

порушника, загроз, вразливості і кібератаки на окремі компоненти інфраструктури БПЛА.

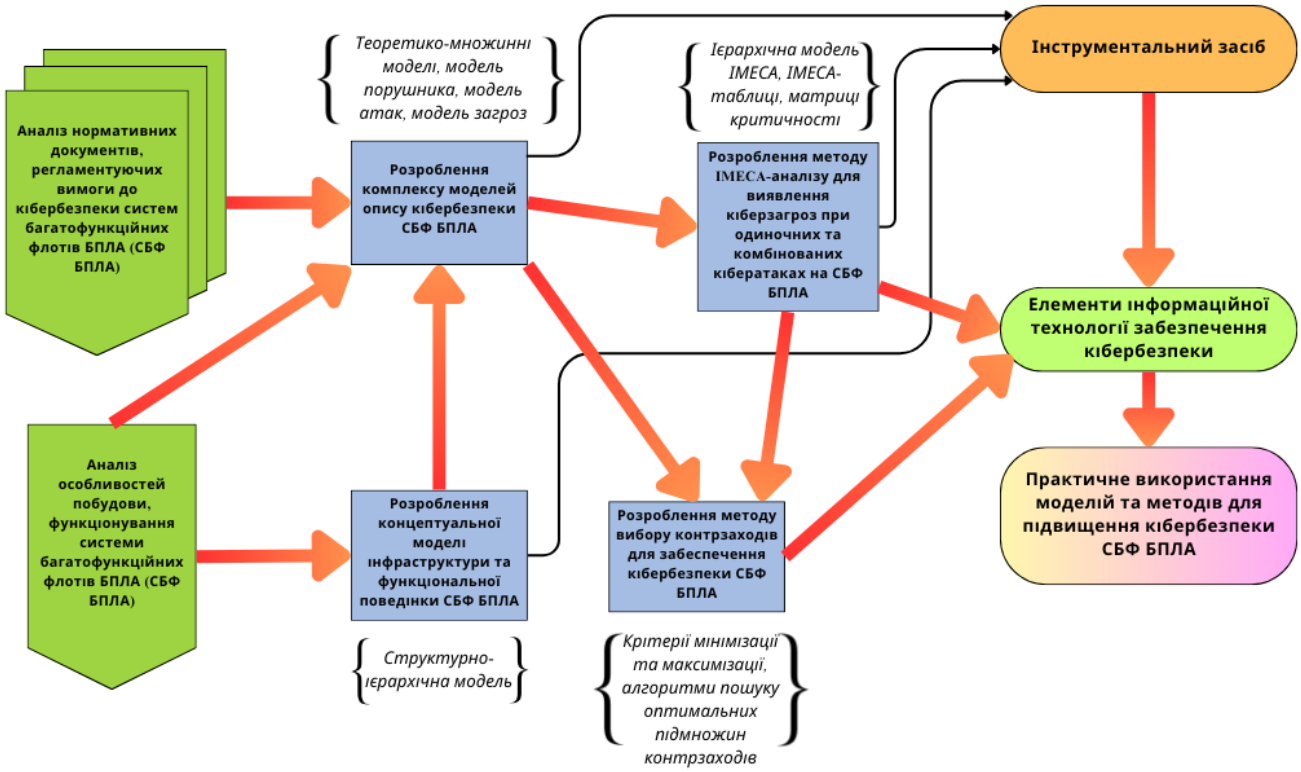


Рисунок 1.3 – Методика дисертаційного дослідження

На третьому етапі вдосконалюється метод забезпечення кібербезпеки СБФ БПЛА на основі IMECA-аналізу для виявлення кіберзагроз при одиночних та комбінованих атаках.

На четвертому етапі розроблюється метод вибору контрзаходів для забезпечення кібрбезпеки СБФ БПЛА, а також визначення критеріїв для їх оцінювання.

Завершальним етапом є розробка інструментального засобу для оцінювання та забезпечення кібербезпеки СБФ БПЛА, а також для об’єднання розроблених моделей оцінювання кібербезпеки, теоретико-множинні моделі та IMECA-аналіз для виявлення кіберзагроз при одиночних та комбінованих атаках, методу вибору контрзаходів в єдину інформаційну технологію оцінювання і забезпечення гарантоздатності кібербезпеки СБФ БПЛА.

1.5 Висновки до першого розділу

На основі аналізу першого розділу можна зробити наступні висновки:

1. Безпілотні апарати в сучасному світі відіграють важливу роль у різних сферах, включаючи комерційний, військовий та науковий сегменти. Вони відрізняються високою автономією та різноманітністю функцій, що призводить до необхідності складного функціонування та високої кібербезпеки.

2. Технології розробки та використання БА включають в себе різноманітні аспекти, такі як класифікація, мережеві технології, групове застосування та фізичні та кіберактиви. Ретельний аналіз цих аспектів дозволяє зрозуміти потенціал та загрози, які вони можуть становити для кібербезпеки.

3. БА є об’єктом підвищеної уваги в контексті кібербезпеки через їхню значущість та потенційну вразливість перед кібератаками. Визначення загроз для безпеки каналів управління є ключовим аспектом цього аналізу.

4. Математичні моделі та методи оцінювання кібербезпеки БПЛА включають різноманітні підходи, такі як формально-логічний, ймовірнісний, еволюційний та нечеткий. Обґрунтування та вибір показників оцінки кібербезпеки флотів БПЛА стає ключовим завданням для ефективного захисту від кіберзагроз.

5. Перший розділ надає базові знання та підґрунтя для подальших досліджень у галузі кібербезпеки БПЛА та визначає напрямок подальших досліджень у цій області.

Література до першого розділу

1. Wang Y., Liu J. Evaluation methods for the autonomy of unmanned systems. *Chinese Science Bulletin*. 2012. Т. 57, № 26. С. 3409–3418. URL: https://doi.org/10.1007/s11434-012-5183-2 (дата звернення: 25.12.2023).

2. A Guidance System for Tactical Autonomous Unmanned Aerial Vehicles / J. A. Marshall та ін. *Journal of Intelligent & Robotic Systems*. 2021. Т. 103, № 4. URL: https://doi.org/10.1007/s10846-021-01526-8 (дата звернення: 25.12.2023).

3. Beni, G. From swarm intelligence to swarm robotics. In *Swarm Robotics, Proceedings of the SAB 2004 International Workshop, Santa Monica, CA, USA, 17 July 2004*; Şahin, E., Spears, W.M., Eds.; LNCS; Springer: Berlin/Heidelberg, Germany, 2004; Volume 3342, pp. 1–9.

4. Dias, P.G.F.; Silva, M.C.; Rocha Filho, G.P.; Vargas, P.A.; Cota, L.P.; Pessin, G. Swarm Robotics: A Perspective on the Latest Reviewed Concepts and Applications. *Sensors* 2021, *21*, 2062.

5. Bini, D.; Pamela, D.; Prince, S. Machine vision and machine learning for intelligent agrobots: A review. In Proceedings of the 2020 5th International Conference on Devices, Circuits and Systems (ICDCS), Coimbatore, India, 5–6 March 2020; pp. 12–16.

6. Li, N.; Remeikas, C.; Xu, Y.; Jayasuriya, S.; Ehsani, R. Task Assignment and Trajectory Planning Algorithm for a Class of Cooperative Agricultural Robots. *J. Dyn. Syst. Meas. Control* 2015, *137*, 1–9.

7. Rezwan, S.; Choi, W. Artificial intelligence approaches for UAV navigation: Recent advances and future challenges. *IEEE Access* 2022, *10*, 26320–26339.

8. Yu, Y.; Shi, C.; Shan, D.; Lippiello, V.; Yang, Y. A hierarchical control scheme for multiple aerial vehicle transportation systems with uncertainties and state/input constraints. *Appl. Math. Model.* 2022, *109*, 651–678.

9. Brust, M.R.; Danoy, G.; Bouvry, P.; Gashi, D.; Pathak, H.; Gonçalves, M.P. Defending against intrusion of malicious uavs with networked uav defense swarms. In Proceedings of the 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops), Singapore, 9 October 2017; pp. 103–111.

10. McNeal, G.S. Drones and the future of aerial surveillance. *George Wash. Law Rev.* 2016, *84*, 354.

11. Bai, Z.; Feng, Q.; Qiu, Y. Design and research of UAV for campus express delivery. In Proceedings of the 2021 2nd International Conference on Intelligent Design (ICID), Xi'an, China, 19 October 2021; pp. 208–213.

12. Yaqot, M.; Meneze, B.C. Unmanned Aerial Vehicle (UAV) in Precision Agriculture: Business Information Technology towards Farming as a Service. In

Proceedings of the 2021 1st International Conference on Emerging Smart Technologies and Applications (eSmarTA), Sana'a, Yemen, 10–12 August 2021; pp. 1–7.

13. Agarwala, N. Integrating UUVs for naval applications. *Marit. Technol. Res.* 2022, *4*, 254470.

14. Brantner, G.; Khatib, O. Controlling Ocean One: Human–robot collaboration for deep-sea manipulation. *J. Field Robot.* 2021, *38*, 28–51.

15. Bella, S.; Belbachir, A.; Belalem, G. A Centralized Architecture for Cooperative Air-Sea Vehicles Using UAV-USV. *Int. J. Comput. Inf. Eng.* 2019, *13*, 201–210.

16. Hu, C.; Fu, L.; Yang, Y. Cooperative navigation and control for surface-underwater autonomous marine vehicles. In Proceedings of the IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chengdu, China, 15–17 December 2017; pp. 589–592.

17. Khaldi, B.; Cherif, F. An overview of swarm robotics: Swarm intelligence applied to multi-robotics. *Int. J. Comput. Appl.* 2015, *126*, 2.

18. Nedjah, N.; Junior, L.S. Review of methodologies and tasks in swarm robotics towards standardization. *Swarm Evol. Comput.* 2019, *50*, 100565.

19. Harik, E.H.C.; Guérin, F.; Guinand, F.; Brethé, J.F.; Pelvillain, H. UAV–UGV cooperation for objects transportation in an industrial area. In Proceedings of the 2015 IEEE International Conference on Industrial Technology (ICIT), Seville, Spain, 17–19 March 2015; pp. 547–552.

20. Krizmancic, M.; Arbanas, B.; Petrovic, T.; Petric, F.; Bogdan, S. Cooperative aerial–ground multi-robot system for automated construction tasks. *IEEE Robot. Autom. Lett.* 2020, *5*, 798–805.

21. Królikowski H. The Use of Unmanned Aerial Vehicles in Contemporary Armed Conflicts – Selected Issues. *Politeja*. 2022. T. 19, № 4 (79). URL: https://doi.org/10.12797/politeja.19.2022.79.02 (дата звернення: 04.07.2023).

22. Optimization of Air Defense System Deployment Against Reconnaissance Drone Swarms / N. Li та ін. *Complex System Modeling and*

Simulation. 2023. Т. 3, № 2. С. 102–117. URL: https://doi.org/10.23919/csms.2023.0003 (дата звернення: 04.09.2023).

23. Development of UAV Tracing and Coordinate Detection Method Using a Dual-Axis Rotary Platform for an Anti-UAV System / B.-H. Sheu та ін. *Applied Sciences*. 2019. Т. 9, № 13. С. 2583. URL: https://doi.org/10.3390/app9132583 (дата звернення: 04.09.2023).

24. Ewelina K. Unmanned Aerial Vehicles in the Security Service and as a New Tool in the Hands of Criminals. *Safety & Defense*. 2018. Т. 4. С. 31–36. URL: https://doi.org/10.37105/sd.6 (дата звернення: 04.09.2023).

25. Jongsik Ahn, Min Young Kim, "ICAIIC - Positional estimation of invisible drone using acoustic array with A-shaped neural network", 2021 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), pg. 320, (2021); URL:10.1109/icaiic51459.2021.9415272 (дата звернення: 04.09.2023).

26. Ростопчин В. В. Ударні безпілотні літальні апарати та протиповітряна оборона – проблеми та перспективи протистояння // Безпілотна авіація. 2019. URL : https://www.researchgate.net/publication/331772628_Udarnye_bespilotnye_letatelnye_apparaty_i_protivovozdusnaa_oborona_-problemy_i_perspektivy_protivostoania (дата звернення: 04.09.2023).

27. 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. Т. 133. С. 102894. URL: https://doi.org/10.1016/j.adhoc.2022.102894 (дата звернення: 04.09.2023).

28. Autonomous Control Systems and Vehicles: Intelligent Unmanned Systems / K. Nonami et al. Springer, 2016. 324 p.

29. Autonomous Vessels in Maritime Affairs: Law and Governance Implications / A. Pastra et al. Springer International Publishing AG, 2023.

30. MahmoudZadeh S., Powers D. M. W., Bairam Zadeh R. Autonomy and Unmanned Vehicles. Singapore : Springer Singapore, 2019. URL: https://doi.org/10.1007/978-981-13-2245-7 (date of access: 12.03.2024).

31. Boyle M. J. Drone Age: How Drone Technology Will Change War and Peace. Oxford University Press, Incorporated, 2020. 336 p.

32. Unmanned Aircraft Systems (UAS). *GlobalSecurity.org*. URL: https://www.globalsecurity.org/military/world/uav.htm (дата звернення: 04.09.2023).

33. European Union drone regulations explained - AgEagle Aerial Systems Inc. *AgEagle Aerial Systems Inc.* URL: https://ageagle.com/blog/european-union-drone-regulations-explained/ (дата звернення: 04.09.2023).

34. Bezpilotniy Letayuschiy Apparat - BPLA. *GlobalSecurity.org*. URL: https://www.globalsecurity.org/military/world/russia/aircraft-uav.htm (дата звернення: 04.09.2023).

35. Алешин Б. С., Суханов В. Л., Шибаев В. М., Шнырев А. Г. Типы беспилотных летательных аппаратов // Межотраслевой альманах. 2014. № 46. URL: http://slaviza.ru/print:page,1,1494-tipy-bespilotnyh-letatelnyh-apparatov.html. (дата звернення: 04.09.2023).

36. | Global Drone Regulations Database. | *Global Drone Regulations Database*. URL: https://www.droneregulations.info/index.html (дата звернення: 16.09.2023).

37. Ivannikova V. Y., Ayrapetyan A. G. UNMANNED AERIAL VEHICLES (UAVS) OPERATION IN UKRAINE: A REGULATIONS REVIEW. *Scientific notes of Taurida National V.I. Vernadsky University. Series: Technical Sciences*. 2021. № 6. С. 209–215. URL: https://doi.org/10.32838/2663-5941/2021.6/34 (дата звернення: 16.09.2023).

38. Pehlivanoglu Y. V., Bekmezci I., Pehlivanoglu P. Efficient Strategy for Multi-UAV Path Planning in Target Coverage Problems. *2022 International Conference on Theoretical and Applied Computer Science and Engineering (ICTASCE)*, м. Ankara, Turkey, 29 верес. – 1 жовт. 2022 р. 2022. URL: https://doi.org/10.1109/ictacse50438.2022.10009728 (дата звернення: 16.09.2023).

39. Jobard R. Les drones: La nouvelle révolution. Paris: Eyrolles, 2014. 175 с.

40. Michaelides-Mateou S. Challenges and Trends in the Aviation Industry: Integrating UAVs in Non-segregated Airspace. *Unmanned Aerial Vehicles Applications:*

Challenges and Trends. Cham, 2023. С. 377–409. URL: https://doi.org/10.1007/978-3-031-32037-8_13 (дата звернення: 16.09.2023).

41. De Freitas, E. P., Heimfarth, T., Netto, I. F., Lino, C. E., Pereira, C. E., Ferreira, A. M., Wagner, F. R., & Larsson, T. (2010). UAV relay network to support WSN connectivity. In Proceedings of the International Congress on Ultra Modern Telecommunications and Control Systems 2010, 309–314. IEEE.

42. A Survey on Swarming with Micro Air Vehicles: Fundamental Challenges and Constraints / M. Coppola та ін. *Frontiers in Robotics and AI*. 2020. Т. 7. URL: https://doi.org/10.3389/frobt.2020.00018 (дата звернення: 04.06.2023).

43. Markus E. D., Fadeyi J. Smart Cities and Spectrum Vulnerabilities in Long-Range Unlicensed Communication Bands: A Review. *Applied Soft Computing and Communication Networks*. Singapore, 2021. С. 207–220. URL: https://doi.org/10.1007/978-981-33-6173-7_14 (дата звернення: 16.09.2023).

44. Al-Bkree M. Managing the cyber-physical security for unmanned aerial vehicles used in perimeter surveillance. *International Journal of Innovative Research and Scientific Studies*. 2023. Т. 6, № 1. С. 164–173. URL: https://doi.org/10.53894/ijirss.v6i1.1173 (дата звернення: 04.06.2023).

45. AL-Dosari K., Hunaiti Z., Balachandran W. Systematic Review on Civilian Drones in Safety and Security Applications. *Drones*. 2023. Т. 7, № 3. С. 210. URL: https://doi.org/10.3390/drones7030210 (дата звернення: 04.06.2023).

46. Computational Intelligent Security in Wireless Communications / S. A. Khan та ін. Boca Raton: CRC Press, 2022. URL: https://doi.org/10.1201/9781003323426 (дата звернення: 04.06.2023).

47. Pevnev, V., Plakhteev, A., Tsuranov, M., Zemlianko, H., Leichenko, K. (2022). “Smart City” Technology: Conception, Security Issues and Cases. In: Nechyporuk, M., Pavlikov, V., Kritskiy, D. (eds) Integrated Computer Technologies in Mechanical Engineering - 2021. ICTM 2021. Lecture Notes in Networks and Systems, vol 367. Springer, Cham. URL: https://doi.org/10.1007/978-3-030-94259-5_19. (дата звернення: 04.06.2023).

48. Das A., Chowdhury A., Sil R. Third Industrial Revolution: 5G Wireless Systems, Internet of Things, and Beyond. *5G and Beyond*. Singapore, 2023. С. 19–43. URL: https://doi.org/10.1007/978-981-99-3668-7_2 (дата звернення: 16.09.2023).

49. Towards Security Mechanism in D2D Wireless Communication: A 5G Network Approach / D. Gupta та ін. *Wireless Communications and Mobile Computing*. 2022. Т. 2022. С. 1–9. URL: https://doi.org/10.1155/2022/6983655 (дата звернення: 16.09.2023).

50. Zhang X., Bai Y., He K. On Countermeasures against Cooperative Fly of UAV Swarms. *Drones*. 2023. Т. 7, № 3. С. 172. URL: https://doi.org/10.3390/drones7030172 (дата звернення: 16.09.2023).

51. Impact of Routing Techniques and Mobility Models on Flying Ad Hoc Networks / M. A. Hassan та ін. *Studies in Computational Intelligence*. Cham, 2022. С. 111–129. URL: https://doi.org/10.1007/978-3-030-97113-7_7 (дата звернення: 16.09.2023).

52. Markus E. D., Fadeyi J. Smart Cities and Spectrum Vulnerabilities in Long-Range Unlicensed Communication Bands: A Review. *Applied Soft Computing and Communication Networks*. Singapore, 2021. С. 207–220. URL: https://doi.org/10.1007/978-981-33-6173-7_14 (дата звернення: 16.09.2023).

53. Flying Sensor Network Optimization Using Bee Intelligence for Internet of Things / A. Salam та ін. *Advances in Intelligent Systems and Computing*. Cham, 2020. С. 331–339. URL: https://doi.org/10.1007/978-3-030-55190-2_25 (дата звернення: 16.09.2023).

54. De Freitas, E. P., Heimfarth, T., Netto, I. F., Lino, C. E., Pereira, C. E., Ferreira, A. M., Wagner, F. R., & Larsson, T. (2010). UAV relay network to support WSN connectivity. In Proceedings of the International Congress on Ultra Modern Telecommunications and Control Systems 2010, 309–314. IEEE.

55. Gupta, L., Jain, R., & Vaszkun, G. (2016). Survey of Important Issues in UAV Communication Networks. IEEE Communications Surveys & Tutorials, 18(2), 1123–1152.

56. Orfanus, D., Eliassen, F., & de Freitas, E. P. (2014). Self-Organizing Relay Network Supporting Remotely Deployed Sensor Nodes in Military Operations. In 6th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 326–333. IEEE.

57. Advanced Sensor Systems for Robotics and Autonomous Vehicles / M. Tolani та ін. *Artificial Intelligence for Robotics and Autonomous Systems Applications*. Cham, 2023. С. 439–459. URL: https://doi.org/10.1007/978-3-031-28715-2_14 (дата звернення: 16.09.2023).

58. Wang J., Wang W., Wu Q. Trajectory Planning of UAV in Unknown Dynamic Environment with Deep Reinforcement Learning. *Lecture Notes in Electrical Engineering*. Singapore, 2019. С. 470–480. URL: https://doi.org/10.1007/978-981-32-9686-2_54 (дата звернення: 16.09.2023).

59. URSI resolution on Criminal activities using electromagnetic tools. - The Radio Science Bulletin. - 1999. - No. 290. - pp. 62-63.

60. Routing in Flying Ad Hoc Networks: Survey, Constraints, and Future Challenge Perspectives / O. S. Oubbati та ін. *IEEE Access*. 2019. Т. 7. С. 81057–81105. URL: https://doi.org/10.1109/access.2019.2923840 (дата звернення: 16.09.2023).

61. IEC 61000-2-10:2021. Electromagnetic compatibility (EMC) - Part 2-10: Environment - Description of HEMP environment - Conducted disturbance. На заміну IEC 61000-2-10:1998; чинний від 2021-11-18. Вид. офіц. International Electrotechnical Commission, 2021. 47 с.

62. Singh R., Singh R., Kaur P. Clustering and Securing IoT Wireless Sensor Network. *International Journal of Computer Science and Mobile Computing*. 2022. Т. 11, № 4. С. 49–60. URL: https://doi.org/10.47760/ijcsmc.2022.v11i04.007 (дата звернення: 16.09.2023).

63. Lateef S., Rizwan M., Hassan M. A. Security Threats in Flying Ad Hoc Network (FANET). *Studies in Computational Intelligence*. Cham, 2022. С. 73–96. URL: https://doi.org/10.1007/978-3-030-97113-7_5 (дата звернення: 16.09.2023).

64. Gupta A., Gupta S. K. A survey on green unmanned aerial vehicles-based fog computing: Challenges and future perspective. *Transactions on Emerging*

Telecommunications Technologies. 2022. URL: https://doi.org/10.1002/ett.4603 (дата звернення: 04.06.2023).

65. International Civil Aviation Organization (ICAO) Standards. URL: https://www.icao.int/ (дата звернення: 04.02.2022).

66. An optimal wsn coverage based on adapted transit search algorithm / T.-K. Dao та ін. *International Journal of Software Engineering and Knowledge Engineering*. 2023. URL: https://doi.org/10.1142/s0218194023400016 (дата звернення: 16.09.2023).

67. Panchal H., Gajjar S. Fuzzy Logic-Based Cluster Head Selection an Underwater Wireless Sensor Network: A Survey. *Communication and Intelligent Systems*. Singapore, 2022. С. 661–673. URL: https://doi.org/10.1007/978-981-19-2130-8_51 (дата звернення: 16.09.2023).

68. Ammari H. M. Spatial Unconditional and Conditional Network Connectivity and Fault-Tolerance Measures for k-Covered Wireless Sensor Networks. *Theory and Practice of Wireless Sensor Networks: Cover, Sense, and Inform*. Cham, 2022. С. 375–396. URL: https://doi.org/10.1007/978-3-031-07823-1_12 (дата звернення: 16.09.2023).

69. Dey B., Bandyopadhyay S., Nandi S. Mobility Assisted Adaptive Clustering Hierarchy for IoT Based Sensor Networks in 5G and Beyond. *Journal of Communications*. 2023. С. 346–356. URL: https://doi.org/10.12720/jcm.18.6.346-356 (дата звернення: 16.09.2023).

70. Implementation of the Communication Network for the Multi-Agent Robotic Systems / R. Kirichek та ін. *International Journal of Embedded and Real-Time Communication Systems*. 2016. Т. 7, № 1. С. 48–63. URL: https://doi.org/10.4018/ijertcs.2016010103 (дата звернення: 16.09.2023).

71. Singh V., Lohani R. B. Mobility Aware Energy Efficient Clustering for Wireless Sensor Network. *2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, м. Coimbatore, India, 20–22 лют. 2019 р. 2019. URL: https://doi.org/10.1109/icecct.2019.8869231 (дата звернення: 16.09.2023).

72. Anitha A. A., Arockiam L. A Review on Intrusion Detection Systems to Secure IoT Networks. *International Journal of Computer Networks and Applications*. 2022. Т. 9,

№ 1. С. 38. URL: https://doi.org/10.22247/ijcna/2022/211599 (дата звернення: 16.09.2023).

73. Rani P., Gupta N. K. Composite Trust for Secure Routing Strategy through Energy based Clustering in WSN. *2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)*, м. Bhilai, India, 19–20 лют. 2021 р. 2021. URL: https://doi.org/10.1109/icaect49130.2021.9392453 (дата звернення: 16.09.2023).

74. Hammoud B., Wehn N. Recent Advances in Oil-Spill Monitoring Using Drone-Based Radar Remote Sensing. *Environmental Sciences*. 2022. URL: https://doi.org/10.5772/intechopen.106942 (дата звернення: 16.09.2023).

75. Falorca J. F., Miraldes J. P. N. D., Lanzinha J. C. G. New trends in visual inspection of buildings and structures: Study for the use of drones. *Open Engineering*. 2021. Т. 11, № 1. С. 734–743. URL: https://doi.org/10.1515/eng-2021-0071 (дата звернення: 04.06.2023).

76. Ahmad H., Farhan M., Farooq U. Computer Vision Techniques for Military Surveillance Drones. *Wasit Journal of Computer and Mathematics Science*. 2023. Т. 2, № 2. С. 56–63. URL: https://doi.org/10.31185/wjcms.148 (дата звернення: 16.09.2023).

77. U.S. Navy Plans to Fly First Drone Swarm This Summer. *Military.com*. URL: https://www.military.com/defensetech/2016/01/04/u-s-navy-plans-to-fly-first-drone-swarm-this-summer#:~:text=The%20aim%20is%20to%20have,swarm%20as%20a%20single%20unit. (дата звернення: 04.09.2023).

78. Drew J. DARPA selects industry teams for 'Gremlins' UAV project. *Flight Global*. URL: https://www.flightglobal.com/civil-uavs/darpa-selects-industry-teams-for-gremlins-uav-project/120171.article (дата звернення: 04.09.2023).

79. Хусити вдарили з дрона по нафтосховищу в Саудівській Аравії – DW – 08.03.2021. *dw.com*. URL: https://www.dw.com/ru/husity-nanesli-udar-s-drona-po-neftehranilishhu-v-portu-saudovskoj-aravii/a-56801618 (дата звернення: 04.09.2023).

80. Militants and Drones: A Trend That is Here to Stay. *Homepage | Royal United Services Institute*. URL: https://www.rusi.org/explore-our-research/publications/commentary/militants-and-drones-trend-here-stay (дата звернення: 04.09.2023).

81. Designers and Manufacturers of Drone Software and Hardware for Enterprise - Sky-Drones Technologies Ltd. *Designers and Manufacturers of Drone Software and Hardware for Enterprise - Sky-Drones Technologies Ltd*. URL: http://sky-drones.com (дата звернення: 04.09.2023).

82. Dynamic Online Trajectory Planning for a UAV-Enabled Data Collection System / S. Li та ін. *IEEE Transactions on Vehicular Technology*. 2022. С. 1–12. URL: https://doi.org/10.1109/tvt.2022.3200458 (дата звернення: 16.09.2023).

83. U.5. URSI Resolution on Criminal Activities using Electromagnetic Tools. *URSI Home*. URL: https://www.ursi.org/files/GeneralAssemblies/resolutions/1999_U05_Criminal%20Activities%20using%20Electromagnetic%20Tools.pdf (дата звернення: 04.09.2023).

84. A Flow Feedback Traffic Prediction Based on Visual Quantified Features / J. Chen та ін. *IEEE Transactions on Intelligent Transportation Systems*. 2023. С. 1–9. URL: https://doi.org/10.1109/tits.2023.3269794 (дата звернення: 04.09.2023).

85. *SumDU Repository: Home*. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/93255/1/Дисертація%20М.%20І.%20Мироненко.pdf;jsessionid=705D24C858FA2261FE8AAC2DF0B69DCB (дата звернення: 08.11.2023).

86. Застосування безпілотних авіаційних систем у сфері цивільного захисту: монографія / Д.В. Бондар, А.В. Гурник, А.О. Литовченко, В.В. Хижняк, В.Л. Шевченко, Д.М. Ядченко. Київ, 2022, 312 с. URL: eSLU7FcmeJYIEPehdm0Ill3Cn39Bi1BMIl3IedcX.pdf (dsns.gov.ua)

87. Repository at ChSTU: Методи та інформаційна технологія автоматизованого планування маршрутів польотів безпілотних літальних апаратів для підвищення ефективності пошуку об’єктів. *Repository at ChSTU: Home*. URL: https://er.chdtu.edu.ua/handle/ChSTU/1144 (дата звернення: 08.04.2024).

88. Internet of Drones: AI Applications for Smart Solutions / A. Solanki et al. Apple Academic Press, Incorporated, 2022.

89. Hu F. Uav Swarm Networks: Models Protocols and Systems. Taylor & Francis Group, 2020.

90. Krishnan S., Murugappan M. Internet of Drones. Boca Raton : CRC Press, 2023. URL: https://doi.org/10.1201/9781003252085 (date of access: 08.04.2024).

91. A Distributed Collaborative Allocation Method of Reconnaissance and Strike Tasks for Heterogeneous UAVs / H. Deng та ін. *Drones*. 2023. Т. 7, № 2. С. 138. URL: https://doi.org/10.3390/drones7020138 (дата звернення: 16.09.2023).

92. Group Target Tracking for Highly Maneuverable Unmanned Aerial Vehicles Swarms: A Perspective / Y. Chen та ін. *Sensors*. 2023. Т. 23, № 9. С. 4465. URL: https://doi.org/10.3390/s23094465 (дата звернення: 16.09.2023).

93. Abdulhae O. T., Mandeep J. S., Islam M. Cluster-Based Routing Protocols for Flying Ad Hoc Networks (FANETs). *IEEE Access*. 2022. Т. 10. С. 32981–33004. URL: https://doi.org/10.1109/access.2022.3161446 (дата звернення: 06.09.2022).

94. Omolara A. E., Alawida M., Abiodun O. I. Drone cybersecurity issues, solutions, trend insights and future perspectives: a survey. *Neural Computing and Applications*. 2023. URL: https://doi.org/10.1007/s00521-023-08857-7 (дата звернення: 16.09.2023).

95. McEnroe P., Wang S., Liyanage M. A Survey on the Convergence of Edge Computing and AI for UAVs: Opportunities and Challenges. *IEEE Internet of Things Journal*. 2022. С. 1. URL: https://doi.org/10.1109/jiot.2022.3176400 (дата звернення: 04.06.2023).

96. A Review on Security Issues and Solutions of the Internet of Drones / W. Yang та ін. *IEEE Open Journal of the Computer Society*. 2022. С. 1–15. URL: https://doi.org/10.1109/ojcs.2022.3183003 (дата звернення: 04.06.2023).

97. Subbarayalu V., Vensuslaus M. A. An Intrusion Detection System for Drone Swarming Utilizing Timed Probabilistic Automata. *Drones*. 2023. Т. 7, № 4. С. 248. URL: https://doi.org/10.3390/drones7040248 (дата звернення: 04.06.2023).

98. L. M. Gladence, V. M. Anu, A. Anderson, I. Stanley, J. A. Fernando J and S. Revathy, "Swarm Intelligence in Disaster Recovery," 2021 5th International Conference

on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2021, pp. 1-8, URL: 10.1109/ICICCS51141.2021.9432146 (дата звернення: 04.06.2023).

99. C. Jeon, J. Ha, H. Ko, B. Lee, B. Ryu. Swarmsense: Effective and Resilient Drone Swarm and Search for Disaster Response and Management Application. URL: https://www.wirelessinnovation.org/assets/Proceedings/2019/TS6.2%20Jeon%20presentation.pdf (дата звернення: 04.06.2023).

100. Про затвердження Змін до Правил інженерно-авіаційного забезпечення державної авіації України: Наказ М-ва оборони України від 03.08.2021 р. № 223. URL: https://zakon.rada.gov.ua/laws/show/z1221-21#Text (дата звернення: 05.09.2023).

101. Про затвердження Правил технічної експлуатації безпілотних авіаційних комплексів І класу державної авіації України : Наказ М-ва оборони України від 10.08.2018 р. № 401. URL: https://zakon.rada.gov.ua/laws/show/z1062-18#Text (дата звернення: 05.09.2023).

102. ДСТУ В 7371:2020. Техніка авіаційна державної авіації. Апарати літальні безпілотні. Основні терміни та визначення понять. Класифікація. На заміну 7371:2013; чинний від 2021-07-01. Вид. офіц. Україна: Стандартизація продукції оборон. призначення, 2020. 16 с.

103. Повітряний кодекс України: Кодекс України від 19.05.2011 р. № 3393-VI: станом на 2 серп. 2023 р. URL: https://zakon.rada.gov.ua/laws/show /3393-17#Text (дата звернення: 05.09.2023).

104. Про затвердження Положення про використання повітряного простору України: Постанова Каб. Міністрів України від 06.12.2017 р. № 954: станом на 5 січ. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/954-2017-п#Text (дата звернення: 05.09.2023).

105. Про затвердження Авіаційних правил України «Правила використання повітряного простору України»: Наказ Держ. авіац. служби України від 11.05.2018 р. № 430/210. URL: https://zakon.rada.gov.ua/laws/show/z1056-18#Text (дата звернення: 05.09.2023).

106. Застосування безпілотних авіаційних систем у сфері цивільного захисту: монографія / Д.В. Бондар та ін. Київ: ГО «Європ. наук. платформа», 2022. 312 с.

107. Міжнародні стандарти цивільної авіації (МКАО). URL: https://www.icao.int/ (дата звернення: 19.08.2022).

108. Європейське агентство з безпеки авіації (EASA). URL: https://www.easa.europa.eu/ (дата звернення: 19.08.2022).

109. STANAG 4586 Ed 4. Standard Interfaces of UAV Control System (UCS) for NATO UAV Interoperability - AEP-84 Edition A. На заміну STANAG 4586; чинний від 2020-02-08. Вид. офіц. NATO, 2017. 13 с.

110. Mathematical Approaches Transform Cybersecurity from Protoscience to Science / I. Trenchev та ін. *Applied Sciences*. 2023. Т. 13, № 11. С. 6508. URL: https://doi.org/10.3390/app13116508 (дата звернення: 08.11.2023).

111. The Etiology of Cybersecurity / M. Ambrosi та ін. *Lecture Notes in Computer Science*. Cham, 2022. С. 299–319. URL: https://doi.org/10.1007/978-3-031-16815-4_17 (дата звернення: 08.11.2023).

112. New Advancements in Cybersecurity: A Comprehensive Survey / M. A. Hassan та ін. *Studies in Big Data*. Cham, 2022. С. 3–17. URL: https://doi.org/10.1007/978-3-031-05752-6_1 (дата звернення: 08.11.2023).

РОЗДІЛ 2. РОЗРОБЛЕННЯ КОНЦЕПТУАЛЬНОЇ ТА МАТЕМАТИЧНИХ МОДЕЛЕЙ КІБЕРФІЗИЧНОЇ СИСТЕМИ БАГАТОФУНКЦІЙНИХ ФЛОТІВ БЕЗПІЛОТНИХ АПАРАТІВ

2.1 Модель інфраструктури системи багатофункційних флотів БА

У сучасному світі СБФ БА стали невід'ємною частиною багатьох галузей, являючи собою складні технічні структури, спроектовані для вирішення різноманітних завдань у різних сферах. Вони виступають як універсальний інструмент, здатний ефективно функціонувати в найрізноманітніших галузях.

Ці системи, засновані на безпілотних апаратах, володіють безліччю функцій і можливостей, що вимагають злагодженої та надійної інфраструктури для свого повноцінного функціонування. Важливість цієї інфраструктури простягається від забезпечення надійності системи до її ефективності та кібербезпеки. Вона є основою для розвитку та еволюції таких комплексних технічних структур.

Для ефективного планування та розробки методів кібербезпеки систем беспілотних апаратів було розроблення кіберфізична схема інфраструктури для системи БА, з огляду на їхню багатофункціональність і потенційні загрози безпеці. Розуміння та моделювання цієї інфраструктури має важливе значення для забезпечення не лише стабільного функціонування системи, а й її захисту від можливих загроз та непередбачуваних ситуацій.

Кіберфізична схема СБФ БПА — система, в якій є взаємодія між фізичними елементами пристроїв та цифровим середовищем, що контролює їх роботу. Система охоплює апаратні компоненти, програмне забезпечення та мережеві зв'язки, які спільно працюють для забезпечення функціонування цієї системи. Ця архітектура системи систем (СС), дозволяє максимізувати переваги роботи більшої системи та розуміє функції, взаємодії та використання кожного маленького компонента. Цей підхід до проектування допомагає розглядати систему в цілому, зосереджуючись на тому, як компоненти взаємодіють, як вони функціонують з

часом і як вони функціонують у контексті більшої системи, що розвивається, яку можна масштабувати відповідно до місій і ситуацій [1].

Після аналізу на рисунку 2.1 показано схему, яка відображає загальну структуру системи. Багатофункціональна безпілотна інфраструктура, яка поєднує БПЛА (безпілотний літальний апарат), БНА (безпілотний наземний апарат), БПА (безпілотний підводний апарат) і БНК (безпілотний надводний корабель), є складною системою, що складається з різних компонентів: флотів, зарядні станції, бази даних, хмарне сховище, центри зв’язку, оператори, супутники, мобільна зарядка, станції зв'язку та інші компоненти. Ці компоненти відіграють ключову роль у роботі та управлінні системою [1].

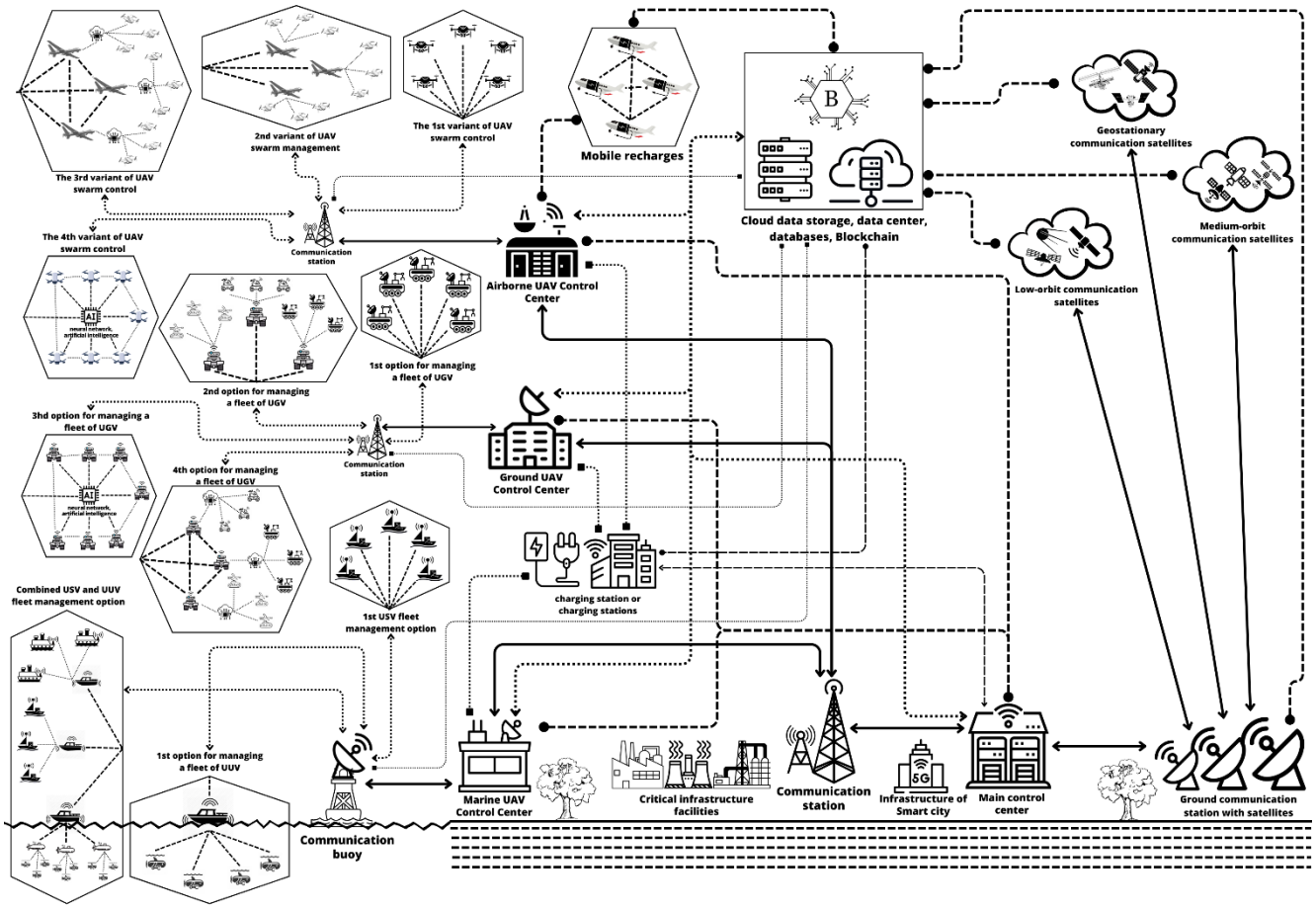


Рисунок 2.1 – Кіберфізична схема СБФ БПА

Ця модель інтегрованої інфраструктури сприяє комплексному управлінню, моніторингу та взаємодії між різними компонентами багатофункціонального

безпілотного транспорту, забезпечуючи ефективність і безпеку в різних сценаріях застосування.

Такі інтегровані системи дозволяють ефективно використовувати переваги кожного типу безпілотного транспортного засобу для вирішення різноманітних завдань у різних середовищах (повітря, земля, вода).

Однак, у зв'язку зі зростанням складності та різноманітності багатофункціональних безпілотних апаратів, необхідно враховувати, що їхні функції та характеристики можуть значно відрізнятися в залежності від конкретного застосування. З цією метою важливим етапом є декомпозиція кіберфізичної схеми на більш дрібні підсистеми, спеціалізовані під кожен вид безпілотного транспорту.

Тому наступним кроком дослідження була декомпозиція систему в напрямку інфраструктурної моделі для багатофункціональних флотів БПЛА зорієнтована на моніторинг критичної інфраструктури. Ця декомпозиція дозволить розглядати кожен вид безпілотника як окрему підсистему з унікальними властивостями та ризиками, сприяючи ефективній розробці та вдосконаленню заходів кібербезпеки для кожного напряму використання безпілотників.

2.1.1 Концептуальна схема системи багатофункційних флотів БПЛА

Для забезпечення кібербезпеки багатофункційних флотів БПЛА та оцінки їх надійності враховуючи функціональні стани, вразливості безпеки, деградацію систем та інше, було розроблено відповідні моделі та концептуальну інфраструктуру.

Концептуальна схема системи багатофункційних флотів (СБФ) БПЛА - це архітектура "системи в системі" (СвС), яка максимізує вигоду від експлуатації більшої системи і розуміє функції, взаємодію і використання кожного невеликого компонента. Такий підхід до проектування допомагає розглядати систему як єдине ціле і фокусується на взаємодії компонентів, їх функціонуванні в часовому вимірі,

а також на їх функціонуванні в контексті більшої системи, що розвивається, яка може бути масштабована відповідно до місій і ситуацій [1, 2, 3].

Рисунок 2.2, згідно з термінологією вище, демонструє схему, яка надає загальне уявлення про структуру системи та взаємодію між її компонентами (флоти БПЛА, зарядні станції, бази даних, хмарні сховища, центри зв'язку, оператори, супутники, мобільні зарядні станції та інші), які відіграють важливу роль у її функціонуванні та управлінні.

Основні компоненти взаємозв'язків та взаємодії з багатофункційним флотом БПЛА:

1. Зарядні станції: флоти БПЛА потребують регулярної зарядки, тому зарядні станції є невід'ємною частиною їхньої інфраструктури. Безпілотні апарати повертаються на зарядні станції для перезаряджання батарей та підготовки до наступних місій.

2. Бази даних: для управління флотами БПЛА використовуються бази даних, де зберігається інформація про кожен апарат, його характеристики, поточний стан, історію польотів та інших даних. Бази даних забезпечують централізоване управління та моніторинг флотом БПЛА.

3. Хмарні сховища: для зберігання великого обсягу даних, таких як відео, фотографії, знімки з камер, журнали польотів та інші дані використовуються хмарні сховища. Вони дозволяють доступ до даних з будь-якого пристрою та забезпечують їх збереження та доступність.

4. Центр зв'язку: центр зв'язку є нерозривним зв'язком між оператором та БПЛА. Він забезпечує передачу команд та отримання зворотного зв'язку від апаратів. Центр зв'язку здійснює моніторинг та контроль над флотом БПЛА, забезпечуючи надійний зв'язок та передачу даних.

5. Оператор: оператори є відповідальними за управління та контроль флотами БПЛА. Вони використовують спеціальні пристрої, такі як планшети, для моніторингу польотів, перегляду даних та виконання необхідних операцій. Оператори також забезпечують взаємодію з іншими системами та компонентами, ухвалюючи рішення на основі отриманих даних.

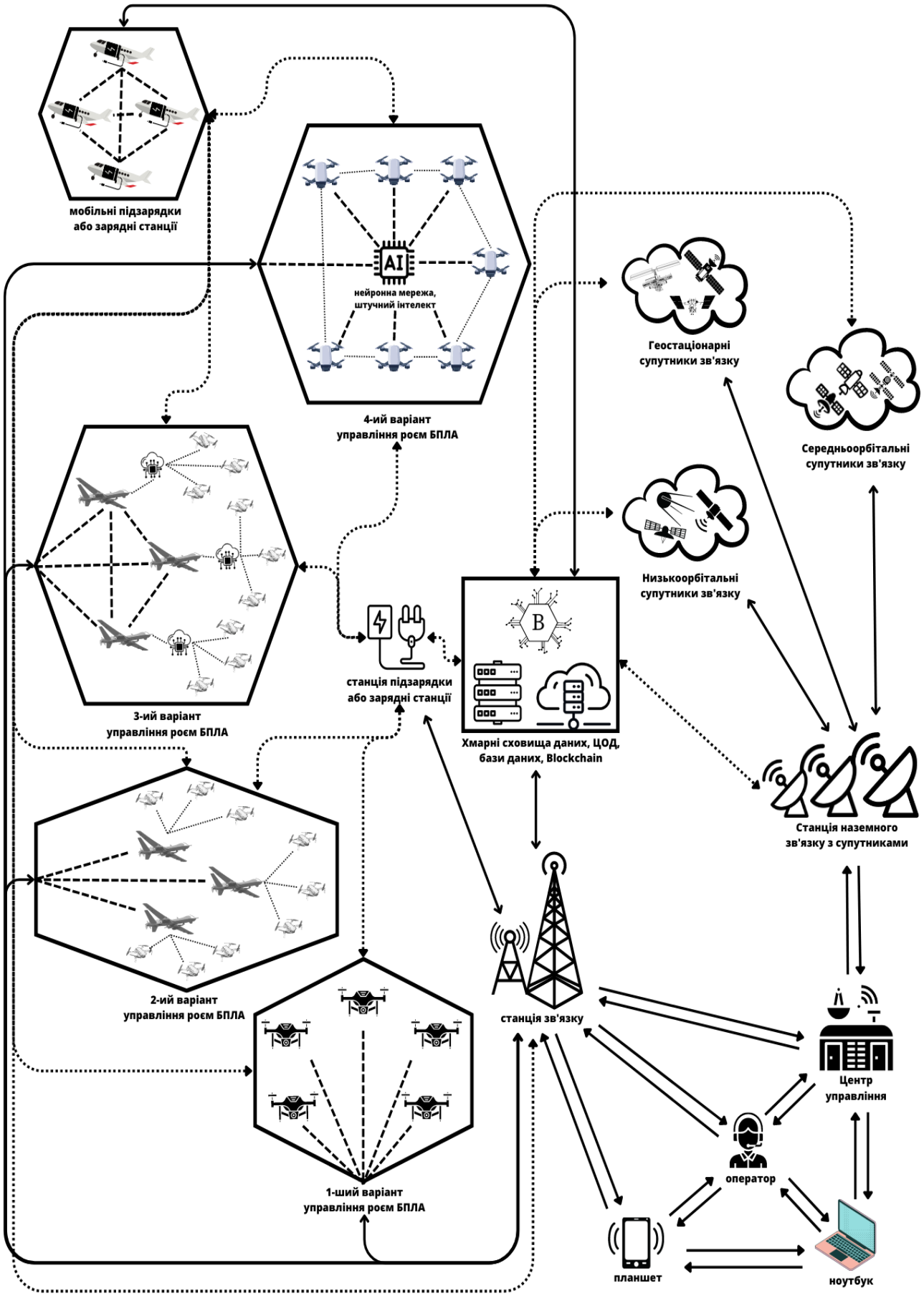


Рисунок 2.2 – Концептуальна схема системи багатофункційних флотів БПЛА

6. Супутники: флоти БПЛА можуть використовувати супутники для глобального позиціонування, навігації та обміну даними. Супутники забезпечують точність позиціонування та передачі даних на великі відстані, що важливо для місій, що потребують широкого охоплення та довгострокової роботи.

7. Мобільні зарядні станції: крім стаціонарних зарядних станцій, флоти БПЛА можуть використовувати мобільні зарядні станції. Вони дозволяють швидко заряджати апарати на віддалених майданчиках або в польових умовах, забезпечуючи гнучкість та мобільність флоту.

8. Планшети: планшети є одним із пристроїв, які оператори використовують для управління та моніторингу флотами БПЛА. Вони надають операторам доступ до даних, керуючим інтерфейсом та функціональності для контроля та взаємодії з апаратами.

9. Контрольні пункти зв'язку: у деяких випадках флоти БПЛА можуть використовувати контрольні пункти зв'язку для забезпечення зв'язку та передачі в певних зонах або на великих відстанях.

Ці компоненти та системи забезпечують необхідну інфраструктуру та можливості для управління, контролю та організації для підвищення безпеки багатофункційних флотів БПЛА у різних сценаріях та операціях. Взаємодія між ними дозволяє ефективно використовувати та керувати БПЛА, забезпечуючи їх надійність, безпеку та ефективність.

2.1.2 Ієрархічна модель інфраструктури

Ієрархічна модель інфраструктури багатофункційних флотів БПЛА передбачає структуру, що складається з різних рівнів: систем, підсистем, компонентів та елементів, згідно рисунку 2.2. Кожен рівень взаємодіє з нижчими рівнями, утворюючи комплексну інфраструктуру для оперативного управління флотами БПЛА, рис. 2.3 [1].

На верхньому рівні знаходяться системи, в яких інтегровані багатофункційні флоти БПЛА, визначені спільні риси та взаємодіють з певними аспектами

управління та безпеки. Наступний рівень підсистем - це групи взаємопов'язаних компонентів, які спільно виконують певні функції та забезпечують окремі аспекти управління та спостереження за флотами БПЛА.

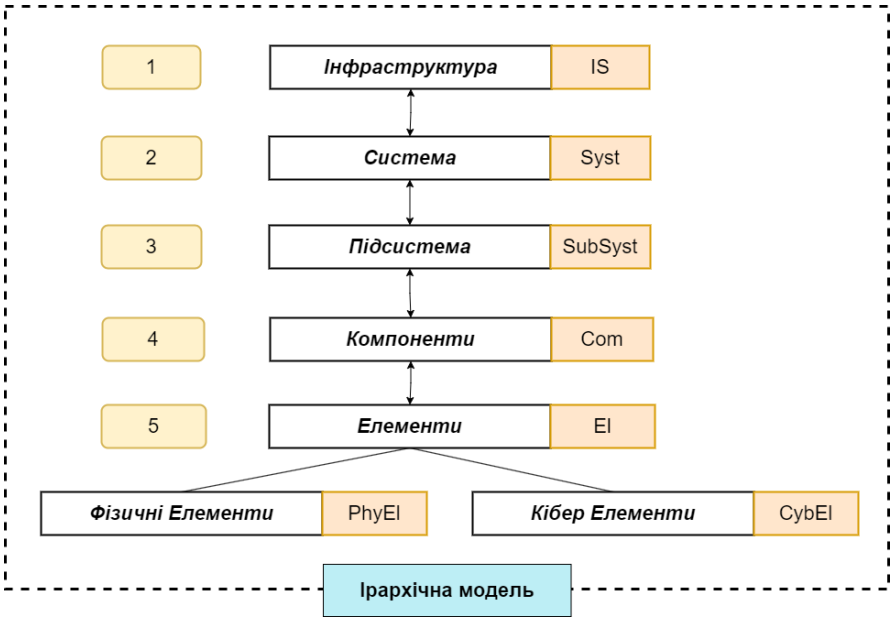


Рисунок 2.3 – Ірархічна модель системи багатофункціональних флотів БПЛА

Компоненти та елементи є найнижчим рівнем інфраструктури і являють собою окремі фізичні частини, з яких складається підсистема. Вони можуть виконувати різні функції, такі як збір і передача даних, управління рухом і стабілізація, зв'язок з центрами управління та іншими БПЛА. Взаємодія між різними рівнями інфраструктури максимізує потенційну функціональність і ефективність багатофункційного флоту БПЛА при виконанні різних завдань і місій. Ієрархічна модель інфраструктури включає як кібер, так і фізичні елементи. Взаємодія між цими елементами визначає структуру і забезпечує ефективність системи в цілому [1].

Ця ієрархічна модель інфраструктури збалансовує взаємозв'язки між різними рівнями системи і забезпечує високий ступінь координації та управління в багатофункційному флоті БПЛА. Взаємодія між системами, підсистемами, компонентами та елементами створює можливість ефективного виявлення та

реагування на складні атаки, підвищуючи кібербезпеку та надійність парку БПЛА в різних сценаріях.

2.1.3 Теоретико-множинний опис інфраструктури системи багатофункційних флотів БПЛА

Опис інфраструктури системи багатофункційних флотів БПЛА на основі теорії множин забезпечує системний підхід до вивчення та аналізу складної структури цих систем. Цей опис дозволяє виявити та формалізувати взаємозв'язки між різними елементами та компонентами інфраструктури [1,4].

У наведеному теоретичному описі інфраструктури багатофункційного флоту БПЛА, за підрозділом 2.1.2, система представлена як сукупність різних наборів: систем, підсистем, компонентів та елементів, згідно рисунку 2.3. Системи представляють найвищий рівень управління та координації і включають підсистеми, підсистеми включають компоненти, а компоненти включають окремі елементи інфраструктури. Для формування математичних множин та визначення позначень елементам інфраструктури багатофункційних флотів БПЛА використовуються наступні позначення:

1. IS – інфраструктура;
2. Syst – системи;
3. SubSyst – підсистеми;
4. Com – компоненти;
5. El – елементи.

Ці позначення дозволяють створити систематичну структуру і визначати зв'язки між різними елементами за допомогою математичних операцій над множинами:

– IS - множина об’єктів інфраструктури:

$$IS = \{\mathrm{Syst}_i, L_i\} \tag{2.1}$$

, де $Syst_i$ – системи, які входять в інфраструктуру згідно рис. 2.2, L_i – множина зв’язків між системами, які можуть мати як кібер так і фізичні зв’язки. Матрицю зв'язків можна записати у вигляді матриці, де елемент *L(i, n)* відповідає наявності зв'язку між системою *i* до системи *n*:

$$L_{IS} = \begin{array}{c} \\ Syst_1 \\ \vdots \\ Syst_i \\ \vdots \\ Syst_n \end{array} \begin{array}{c} \begin{array}{ccccccc} Syst_1 & \cdots & Syst_i & \cdots & Syst_n \end{array} \\ \begin{bmatrix} - & \cdots & L_{1,i}^{cyber}, L_{1,i}^{phys} & \cdots & L_{1,n}^{cyber}, L_{1,n}^{phys} \\ L_{i,1}^{cyber}, L_{i,1}^{phys} & \cdots & - & \cdots & L_{i,n}^{cyber}, L_{i,n}^{phys} \\ L_{n,1}^{cyber}, L_{n,1}^{phys} & \cdots & L_{n,i}^{cyber}, L_{n,i}^{phys} & \cdots & - \end{bmatrix} \end{array} \quad (2.2)$$

, де $L_{IS_{b,q}}$ – зв’язок між елементами b і q компоненти IS , який описується двома (кібер та фізичною) складовими:

$$L_{IS_{b,q}} = \left\{L_{ib,iq}^{cyber}, L_{ib,iq}^{phys}\right\} \quad (2.3)$$

, при цьому цей зв’язок може бути описаний чотирма кодами:

$$L_{IS_{b,q}} = \begin{cases} 00, \text{кібер та фізичні зв’язки відсутні;} \\ 01, \text{є тільки фізичний зв’язок;} \\ 10, \text{є тільки кібер зв’язок;} \\ 11, \text{є кібер та фізичні зв’язки.} \end{cases}$$

– Syst – множина об’єктів системи:

$$Syst_i = \left\{Syst_i^{cyber}, Syst_i^{phys}, F_i, L_{ij}\right\} , \quad (2.4)$$

, де $Syst_i^{cyber} = \left\{Syst_{ij}^{cyber}, j = 1,2, \dots, m\right\}$ – множина кіберсистем, а $Syst_i^{phys} = \left\{Syst_{ik}^{phys}, k = 1,2, \dots, m\right\}$ – множина фізичних систем, а m – їх кількість у системі $Syst_i$. Прикладом таких систем можуть бути: флоти БПЛА, центри зв'язку, центри збереження даних та інше, де множина $F_i = \{F_{iv}, v = 1,2, \dots, m\}$ – це набір функцій, які виконує система залежно від поставлених задач або цілей, де m – їх кількість у системі $Syst_i$, а L_{ij} – зв'язок між підсистемами *i* та *j* в системі:

$$L_{Syst_i} = \begin{array}{c} \\ SubSyst_{i1} \\ \vdots \\ SubSyst_{ij} \\ \vdots \\ SubSyst_{in_i} \end{array} \begin{array}{c} \begin{array}{ccccc} SubSyst_{i1} & \cdots & SubSyst_{ij} & \cdots & SubSyst_{in_i} \end{array} \\ \begin{bmatrix} - & \cdots & L_{i1,ij}^{cyber}, L_{i1,ij}^{phys} & \cdots & L_{i1,in_i}^{cyber}, L_{i1,in_i}^{phys} \\ L_{ij,i1}^{cyber}, L_{ij,i1}^{phys} & \cdots & - & \cdots & L_{ij,in_i}^{cyber}, L_{ij,in_i}^{phys} \\ L_{in_i,i1}^{cyber}, L_{in_i,i1}^{phys} & \cdots & L_{in_i,ij}^{cyber}, L_{in_i,ij}^{phys} & \cdots & - \end{bmatrix} \end{array} \quad (2.5)$$

, де $L_{Syst_{ib,iq}}$ – зв'язок між елементами b і q компоненти $Syst_i$, який описується двома (кібер та фізичною) складовими:

$$L_{Syst_{ib,iq}} = \left\{L_{ijb,ijq}^{cyber}, L_{ijb,ijq}^{phys}\right\} \quad (2.6)$$

, при цьому цей зв'язок може бути описаний чотирма кодами:

$$L_{Syst_{ib,iq}} = \begin{cases} 00, \text{кібер та фізичні зв'язки відсутні;} \\ 01, \text{є тільки фізичний зв'язок;} \\ 10, \text{є тільки кібер зв'язок;} \\ 11, \text{є кібер та фізичні зв'язки.} \end{cases}$$

– SubSyst – множина об'єктів підсистеми:

$$SubSyst_j = \left\{SubSyst_j^{cyber}, SubSyst_j^{phys}, F_{ij}, L_{ijk}\right\} \quad (2.7)$$

, де $SubSyst_j^{cyber} = \left\{SubSyst_{js}^{cyber}, s = 1,2, \dots, m\right\}$ – множина кіберпідсистем, а $SubSyst_j^{phys} = \left\{SubSyst_{jk}^{phys}, k = 1,2, \dots, m\right\}$ – множина фізичних підсистем, а m – їх кількість у підсистемі $SubSyst_j$. Прикладом таких підсистем можуть бути: БПЛА, оператори, супутники та інше, де множина $F_{ij} = \left\{F_{ijw}, w = 1,2, \dots, m\right\}$ – це набір функцій, які виконує підсистема залежно від системи в якій знаходится (згідно формулі 2.4) та поставлених задач або цілей, де m – їх кількість у підсистемі $SybSyst_j$, L_{ijk} – зв'язок між об'єктами інфраструктури, де i - система, j - підсистема, k – компонент, які знаходяться на різних рівнях ієрархії:

$$L_{SubSyst_{ij}} = \begin{matrix} \\ Com_{ij1} \\ \vdots \\ Com_{ijk} \\ \vdots \\ Com_{ijn_{ij}} \end{matrix} \begin{matrix} \begin{matrix} Com_{ij1} & \cdots & Com_{ijk} & \cdots & Com_{ijn_{ij}} \end{matrix} \\ \begin{bmatrix} - & \cdots & L^{cyber}_{ij1,ijk}, L^{phys}_{ij1,ijk} & \cdots & L^{cyber}_{ij1,ijn_{ij}}, L^{phys}_{1,ijn_{ij}} \\ L^{cyber}_{ijk,ij1}, L^{phys}_{ijk,ij1} & \cdots & - & \cdots & L^{cyber}_{ijk,ijn_{ij}}, L^{phys}_{ijk,ijn_{ij}} \\ L^{cyber}_{ijn_{ij},ij1}, L^{phys}_{ijn_{ij},ij1} & \cdots & L^{cyber}_{ijn_{ij},ijk}, L^{phys}_{ijn_{ij},ijk} & \cdots & - \end{bmatrix} \end{matrix} \quad (2.8)$$

, де $L_{SubSyst_{ijb.ijq}}$ – зв'язок між елементами b і q компоненти $SubSyst_{ij}$, який описується двома (кібер та фізичною) складовими:

$$L_{SubSyst_{ijb,ijq}} = \left\{ L^{cyber}_{ijb,ijq}, L^{phys}_{ijb,ijq} \right\} \quad (2.9)$$

, при цьому цей зв'язок може бути описаний чотирма кодами:

$$L_{SubSyst_{ijb,ijq}} = \begin{cases} 00, \text{кібер та фізичні зв'язки відсутні;} \\ 01, \text{є тільки фізичний зв'язок;} \\ 10, \text{є тільки кібер зв'язок;} \\ 11, \text{є кібер та фізичні зв'язки.} \end{cases}$$

– Com – множина компонентів:

$$Com_k = \left\{ Com^{cyber}_k, Com^{phys}_k, L_{ijkp} \right\} \quad (2.10)$$

, де $Com^{cyber}_k = \left\{ Com^{cyber}_{kj}, j = 1,2, \dots, m \right\}$ – множина кіберкомпонентів, а $Com^{phys}_k = \left\{ Com^{phys}_{kc}, c = 1,2, \dots, m \right\}$ – множина фізичних компонентів, а m – їх кількість у Com_k. Прикладом компонентів можуть бути, наприклад, датчики, актуатори, навігаційні пристрої або додатки для БПЛА та інше. L_{ijkp} - зв'язок між елементами i, j, k, p інфраструктури багатофункційних флотів БПЛА:

$$L_{Com_{ijk}} = \begin{matrix} \\ \mathrm{El}_{ijk1} \\ \vdots \\ \mathrm{El}_{ijkp} \\ \vdots \\ \mathrm{El}_{ijkn_{ijk}} \end{matrix} \begin{matrix} \begin{matrix} \mathrm{El}_{ijk1} & \cdots & \mathrm{El}_{ijkp} & \cdots & \mathrm{El}_{ijkn_{ijk}} \end{matrix} \\ \begin{bmatrix} - & \cdots & L^{cyber}_{ijk1,ijkp}, L^{phys}_{ijk1,ijkp} & \cdots & L^{cyber}_{ijk1,ijkn_{ijk}}, L^{phys}_{ijk1,ijkn_{ijk}} \\ L^{cyber}_{ijkp,ijk1}, L^{phys}_{ijkp,ijk1} & \cdots & - & \cdots & L^{cyber}_{ijkp,ijkn_{ijk}}, L^{phys}_{ijkp,ijkn_{ijk}} \\ L^{cyber}_{ijkn_{ijk},ijk1}, L^{phys}_{ijkn_{ijk},ijk1} & \cdots & L^{cyber}_{ijkn_{ijk},ijkp}, L^{phys}_{ijkn_{ijk},ijkp} & \cdots & - \end{bmatrix} \end{matrix} \quad (2.11)$$

, де $L_{Com_{ijkb,ijkq}}$ – зв’язок між елементами b і q компоненти Com_{ijk} , який описується двома (кібер та фізичною) складовими:

$$L_{Com_{ijkb,ijkq}} = \{L^{cyber}_{ijkb,ijkq}, L^{phys}_{ijkb,ijkq}\} \quad (2.12)$$

, при цьому цей зв’язок може бути описаний чотирма кодами:

$$L_{Com_{ijkb,ijkq}} = \begin{cases} 00, \text{кібер та фізичні зв’язки відсутні;} \\ 01, \text{є тільки фізичний зв’язок;} \\ 10, \text{є тільки кібер зв’язок;} \\ 11, \text{є кібер та фізичні зв’язки.} \end{cases}$$

– El – множина елеметнів:

$$El_q = \{CybEl_q, PhyEl_q, L_{ijkp}\} \quad (2.13)$$

, де $CybEl_q = \{CybEl_{qj}, j = 1,2, \dots, m\}$ – множина кіберелементів, а $PhyEl_q = \{PhyEl_{qk}, k = 1,2, \dots, m\}$ – множина фізичних елементів, а m – їх кількість у El_i. Приклад елементів можуть бути апаратні та програмні складові пристроїв.

Такий підхід дає змогу більш точно та систематично відслідити та проаналізувати інфраструктуру системи багатофункційних флотів БПЛА з точки зору кібербезпеки та вразливостей перед комбінованими атаками [1].

Відповідно до ієрархічної моделі (рис. 2.3), взаємозв'язки в інфраструктурі є основними елементами, які з'єднують різні об'єкти системи. Ці зв'язки визначаються функціональними, структурними вимогами та вимогами безпеки системи. У таблиці 2.1 взаємозв'язки між об'єктами представлені у вигляді матриці, де елемент L(i,j) матриці вказує на наявність зв'язку між елементами i та j, як рядки і стовпці, які відповідають різним елементам інфраструктури. Згідно з рисунком 2.2, "1" - зв'язок існує, а "0" - зв'язку не існує. Наприклад, зв'язки існують між системами та підсистемами, між підсистемами та компонентами, між

компонентами та елементами. Однак прямих зв'язків між системами та компонентами або між підсистемами та елементами не існує.

Таблиця 2.1 – Матриця зв’язку об’єктів інфраструктури

	Система	*Підсистема*	*Компонент*	*Елемент*
Система	1	1	0	0
Підсистема	1	1	1	0
Компонент	0	1	1	1
Елемент	0	0	1	1

Об'єднуючи інфраструктуру (рис. 2.1) та ієрархічну модель (таблиця 2.1), можна припустити, що СБФ БПЛА, за першим прикладом, використовує зарядні станції, бази даних, хмарні сховища та центри зв'язку (таблиця 2.2). У цьому випадку координаційна матриця виглядає так:

Таблиця 2.2 – Приклад 1 матриці координації інфраструктури

	Зарядні станції	*Бази даних*	*Хмари*	*Центр зв'язку*
Зарядні станції	1	0	0	1
Бази даних	0	1	1	1
Хмари	0	1	1	1
Центр зв'язку	1	1	1	1

Як інший приклад, припустимо, що система використовує базу даних, центр зв'язку, оператора і супутник (таблиця 2.3). Тоді матриця агрегації буде виглядати наступним чином:

Таблиця 2.3 – Приклад 2 матриці координації інфраструктури

	Бази даних	*Центр зв'язку*	*Оператори*	*Супутники*
Бази даних	1	1	0	1
Центр зв'язку	1	1	1	1
Оператори	0	1	1	0
Супутники	1	1	0	1

Ці матриці показують зв'язки між різними елементами інфраструктури і позначені "1" - наявність зв'язків, "0" - відсутність зв'язків між об'єктами.

2.2 Модель загроз системи багатофункційних флотів БПЛА

Забезпечення кібербезпеки включає різноманітні заходи, технології та стратегії, спрямовані на захист інформаційних систем, мереж, програмного забезпечення та даних від несанкціонованого доступу та інших загроз [1,5,6]. Концептуальна модель безпеки (КМБ) визначає основні аспекти безпеки у системі або організації, служить основою для розробки та реалізації заходів безпеки, а також допомагає керувати ризиками та загрозами [7,8].

Схема керування інформаційною безпекою (ІБ) в СБФ БПЛА - це план для забезпечення безпеки інформації та даних у складній інфраструктурі флотів БПЛА. ІБ СБФ БПЛА включає заходи для захисту конфіденційності, цілісності, доступності та спостережності компонентів та елементів у системі флотів та мережах інфраструктури БПЛА [1,9], рисунок 2.4.

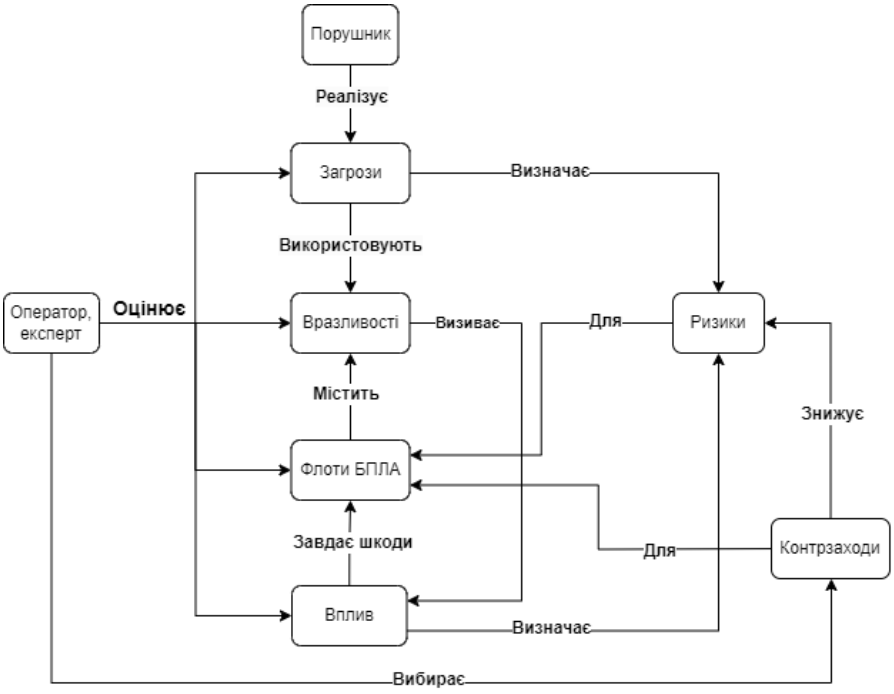


Рисунок 2.4 – Схема системи керування ІБ в СБФ БПЛА

Згідно стандарту 27001:2022 на рисунку 2.4 схема системи керування ІБ (СКІБ) СБФ БПЛА важлива для інфраструктури флотів та елементів системи, оскільки вона допомагає забезпечити захист інформації від загроз, які можуть призвести до витоку даних, порушення конфіденційності або втрати доступності важливої інформації. Вона допомагає відстежити процесс порушника, виявлення ризиків та витрати, а також допогає спланувати законодавчи вимоги та нормативні акти щодо захисту інформації [1,9].

На базі рисунка 2.1 - СБФ БПЛА та системи керування ІБ СБФ БПЛА була сформована класифікація загроз та модель загроз, рисунок 2.5, яка надає конкретні деталі та сценарії загроз, з якими СБФ БПЛА та самі БПЛА можуть стовкнутися. Побудова моделі загроз СБФ БПЛА дозволяє подивитися на проблему ІБ у системі та варіанти поведінки порушника. Завдяки аналізу, проведеному в статті [7], застосована у рисунку 2.5 КМБ СБФ БПЛА дозволяє відокремитися від впливів, які не залежать від дослідника, і водночас надає можливість протидіяти загрозам.

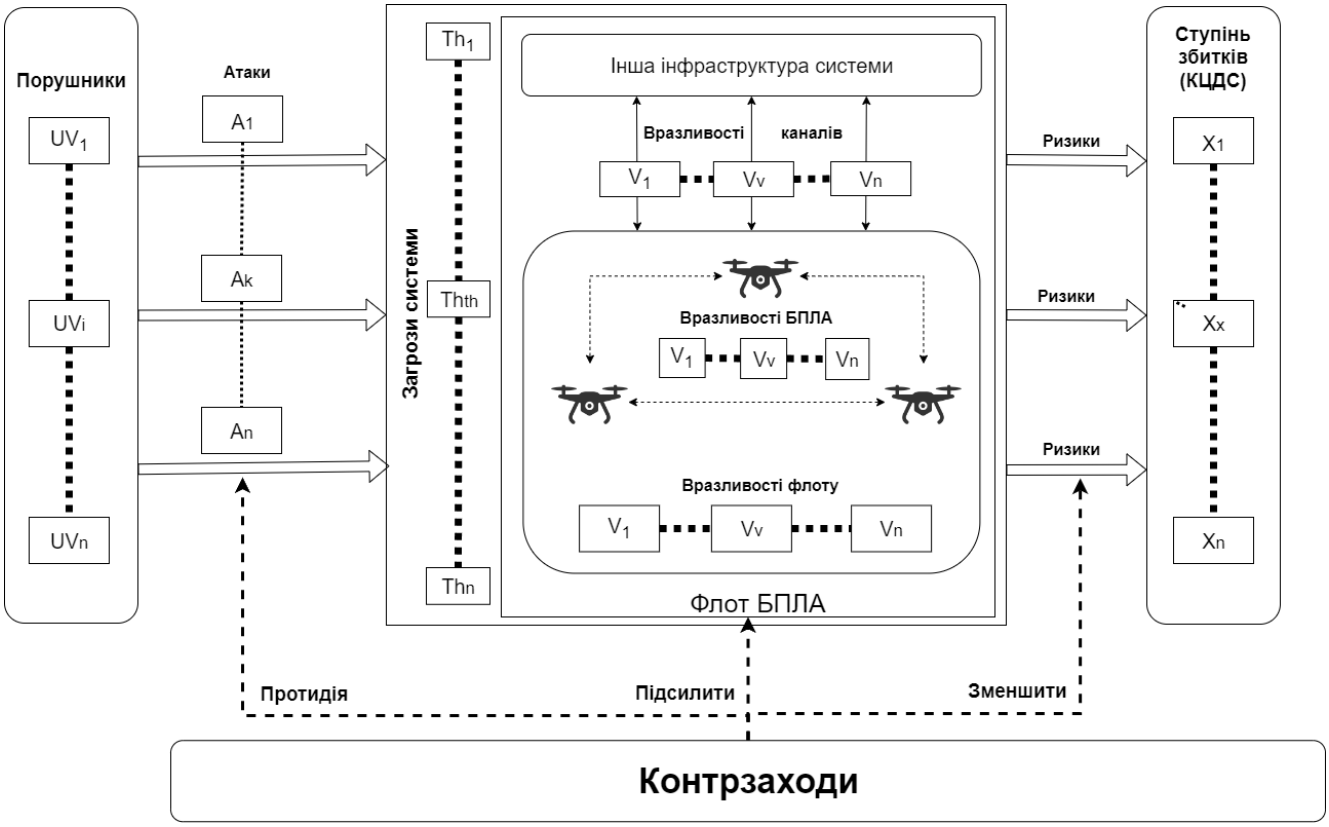


Рисунок 2.5 – Концептуальна модель безпеки СБФ БПЛА

У запропонованій моделі, згідно рисунку 2.5, ключовим елементом є БПЛА та флоти БПЛА, які в данній роботі були представлені згідно рисунку 2.2, як різні рівні та об'єкти інфрастурктури у системі багатофункційних флотів БПЛА.

Використання КМБ СБФ БПЛА дозволяє сформувати модель загроз СБФ БПЛА, яка дозволяє створити цілісну та ефективну систему безпеки, яка враховує різні аспекти безпеки та адаптується до змінних умов та загроз у СБФ БПЛА та її компонентах, як це зазначено у [7, 8].

Загальною метою моделі загроз і вразливостей є забезпечення цілісності, конфіденційності, спостереженості та доступності систем багатофункційного флоту БПЛА, розробка ефективних заходів захисту від потенційних загроз і вразливостей, а також забезпечення стійкості та безпеки системи в мінливих умовах експлуатації.

Згідно рисунку 2.2, де схема надає загальне уявлення про структуру інфраструктури багатофункційних флотів БПЛА та зазначає основні компоненти, що беруть участь у взаємодії та взаємозв'язку всієї системи та матриці множин, які наведені у таблиці 2.2, дає повноцінно ідентифікувати ключові місця у системі, де можуть виникати загрози безпеки та вразливості, забезпечуючи базу для подальшого аналізу та розробки стратегій кібербезпеки.

При цьому, зважаючи на широкий спектр компонентів у системі та їх взаємодію, розробка моделі загроз на основі виявлених уразливостей БПЛА - це модель, яка допоможе виявити важливі складові для забезпечення їх безпеки. Завдяки цьому, визначині потенційні загрози, які можуть виникнути внаслідок зловживання уразливостями системи управління БПЛА, можна буде обійти, уникнути чи знизити критичність і тяжкість їх.

2.2.1 Класифікація загроз в системі багатофункційних флотів БПЛА

У галузі БПЛА безпека і надійність є ключовими елементами, які потребують постійної уваги і захисту. У робочому середовищі БПЛА є безліч різних компонентів і систем, які піддаються впливу різних джерел загроз. Однак під час

забезпечення безпеки БПЛА необхідно враховувати безліч чинників, у даній роботі після проведеного аналізу наявних систем і рішень, було виділено такі основні елементи БПЛА, які використовуються в проектуванні моделі загроз флотів БПЛА, рисунок 2.6: канали управління, програмне забезпечення, апаратні засоби БПЛА і канали передачі даних (мультимедіа).

У відповідності до ДСТУ ISO/IEC 27001:2015 "Канали управління" можна описати як комунікаційні маршрути або засоби, що використовуються для передачі команд та інформації між системою управління та об'єктом управління. У загальному випадку канали управління забезпечують зв'язок між відправником команд і одержувачем, даючи змогу передавати дані, інструкції, параметри та іншу інформацію, необхідну для керування об'єктом [10, 11].

У контексті БПЛА, канали управління - це спеціально створені системи зв'язку, які забезпечують передачу команд і даних між оператором або автономною системою управління і БПЛА. Ці канали необхідні для встановлення зв'язку та обміну інформацією, даючи змогу операторові або системі управління контролювати і направляти політ БПЛА [12, 13].

Розглядання програмного забезпечення відіграє вирішальну роль у функціонуванні та управлінні БПЛА. Загрози для програмного забезпечення можуть включати в себе шкідливе ПЗ (віруси, трояни), несанкціонований доступ до коду, атаки на сервери та інші види кібератак.

У відповідності до ДСТУ ISO/IEC/IEEE 12207:2018 "Програмне забезпечення" (ПЗ) - це набір інструкцій і даних, які керують операцією комп'ютерної системи. Воно являє собою логічну складову комп'ютера, яка дає змогу виконувати різні завдання та функції. Програмне забезпечення може включати операційні системи, прикладне програмне забезпечення, утиліти та інші компоненти, які забезпечують функціональність і взаємодію з апаратним забезпеченням [14].

Програмне забезпечення для БПЛА - це спеціально розроблене ПЗ, яке керує і контролює роботу безпілотних літальних апаратів. Воно охоплює набір програм, які забезпечують керування польотом, навігацію, обробку даних із датчиків,

передачу даних та інші функції, необхідні для безпечного та ефективного функціонування БПЛА [14, 15], рисунок 2.6.

Низькорівневе ПЗ (Low-level Software) - це програмне забезпечення, яке працює безпосередньо з апаратним забезпеченням комп'ютерної системи. Воно забезпечує основні функції та взаємодію з апаратурою, як-от керування пам'яттю, робота з периферійними пристроями та введення-виведенням даних. Низькорівневе ПЗ часто пишеться мовами програмування, близькими до апаратної архітектури, і надає базові операційні можливості для більш високорівневого ПЗ [14, 15].

Високорівневе ПЗ (High-level Software) - це програмне забезпечення, що забезпечує більш абстрактний рівень функціональності та управління. Воно часто написане на більш високорівневих мовах програмування, таких як Python, Java, C++ та інших. Високорівневе ПЗ містить у собі прикладне програмне забезпечення, яке розв'язує конкретні задачі та надає користувацький інтерфейс для взаємодії з БПЛА [14, 15].

Устаткування БПЛА містить різні фізичні компоненти, такі як датчики, камери, системи навігації та інші системи. Загрози для обладнання БПЛА можуть включати фізичні пошкодження, несправності, заміну або підміну компонентів, крадіжку або втрату пристроїв.

Згідно з ДСТУ 9067:2021 "Апаратне обладнання" БПЛА являє собою фізичні компоненти, що складають і забезпечують роботу безпілотних літальних апаратів. Воно включає в себе різні елементи, такі як плати керування, датчики, актуатори, системи навігації, передавачі та інші компоненти, необхідні для виконання різних функцій і завдань під час польоту [16].

В даній роботі базову модель БПЛА буде визначатись як комбінацію шести окремих, але взаємозалежних систем: модуль збору даних, AHRS (система визначення висоти і курсу), NAV (навігаційна система), модуль управління, модуль реєстрації даних і модуль телеметрії [1, 17, 18]. Модуль системи зв'язку при такому підході окремо не показано, оскільки він охоплює всі модулі і через нього проходять всі вхідні/вихідні сигнали управління та передавання даних, рисунок 2.5.

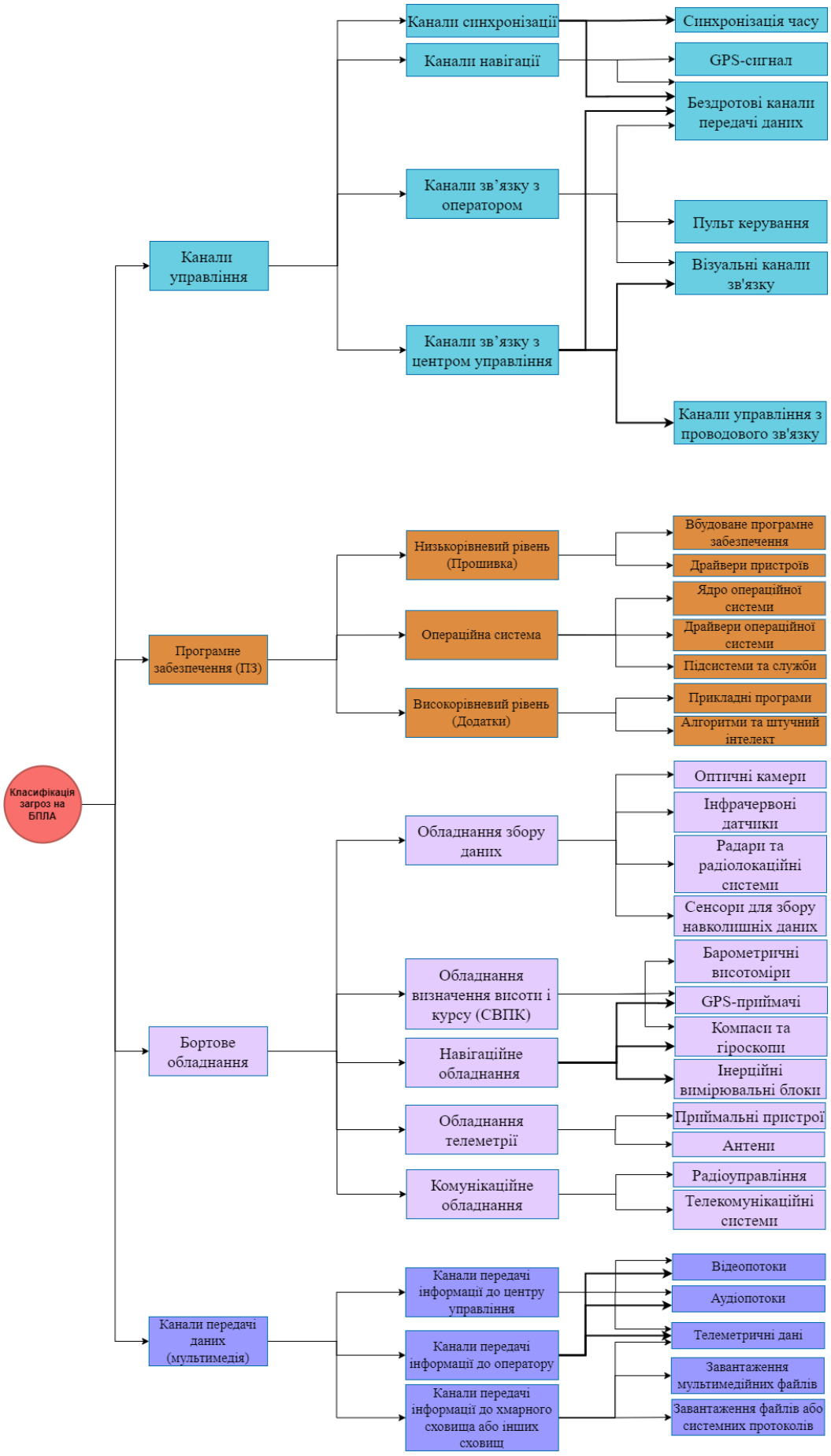


Рисунок 2.6 – Класифікація загроз в системі багатофункціональних флотів БПЛА

Канали передачі даних від БПЛА назад до оператора або системи управління відіграють важливу роль у забезпеченні зв'язку і передачі інформації про стан БПЛА, відео- і зображень, телеметрії та інших параметрів. Загрози для каналів передачі даних можуть включати в себе інтерференцію сигналу, блокування або відключення зв'язку, а також несанкціонований доступ і перехоплення даних.

Канал передачі даних (мультимедіа) в БПЛА є засобом зв'язку, який дозволяє передавати різні типи даних, включаючи аудіо, відео, зображення та інші мультимедійні дані між БПЛА і його наземною станцією або іншими пристроями [10, 12].

Відмінності апаратно та програмно каналів передачі даних від каналів управління полягають у їх призначенні та способі передачі інформації [10, 12]:

1. Канали управління використовують команд і сигнали управління, які необхідні для управління польотом і функціями БПЛА. Вони забезпечують зв'язок між наземною станцією або оператором та БПЛА для передачі керуючої інформації. Канали даних призначені для передачі мультимедійної інформації, такої як відео, аудіо або зображення, для спостереження, запису або інших цілей.

2. Канали управління зазвичай використовуються для передачі даних низької швидкості, таких як керуючі команди та параметри польоту. Вони працюють на надійних та низькочастотних радіозв'язках або за допомогою провідного зв'язку. Канали передачі даних вимагають більш високої пропускної спроможності передачі великого обсягу даних. Вони можуть використовувати більш високочастотні радіоканали, мережі передачі даних (наприклад, Wi-Fi, 4G/5G) або навіть спеціальні відеопотокові протоколи, як зображено на рисунку 2.6.

Щодо можливості фізичних можливостей каналу управління, то він також може служити каналом передачі даних (мультимедіа), це залежить від конкретних можливостей та конфігурації БПЛА та його системи зв'язку. У деяких випадках фізичний канал управління може бути здатний передавати мультимедійні дані, але це вимагає відповідної підтримки і функціональності.

Важливо, що для забезпечення стабільної та безпечної роботи БПЛА зазвичай використовуються окремі канали для управління та передачі даних

(мультимедіа). Це пов'язано з різними вимогами до пропускної спроможності, надійності та затримок, які можуть бути унікальними для кожного типу інформації та завдання БПЛА [10, 12], рисунок 2.6.

Ці чотири основні джерела загроз відіграють важливу роль у контексті безпеки БПЛА, що дає можливість ефективно запобігати і виявляти потенційні загрози через системний підхід і ретельно розробляти заходи безпеки [1].

2.2.2 Теоретико-множинний опис моделі загроз

Систематичний підхід до визначення загроз безпеці інформації передбачає реалізацію безперервного процесу, в рамках якого визначається сфера застосування процесу визначення загроз, ідентифікуються джерела загроз та загрози безпеці інформації, оцінюється можливість реалізації загроз безпеці інформації та ступінь можливої шкоди у разі такої реалізації, здійснюється моніторинг (періодичний перегляд) та переоцінка загроз безпеці інформації [1, 5, 6].

Модель загроз для багатофункційних флотів БПЛА визначають низку потенційних небезпек і несприятливих подій, які можуть вплинути на безпеку, надійність і функціонування системи. Згідно з Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, загрози варіюються від кібератак і порушень безпеки до фізичних небезпек, таких як стихійні лиха і несанкціонований доступ до фізичного обладнання [5, 6]. Ці загрози можуть бути зовнішніми або внутрішніми за своїм місцем знаходження. До зовнішніх загроз належать кібератаки хакерів, кібершпигунство, віруси та інші шкідливі програми, а також фізичні впливи, такі як збої в роботі електронних систем, електромагнітні перешкоди та інші небажані впливи на пристрої.

Моделювання загроз зазвичай передбачає аналіз потенційних загроз та їхнього впливу на різні компоненти системи. Кожна загроза оцінюється відповідно до ймовірності її виникнення та впливу на систему.

У якості джерел загроз безпеки системи багатофункційних флотів БПЛА будуть виступати суб’єкти (фізичні особи, організації, держави) або явища (техногенні аварії, стихійні лиха, інші). В даній роботі згідно нормативному акту [19] загрози будуть розділятися на наступні типи:

– антропогенні джерела (загрози): корумповані чиннки, хибна поведінка, соціальна інженерія, хакерські атаки;

– техногенні джерела (загрози): виробничі аварії, технічні вади, кіберінціденти;

– стихійні джерела (загрози): природні явища та катастрофи, екологічні проблеми, епідемії та пандемії.

Множина загроз може відрізнятися згідно акту [19], за такими ознаками:

– за метою реалізації (порушення конфіденційності, цілісності, доступності чи спостережності);

– за ступенем збитків, які можуть бути завдані внаслідок реалізації загрози;

– за типом прояву (збій, відмова, помилка, витік, модифікація, ін.);

– інше…

За суб'єктивною природою, можна класифікувати за ознакою навмисності (випадкові чи навмисні). За типом прояви можуть виражатися як у стихійних лихах, так і у відмові компонентів інфраструктури БПЛА, збоях обладнання, помилках персоналу та інше.

Для формування математичних множин та визначення позначень елементам моделі загроз використовуються наступні позначення:

– Th – загрози (threat), які можуть бути фізичними або кібернетичними.

– V – вразливості.

– I – порушники, які реалізують загрози безпеки системи.

Множина загроз (Th):

$$Th = \{Th^{cyber}, Th^{phys}\} \quad (2.14)$$

, де $Th^{cyber} = \{Th_j{}^{cyber}, j = 1,2,\dots,h\}$ – множина кіберзагроз, а $Th^{phys} = \{Th_k^{phys}, k = 1,2,\dots,h\}$ – множина фізичних загроз, а h – кількість загроз за двома видами Th_i, які можуть впливати на інфраструктуру многофункційних флотів БПЛА. Відповідно до цього, математична формула для моделі загроз може бути виражена наступним чином:

$$Th_i = I \times V \tag{2.15}$$

, де I_i визначає конкретного порушника, наприклад, тип порушника: $intruder\ (I) = \{I_1, I_2, \dots, I_n\}$, де V_v представляє конкретну вразливість, яку може бути використано порушником для реалізації загрози: $V = \{V_1, V_2, \dots, V_m\}$.

Індентифіковані загрози безпеки інформації підлягають нейтралізації, якщо вони є актуальними (Th^A) для інфраструктури системи та порушника який її буде використовувати, тобто є ймовірність реалізації загрози порушником з деяким потенціалом її реалізації:

$$Th^A = \begin{array}{c} \\ I_1 \\ \vdots \\ I_i \\ \vdots \\ I_n \end{array} \begin{array}{c} \begin{array}{cccccc} V_1 & \cdots & V_v & \cdots & V_m \end{array} \\ \begin{bmatrix} Th_{1,1} & \cdots & Th_{1,v} & \cdots & Th_{1,m} \\ \\ Th_{i,1} & \cdots & Th_{i,v} & \cdots & Th_{i,m} \\ \\ Th_{n,1} & \cdots & Th_{n,v} & \cdots & Th_{n,m} \end{bmatrix} \end{array} \tag{2.16}$$

Тоді побудувана матриця TS (загрози системи) між елементами інфраструктури та загрозами, згідно формулам 2.1 та 2.16 буде виглядати:

$$TS = \begin{array}{c} \\ Th_1^A \\ \vdots \\ Th_{th}^A \\ \vdots \\ Th_n^A \end{array} \begin{array}{c} \begin{array}{cccccc} Syst_1 & \cdots & Syst_i & \cdots & Syst_m \end{array} \\ \begin{bmatrix} TS_{1,i} & \cdots & TS_{1,i} & \cdots & TS_{1,m} \\ \\ TS_{th,1} & \cdots & TS_{th,i} & \cdots & TS_{th,m} \\ \\ TS_{n,1} & \cdots & TS_{n,i} & \cdots & TS_{n,m} \end{bmatrix} \end{array} \tag{2.17}$$

Таким чином, матриця TS відображає усі можливі комбінації зв'язків між елементами інфраструктури та загрозами з урахуванням параметрів, де TS_i – комбінації взаємозв'язків між системами інфраструктури та загрозами, $TS_{b,q}$ – зв’язок між елементами b і q компонентами Th та $Syst_i$, які описуються двома (кібер та фізичною) складовими:

$$TS_{b,q} = \left\{TS_{thb,iq}^{cyber}, TS_{thb,iq}^{phys}\right\} \quad (2.18)$$

при цьому цей зв’язок може бути описаний чотирма кодами:

$$TS_{b,q} = \begin{cases} 00, \text{відсутні загрози;} \\ 01, \text{є тільки фізичні загрози;} \\ 10, \text{є тільки кіберзагрози;} \\ 11, \text{є кібер та фізичні загрози.} \end{cases}$$

2.2.3 Вразливості багатофункційних флотів БПЛА

Моделювання вразливостей багатофункційних флотів безпілотних літальних апаратів (БПЛА) допомагає виявити можливість атак та шкоди для системи. Вразливості можуть бути знайдені в програмному та апаратному забезпеченні, комунікаційних протоколах, системах управління та інших аспектах інфраструктури. Аналіз компонентів системи допомагає виявити слабкі місця та потенційні вразливості, їх серйозність та потенційний вплив. Це важливо для розробки стратегій захисту та підвищення безпеки, включаючи усунення виявлених вразливостей. Моделі вразливостей також повинні враховувати людський фактор, такий як недостатня підготовка операторів або несанкціонований доступ до систем.

Вразливості можуть відрізнятися:

- внаслідок виникнення (якісна або кількісна недостатність);
- за ознакою навмисності (випадкова чи навмисна);
- за тривалістю існування (тимчасова чи систематична);

– за часом виникнення щодо етапу життєвого циклу (технологічна, експлуатаційна);

– за характером (програмна, апаратна, програмно-апаратна, адміністративна, організаційно-правова).

Множина вразливостей системи передбачає аналіз потенційних вразливостей компонентів системи та їхнього впливу на інфраструктуру. Для цього використовуються наступне відображення вразливостей (V):

$$V = \{V_1, V_2, \ldots, V_m\} \tag{2.19}$$

, де V_v представляє конкретну вразливість, яку може бути використано порушником для реалізації загрози.

Згідно моделі загроз за формулою 2.16, 2.17, матриця вразливостей буде виглядати:

$$TSV = \begin{array}{c} \\ V_1 \\ \vdots \\ V_v \\ \vdots \\ V_m \end{array} \begin{array}{c} \begin{array}{ccccccc} Syst_1 & \cdots & Syst_i & \cdots & Syst_m \end{array} \\ \begin{bmatrix} TSV_{1,1} & \cdots & TSV_{1,i} & \cdots & TSV_{1,m} \\ TSV_{v,1} & \cdots & TSV_{v,i} & \cdots & TSV_{v,m} \\ TSV_{m,1} & \cdots & TSV_{m,i} & \cdots & TSV_{m,m} \end{bmatrix} \end{array} \tag{2.20}$$

Таким чином, матриця TSV відображає усі можливі комбінації зв'язків між системами інфраструктури та вразливостями цієї системи, де TSV – конкретні вразливості на системі інфраструктури, при цьому цей зв’язок може бути описаний двома кодами:

$$TSV = \begin{cases} 0, \text{відсутні вразливості;} \\ 1, \text{є вразливості для кібер та фізичних зв}'\text{язків.} \end{cases}$$

2.3 Модель порушника для системи багатофункційних флотів БПЛА

Порушниками системи багатофункційних флотів БПЛА відповідно до українських стандартів та законодавства є організації або люди, які вчиняють дії, що суперечать законодавству України [20, 21, 11] у сфері використання та експлуатації багатофункційних флотів БПЛА. До них відносяться фізичні, юридичні особи або групи осіб, які не враховують специфіку використання БПЛА і тим самим порушують встановлені державою правові норми.

2.3.1 Визначення та класифікація порушників

Моделювання дій зловмисників проти систем багатофункційних флотів БПЛА відповідно до українських національних стандартів вимагає детального вивчення можливих загроз та аналізу впливу зловмисників на роботу системи. Відповідно до законодавства України [20, 21], зловмисники можуть бути класифіковані за наступними ознаками:

1. Тип порушника (Тип): Визначається, чи порушник є кібернетичним або фізичним. Ця класифікація допомагає розрізнити атаки, що відбуваються в електронному просторі, та атаки, які можуть мати фізичний вплив.

2. Мотивація порушника (Мотив): Відображає цілі або стимули, які спонукають порушника до атаки. Це може бути фінансовий зиск, розголошення конфіденційної інформації, політичні мотивації тощо.

3. Рівень навичок порушника (Навички): Відображає рівень технічних знань та вмінь, якими володіє порушник. Цей критерій може варіюватися від необізнаності до високої експертизи.

4. Джерело загроз (Джерело): Розглядає, чи порушник внутрішній (з організації) чи зовнішній (за її межами). Це може вказувати на можливі шляхи проникнення.

Припущення про цілі (мотивації) порушників робляться з урахуванням цілей та завдань інформаційної системи, виду оброблюваної інформації, а також з

урахуванням результатів оцінки ступеня можливих наслідків (збитків) від порушення конфіденційності, цілісності, спостережуваності чи доступності інформації.

Види порушника та його можливі цілі (мотивація) реалізації загроз безпеки багатофункційних флотів БПЛА наведено у таблиці 2.4.

Таблиця 2.4 – Класифікація порушників

Тип. пору ш.	№ ви ду	Види порушника	Можливі цілі (мотивація) реалізації загроз
1	2	3	4
Внутрішній	1	Робітники, що залучаються для монтажу та пусконалагодження	Обман і зловживання довірою, а також необачні дії, що завдають майнової шкоди.
	2	Особи, які обслуговують інфраструктуру інформаційних систем (адміністрація, охорона, прибиральники і т. д.)	Майнова шкода через обман чи недбалість. Ненавмисні, необережні чи некваліфіковані дії.
	3	Адміністратори інформаційної системи та адміністратори безпеки	Злочинне шахрайство та помста за минулі дії, виявлення і продаж вразливостей для отримання вигод, а також необережні або некваліфіковані дії, що завдають майнової шкоди.
Зовнішній	4	Спеціальні служби іноземних держав (блоків держав)	Завдання шкоди державі, окремим її сферам діяльності або секторам економіки. Дискредитація чи дестабілізація діяльності органів державної влади, організацій
	5	Терористичні, екстремістські угруповання	Завдання шкоди державі, окремим її сферам діяльності або секторам економіки. Вчинення терористичних актів. Ідеологічні чи політичні мотиви. Дестабілізація діяльності органів державної влади, організацій

Продовження таблиці 2.4

1	2	3	4
Зовнішній	6	Злочинні групи (кримінальні структури)	Заподіяння майнових збитків шляхом шахрайства чи іншим злочинним шляхом. Виявлення вразливостей з метою їх подальшого продажу та отримання фінансової вигоди
	4	Зовнішні суб'єкти (фізичні особи), колишні працівники (користувачі)	Ідеологічні чи політичні мотиви. Виявлення вразливостей з метою їх подальшого продажу та отримання фінансової вигоди. Помста за раніше вчинені дії
	8	Конкуруючі організації	Отримання конкурентних переваг. Заподіяння майнової шкоди шляхом обману чи зловживання довірою.
	9	Розробники, виробники, постачальники програмних, технічних та програмно-технічних засобів	Впровадження додаткових функцій у програмне забезпечення чи програмно-технічні засоби на етапі розробки. Ненавмисні, необережні чи некваліфіковані дії.

При оцінці можливостей порушників необхідно виходити з умов, що для підвищення своїх можливостей порушники 4 виду можуть вступати в змову з порушниками 6, 7, 8, 9, 1, 2 та 10 видів. Порушники 5 види можуть вступати в змову з порушниками 7, 1, 2, та 3 видів. Порушники 6 види можуть вступати в змову з порушниками 7, 1, 2, 3 видів. У разі прийняття таких припущень цілі (мотивація) та можливості порушників підлягають об'єднанню.

Можливості кожного виду порушника щодо реалізації загроз безпеці інформації характеризуються його потенціалом. Потенціал порушника визначається компетентністю, ресурсами та мотивацією, необхідними для реалізації загроз безпеці.

В залежності від потенціала, який потрібен для реалізації загроз безпеки інформації, відповідно до [5, 19, 20], порушники розділяються на:

– порушники з низьким потенціалом, які можуть використовувати у своїх атаках лише інформацію з загальнодоступних джерел. До порушників з низьким

потенціалом належать усі "зовнішні" сторони, а також внутрішній персонал і користувачі системи.

– порушники з середнім потенціалом здатні самостійно аналізувати код прикладного програмного забезпечення, знаходити та використовувати вразливості. До таких зловмисників належать терористи, злочинні угруповання, конкуруючі організації, системні адміністратори та розробники програмного забезпечення.

– порушники з високим потенціалом здатні створювати закладки в системі програмного та апаратного забезпечення, проводити спеціалізовані дослідження та використовувати спеціалізовані інструменти для проникнення та вилучення інформації. Такими злочинцями є виключно іноземні спецслужби.

2.3.2 Теоретико-множинний опис моделі порушника

Модель порушника передбачає аналіз потенційних порушників системи та їхнього впливу на інфраструктуру. Для цього використовуються наступні математичні представлення [1]:

– I (intruder) - множина можливих порушників.

– A - множина можливих атак, які використовує порушник.

Множина можливих порушників: $I = \{I_1, I_2, \ldots, I_n\}$, де I_i визначає конкретного порушника, наприклад, тип порушника.

Кожний порушник, це декартове множення:

$$I_i = \mathrm{A} \times Syst \tag{2.21}$$

, де A - множина способів реалізації загроз (атаки) (A): $\mathrm{A} = \{\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_k\}$, $Syst$ - множина об'єктів впливу, тобто інфраструктура БПЛА за рисунком 2.1 (Syst): $Syst = \{Syst_\mathrm{i}, \mathrm{i} = 1,2, \ldots, m\}$. Тут A представляє метод чи спосіб, які можуть використовувати порушники для реалізації загроз. Кожна $Syst$ вказує на конкретний флот БПЛА в системі, на який може бути спрямована реалізація загрози:

$$I_i = \begin{matrix} \\ \mathrm{A}_1 \\ \vdots \\ \mathrm{A}_k \\ \vdots \\ \mathrm{A}_n \end{matrix} \begin{matrix} \begin{matrix} Syst_1 & \cdots & Syst_i & \cdots & Syst_m \end{matrix} \\ \begin{bmatrix} I_{1,1} & \cdots & I_{1,i} & \cdots & I_{1,m} \\ \\ I_{k,1} & \cdots & I_{k,i} & \cdots & I_{k,m} \\ \\ I_{n,1} & \cdots & I_{n,i} & \cdots & I_{n,m} \end{bmatrix} \end{matrix} \tag{2.22}$$

2.4 Модель атак на системи багатофункційних флотів БПЛА

Атаки на СБФ БПЛА - це намагання незаконних суб'єктів (зловмисників, хакерів тощо) отримати незаконний доступ до інформаційних, фізичних або функціональних компонентів системи БПЛА з метою завдати шкоди або отримати користь. Атаки можуть включати кібернетичні та фізичні методи для досягнення своєї мети.

2.4.1 Класифікація атак

Класифікація комбінованих атак на СБФ БПЛА може бути здійснена відповідно до декількох аспектів, що охоплюють характеристики цих атак та їхні цілі [1, 22]. Нижче наведена запропонована класифікація, рисунок 2.7:

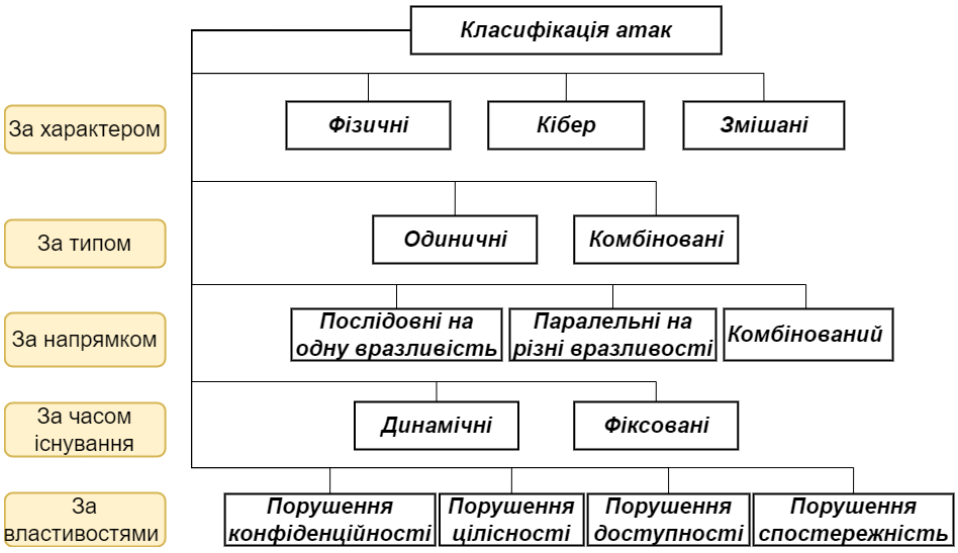


Рисунок 2.7 – Класифікація атак на систему багатофункціональних флотів БПЛА

Цю класифікацію також можна розділити наступним чином.

– За типом атак:

1. Комбіновані фізичні та кібернетичні атаки: ця категорія охоплює атаки, які поєднують фізичні дії з кібернетичними компонентами. Наприклад, фізичне пошкодження обладнання може поєднуватися з кібератаками на системи управління або навігації.

2. Комбіновані кібер-фізичні атаки: ця категорія поєднує кібератаки з фізичними наслідками. Наприклад, зловмисник може здійснити кібератаку з метою зміни кінематичних параметрів БПЛА, що призведе до фізичного зіткнення або аварії.

– За впливом:

1. Фізичні та кібердестабілізуючі атаки: атаки, що спричиняють фізичні порушення або дисфункції, можуть поєднуватися з кібератаками для посилення їхнього впливу.

2. Шпигунство та кібератаки: комбіновані атаки можуть бути спрямовані на витік конфіденційної інформації, а кіберінструменти можуть використовуватися для отримання та передачі цієї інформації.

– Інше.

Ця класифікація може бути використана для розуміння різних аспектів комбінованих атак на СБФ БПЛА та розробки політики безпеки.

2.4.2 Теоретико-множинний опис моделі фізичних і кібератак

Моделі атак на СБФ БПЛА передбачають поділ атак на дві основні категорії: фізичні атаки та кібератаки. Як було вище зазначено в формулі 2.22: A - множина способів реалізації загроз (атаки) (A): $A = \{A_1, A_2, \ldots, A_k\}$.

Фізичні атаки включають спроби вплинути на інфраструктуру флотів БПЛА шляхом проникнення або маніпулювання фізичними об'єктами. Модель фізичної

атаки можна описати наступним чином: $A^{phys} = \{A_1^{phys}, A_2^{phys}, \ldots, A_k^{phys}\}$, де A^{phys} - множина можливих фізичних атак.

Узагальнюючи, комплекс фізичних атак (A^{phys}) може бути представлений як декартовий добуток різних фізичних атак (A_k^{phys}) і множини об'єктів впливу, тобто фізичних компонентів флоту БПЛА ($Syst_i$):

$$A^{phys} = \begin{array}{c} \\ A_1^{phys} \\ \vdots \\ A_k^{phys} \\ \vdots \\ A_n^{phys} \end{array} \begin{array}{c} \begin{array}{cccccc} Syst_1 & \cdots & Syst_i & \cdots & Syst_m \end{array} \\ \begin{bmatrix} A_{1,1}^{phys} & \cdots & A_{1,i}^{phys} & \cdots & A_{1,m}^{phys} \\ A_{k,1}^{phys} & \cdots & A_{k,i}^{phys} & \cdots & A_{k,m}^{phys} \\ A_{n,1}^{phys} & \cdots & A_{n,i}^{phys} & \cdots & A_{n,m}^{phys} \end{bmatrix} \end{array} \quad (2.23)$$

З цього виходить, що модель фізичного нападу може бути виражена наступним чином: $A^{phys} = \{A_k^{phys} \times Syst_i \mid A_k^{phys} \in A^{phys}, Syst_i \in Syst\}$.

Кібератаки - це зловмисне втручання з метою пошкодження або отримання незаконного доступу до інформаційної та комп'ютерної інфраструктури флоту БПЛА. Модель кібератаки можна описати наступним чином: $A^{cyber} = \{A_1^{cyber}, A_2^{cyber}, \ldots, A_k^{cyber}\}$, де A^{cyber} - множина можливих кібератак.

Узагальнюючи, комплекс кібератак (A^{cyber}) може бути представлений, як у формулі 2.23:

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

З цього виходить, що модель кібернападу може бути виражен наступним чином: $A^{cyber} = \{A_k^{cyber} \times Syst_i \mid A_k^{cyber} \in A^{cyber}, Syst_i \in Syst\}$.

Деякі атаки поєднують фізичні та кібер-елементи для досягнення максимального ефекту:

$$CombA_{ij} = \mathrm{A}_k^{cyber} \cup \mathrm{A}_k^{phys}, \quad (2.25)$$

$$Comb\mathrm{A} = \{CombA_{ij} \mid \mathrm{A}_k^{cyber} \in \mathrm{A}^{cyber}, \mathrm{A}_k^{phys} \in \mathrm{A}^{phys}\} \quad (2.26)$$

2.4.3 Сценарії комбінованих атак

Комплексний сценарій атак - це складна комбінація різних типів атак і методів експлуатації, які зловмисники використовують для пошкодження таких систем, як багатофункційні флоти БПЛА, і досягнення своїх цілей. У таких сценаріях зловмисники використовують комбінацію різних атак і вразливостей, щоб збільшити ймовірність успішної атаки.

Комбіновані сценарії атак потрібні:

1. Підвищення ефективності: комбінування різних атак може збільшити ймовірність досягнення цілей атаки або заподіяння значної шкоди системі.

2. Обхід захисту: зловмисники можуть використовувати різні атаки, щоб обійти захист або вразливості, які можна відключити окремо.

3. Комбінація вразливостей: зловмисники можуть використовувати декілька вразливостей одночасно, щоб отримати доступ до системи або провести атаку.

4. Складність виявлення: комбіновані атаки може бути складніше виявити і протистояти їм, оскільки вони можуть використовувати різні канали атаки і залишати менше слідів.

Комбінований сценарій атаки на СБФ БПЛА відноситься до ситуації, коли зловмисник використовує як кібер-, так і фізичні атаки і комбінує їх для отримання контролю, заподіяння шкоди або витоку інформації.

Види сценаріїв комбінованих атак:

– сценарії комбінованих атак на одну вразливість: у цьому сценарії зловмисник використовує кілька різних атак або експлойтів на одну й ту саму

вразливість, щоб цю вразливість можна було ефективно використати або нейтралізувати.

– сценарії комбінованих атак на різні вразливості: У цьому сценарії зловмисник може запустити паралельні атаки на різні вразливості в системі, збільшуючи можливості для вторгнення і нанесення шкоди.

Всі ці сценарії можуть бути використані зловмисниками з різних причин, таких як економічна вигода, політичні цілі, шпигунство та саботаж та багато іншого.

2.5 Оцінка ризиків (критичності) кібератак на системи багатофункційних флотів БПЛА

Для оцінки ступеня можливої шкоди від загрози безпеки БПЛА визначаються можливий результат реалізації загрози безпеки БПЛА в СБФ, вид збитків, до якого може призвести реалізація загрози безпеці, ступінь наслідків реалізації загрози безпеці БПЛА кожному за виду шкоди, згідно нормативнім документам за [5, 19, 20, 22].

2.5.1 Визначення складових критичності

Як результат реалізації загрози безпеки багатофункційних флотів БПЛА та саміх БПЛА розглядаються безпосередній чи опосередкований вплив на конфіденційність, цілісність, доступність та спостережність (КЦДС), що міститься в СБФ БПЛА.

Безпосередній вплив на 4 властивості інформації можливий в результаті прямої загрози безпеці інформації. Тому аналіз та оцінку потенційних наслідків атак на різні аспекти безпеки, такі як КЦДС, для цього було використана система оцінки ризиків, яка включає різні метрики та критерії. Ступінь збитків для властивостей безпеки може бути оцінений за такими показниками [1]:

1. Конфіденційність: оцінює рівень ймовірності того, що конфіденційна інформація буде скомпрометована в результаті атаки. Шкала оцінювання варіюється від низького (мінімально конфіденційна інформація) до високого (критично конфіденційна інформація).

2. Цілісність: оцінює рівень потенційної модифікації або загрози цілісності інформації. Вона варіюється від низького (некритичні дані) до високого (критичні дані, які не повинні бути змінені або скомпрометовані).

3. Доступність: оцінює вплив атаки на доступність систем та інформації. Він може варіюватися від низького (короткочасна низька доступність) до високого (довготривала повна зупинка системи).

4. Спостережуваність: оцінює вимоги щодо ідентифікації і контролю, які можуть бути втрачені або знищені. Шкала оцінювання варіюється від низької (не має значення для зовнішнього світу) до високої (важлива спостережувана інформація).

Оцінка ризиків (критичності) атак на СБФ БПЛА визначаються відповідно до таблиці 2.5, де вплив загрози на кожну властивість безпеки (КЦДС) визначається окремо.

Таблиця 2.5 – Результат ризиків збитків інформаціїї для властивостей безпеки СБФ БПЛА

Властивості безпеки	Результат реалізації загроз безпеки флотів БПЛА	
	Не впливають	Впливають
1	2	3
Конфіденційність $X_{r1}^{К}$	Відсутня можливість несанкціонованого доступу, копіювання, надання або розповсюдження інформації внаслідок загроз інформаційної безпеки.	Внаслідок загроз інформаційної безпеки інформація може бути незаконно доступна, скопійована, надана або поширена.
Цілісність $X_{r1}^{Ц}$	Відсутність потенціалу для знищення або зміни інформації внаслідок загроз інформаційної безпеки	Інформація може бути знищена або змінена внаслідок загроз інформаційної безпеки

Продовження таблиці 2.5

1	2	3
Доступність $X_{r1}^{Д}$	Відсутня можливість блокування інформації внаслідок загроз інформаційної безпеки	Інформація може бути заблокована внаслідок загроз інформаційної безпеки.
Спостережність $X_{r1}^{С}$	Внаслідок реалізації загрози безпеки інформації відсутня можливість ідентифікації та контролю інформації	Внаслідок реалізації загрози безпеці інформації можлива зміна або знищення ідентифікації та контролю інформації

При визначенні ступеня можливої шкоди необхідно виходити з того, що залежно від цілей та завдань, які вирішуються СБФ БПЛА, видів оброблюваної інформації, вплив на КЦДС кожного виду інформації, що міститься в системі, може призвести до різних видів шкоди. При цьому для різних власників інформації та порушників будуть характерні різні види збитків.

2.5.2 Оцінювання ризиків при комбінованих атаках

Ступінь можливої шкоди від реалізації загрози безпеці даних багатофункційних флотів БПЛА визначається ступенем негативних наслідків від порушення КЦДС кожного виду інформації, що міститься в системі.

Кожному з цих показників було призначено символьний коефіцієнт відповідно до важливості властивостей безпеки для конкретної системи багатофункціональних флотів БПЛА, згідно таблиці 2.5.

У випадках, коли в системі обробляється два і більше видів інформації (службова таємниця, персональні дані, військова таємниця та інші види інформації, визначені законодавством України [20, 21]), вплив на КЦДС визначається окремо для кожного виду флотів БПЛА та саміх БПЛА, що міститься в системі (r, ... , m), визначається окремо для кожного виду, що міститься в системі.

Як єдина шкала вимірювання ступеня негативних наслідків будуть прийматися значення «незначні», «помірні» та «суттєві» негативні наслідки.

Порушення кожного порушника визначаються у зазначеній єдиній шкалі вимірювань ступіню негативних наслідків від порушення КЦДС даних багатофункційних флотів БПЛА та самих БПЛА стосовно всіх цілей та завдань, які вирішуються в системі.

Ступінь шкоди визначається експертним методом відповідно до таблиці 2.6.

Таблиця 2.6 – Ступінь збитків (КЦДС)

Ступінь збитку	Характеристика ступеню збитку
Високий	Внаслідок порушення однієї з властивостей безпеки інформації (КЦДС) можливі суттєві негативні наслідки. Флот БПЛА, БПЛА або оператор (власник доступу до флоту) не можуть виконувати поставлені на них функції та завдання.
Середній	Внаслідок порушення однієї з властивостей безпеки інформації (КЦДС) можливі помірні негативні наслідки. Флот БПЛА, БПЛА або оператор (власник доступу до флоту) не можуть виконувати хоча б одну з покладених на них функцій
Низький	Внаслідок порушення однієї з властивостей безпеки інформації (КЦДС) можливі незначні негативні наслідки. Флот БПЛА, БПЛА або оператор (власник доступу до флоту) можуть виконувати покладені на них функції з недостатньою ефективністю або виконання функцій можливе лише за допомогою додаткового інструментарію

Підсумковий ступінь можливої шкоди встановлюється за найвищими значеннями ступеня можливої шкоди, визначеними для КЦДС інформації кожного виду флотів БПЛА, БПЛА або системи зв’язку стосовно кожного виду шкоди.

$$X_r = \max(X_r^l)\,; l = \{\,\text{К}, \text{Ц}, \text{Д}, \text{С}\,\} \tag{2.27}$$

Відповідно до формули 2.19, про актуальність загрози безпеки даних флотів БПЛА та самих БПЛА для системи із заданими структурно-функціональними характеристиками та умовами функціонування приймається відповідно до таблиці 2.7.

Ця оцінка ризиків допомагає приймати рішення щодо впровадження заходів кібербезпеки та встановлення пріоритетів у захисті системи багатофункціональних флотів БПЛА від можливих кібератак.

Таблиця 2.7 – Визначення актуальності загрози за ступеню збитків

Ймовірність (можливість) реалізації загрози (Th^A)	Ступень ймовірного збитку (X_r)		
	Низький	Середній	Високий
Низкий	Низький	Низький	Середній
Середній	Низький	Середній	Високий
Високий	Середній	Високий	Високий

2.6 Висновок до другого розділу

У цій частині дисертаційної роботи досліджено та розроблено моделі оцінки кібербезпеки багатофункційного флоту БПЛА. Проаналізовано інфраструктуру такої системи та представлено у вигляді концептуальної схеми та ієрархічної моделі. Теоретико-множинний опис інфраструктури забезпечив розуміння її компонентів та їх взаємозв'язків.

Потім була розроблена модель загроз для СБФ БПЛА, включаючи класифікацію можливих загроз і розробку моделі порушника. Була розроблена математична модель вразливостей для цієї системи, яка показує як може бути використані зловмисниками вразливості та загрози для здійснення атак.

Розроблена модель порушника включає ідентифікацію та класифікацію зловмисників. Ця модель дає розуміння потенційних загроз для СБФ БПЛА.

В розділі представлена модель атак на такі системи, включаючи класифікацію атак і розробку моделей фізичних і кібернетичних атак. Також розглядаються комбіновані сценарії атак, які можуть використовувати різні методи для досягнення своїх цілей.

Оцінка ризику атак на СБФ БПЛА допомагає зрозуміти потенційні загрози, особливо у випадку комбінованих атак, і визначити важливість цих систем для кібербезпеки флотів БПЛА.

Література до першого розділу

1. Zemlianko H., Kharchenko V. Cybersecurity risk analysis of multifunctional UAV fleet systems: a conceptual model and IMECA-based technique. *Radioelectronic and Computer Systems*. 2023. № 4. С. 152–170. URL: https://doi.org/10.32620/reks. 2023.4.11.

2. ISO/IEC/IEEE 21839:2019 Systems and software engineering – System of systems (SoS) considerations in life cycle stages of a system. *ISO*. URL: https://www.iso.org/ru/standard/71955.html. (дата звернення: 05.03.2022).

3. ISO/IEC/IEEE 21840:2019 Systems and software engineering – Guidelines for the utilization of ISO/IEC/IEEE 15288 in the context of system of systems (SoS). *ISO*. URL: https://www.iso.org/ru/standard/71956.html. (дата звернення: 05.03.2022).

4. Сігорський В. П. Математичний апарат інженера. - Київ: Техніка, 1975. - 768 с.

5. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: Норм. док. системи техн. зах. інформації від 28.05.1999 р. № НД ТЗІ 1.1-002-99: станом на 28 груд. 2012 р. URL: https://tzi.com.ua/downloads/1.1-002-99.pdf (дата звернення: 03.11.2021).

6. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу: Норм. док. системи техн. зах. інформації від 28.05.1999 р. № НД ТЗІ 1.1-003-99. URL: https://tzi.ua/assets/files/1.1_003_99.pdf (дата звернення: 03.11.2021).

7. Pevnev, V., Tsuranov, M., Zemlianko, H., Amelina, O. (2021). Conceptual Model of Information Security. In: Nechyporuk, M., Pavlikov, V., Kritskiy, D. (eds) Integrated Computer Technologies in Mechanical Engineering - 2020. ICTM 2020.

Lecture Notes in Networks and Systems, vol 188. Springer, Cham. https://doi.org/10.1007/978-3-030-66717-7_14.

8. J. Geismann, C. Gerking, and E. Bodden, “Towards ensuring security by design in cyber-physical systems engineering processes // in Proceedings of the 2018 international conference on software and system process, 2018, pp. 123–127. URL: https://www.researchgate.net/publication/325373997_Towards_ensuring_security_by_design_in_cyber-physical_systems_engineering_processes (дата звернення: 08.05.2022).

9. ISO/IEC 27001:2022. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection. На заміну EN ISO/IEC 27001:2017; ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015; чинний від 2022-12-28. Вид. офіц. 3, 2022. 19 с.

10. ДСТУ В 7371:2020. Техніка авіаційна державної авіації. Апарати літальні безпілотні. Основні терміни та визначення понять. Класифікація. На заміну ДСТУ В 7371:2013 ; чинний від 2021-07-01. Наказ про прийняття НД: 2020-05-06 № 88. Вид. офіц. Україна : ДП «УкрНДНЦ», 2020. 21 с.

11. ДСТУ EN ISO/IEC 27001:2022. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. На заміну EN ISO/IEC 27001:2017, IDT; ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015, IDT ; чинний від 2023-12-31. Наказ про прийняття НД: 2022-12-28 № 285. Вид. офіц. Україна : ДП «УкрНДНЦ», 2022. 37 с.

12. ISO/IEC/IEEE 21450:2010 Information technology – Smart transducer interface for sensors and actuators – Common functions, communication protocols, and Transducer Electronic Data Sheet (TEDS) formats. *ISO*. URL: https://www.iso.org/ru/standard/54356.html (дата звернення: 06.08.2022).

13. ITU-R M.1796-2 Characteristics of and protection criteria for terrestrial radars operating in the radiodetermination service in the frequency band 8 500-10 680 MHz. *ITU-R Recommendations*. URL: https://extranet.itu.int/brdocsearch/_layouts/15/WopiFrame.aspx?sourcedoc=%7BA8A0C3D3-2095-4E3A-9AA1-668D4425E469%7D&file=R-REC-M.1796-2-201402-I!!MSW-E.docx&action=default&DefaultItemOpen=1 (дата звернення: 08.08.2023).

14. ДСТУ ISO/IEC/IEEE 12207:2018. Інженерія систем і програмних засобів. Процеси життєвого циклу програмних засобів (ISO/IEC/IEEE 12207:2017, IDT). На заміну ДСТУ ISO/IEC 12207:2016 ; чинний від 2018-08-15. Наказ про прийняття НД: 2018-08-06 № 261. Вид. офіц. Україна : ДП «УкрНДНЦ», 2018. 156 с.

15. ISO/IEC/IEEE 15288:2023 Systems and software engineering – System life cycle processes. *ISO*. URL: https://www.iso.org/ru/standard/81702.html (дата звернення: 22.06.2023).

16. ДСТУ 9067:2021. Дизайн і ергономіка. Комплекси безпілотних повітряних суден. Правила оцінювання рівня якості. Чинний від 2021-09-01. Наказ про прийняття НД: 2021-02-16 № 54. Вид. офіц. Україна : ДП «УкрНДНЦ», 2021. 7 с.

17. Austin R. Unmanned aircraft systems: UAVs design, development and deployment. Reston, Va: American Institute of Aeronautics and Astronautics, 2010. 332 p.

18. A Survey of Indoor and Outdoor UAV-based Target Tracking Systems: Current Status, Challenges, Technologies, and Future Directions / M. Alhafnawi та ін. *IEEE Access*. 2023. С. 1. URL: https://doi.org/10.1109/access.2023.3292302 (дата звернення: 08.08.2023).

19. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу: Норм. док. системи техн. зах. інформації від 28.05.1999 р. № НД ТЗІ 2.5-004-99: станом на 28 груд. 2012 р. URL: https://tzi.com.ua/downloads/2.5-004-99.pdf (дата звернення: 10.04.2022).

20. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2469-19 (дата звернення: 08.08.2023).

21. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2163-19. (дата звернення: 08.08.2023)

22. ДСТУ ISO/IEC TR 20004:2017 Інформаційні технології. Методи захисту. Уточнений аналіз вразливості програмного забезпечення згідно з ISO/IEC 15408 та

ISO/IEC 18045 (ISO/IEC TR 20004:2015, IDT). *БУДСТАНДАРТ Online - нормативні документи будівельної галузі України*. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=74704 (дата звернення: 08.06.2023).

РОЗДІЛ 3. РОЗРОБЛЕННЯ МЕТОДУ АНАЛІЗУ КІБЕРЗАГРОЗ, НАСЛІДКІВ ТА КРИТИЧНОСТІ ОДИНИЧНИХ І КОМБІНОВАНИХ АТАК НА АКТИВИ КІБЕРФІЗИЧНОЇ СИСТЕМИ БАГАТОФУНКЦІЙНИХ ФЛОТІВ БПЛА

3.1 Модель IMECA аналізу системи багатофункційних флотів БПЛА

Під час проведеного дослідження, що включає розроблення моделей та ієрархічного поділу безпеки СБФ БПЛА в розділі 2, було здійснено аналіз видів і наслідків загроз, а також виявлених вразливостей відповідно до розділу 1. Результати цього аналізу подано у формі таблиці, у якій рядки відображають виявлені загрози та вразливості, а стовпчики містять інформацію про причини, вплив і наслідки цих загроз із вразливостями, а також імовірність їх виникнення та ступінь серйозності наслідків.

Очевидно, що залежно від об'єкта аналізу розмірність такої IMECA-таблиці істотно варіюватиметься. Для СБФ БПЛА, до яких відносяться системи моніторингу, системи повітряної розвідки та інші, що налічують десятки і навіть сотні різноманітних підсистем, компонентів і десятки тисяч елементів, розмірність IMECA-таблиці може істотно утруднити або зовсім унеможливити практичне використання такого методу.

Крім того, було розширено спектр характеристик IMECA-таблиці, що впливають на визначення ступеня їх критичності, загроз і вразливостей, які переходять в атаки на систему, а також їхні наслідки (під час оцінювання критичності атак ураховують лише ймовірність виникнення і тяжкість її наслідків, причому остання характеристика потребує подальшого уточнення). Нарешті, найважливішим завданням є використання отриманих унаслідок аналізу даних про атаки, їхні загрози та вразливості для розв'язання завдання забезпечення необхідного рівня кібербезпеки розроблюваної системи.

Для вдосконалення методу аналізу видів і наслідків атак для СБФ БПЛА в цьому розділі розв'язуються такі завдання:

- формалізація моделі IMECA-аналізу та шляхів її розширення;

- застосування ієрархічного підходу до оцінки та перехід від "плоскої" IMECA-таблиці до вкладеної ієрархії таких таблиць;

- врахування додаткових чинників під час оцінювання критичності атак, загроз і вразливостей, характерних для СБФ БПЛА;

- розроблення методики кількісного оцінювання критичності атак, загроз і вразливостей з урахуванням ієрархічної вкладеності IMECA-таблиці;

- розроблення методу зниження критичності відмов із використанням етапів оптимізації вибору контрзаходів і забезпечення стійкості системи до атак, загроз і вразливостей.

3.1.1 Елементи IMECA таблиці для аналізу кібербезпеки СБФ БПЛА

В сучасному середовищі кібербезпеки систем безпілотних літальних апаратів (СБФ БПЛА) одним із ключових інструментів аналізу є IMECA таблиця.

Згідно моделям порушника, загроз, та вразливостей у розділі 2, було виявлено такі елементи IMECA-таблиці:

– порушник**:** ідентифікація особи чи групи, які можуть здійснювати атаки на СБФ БПЛА;

– потенціал порушника**:** оцінка здатності потенційного порушника виконати атаки;

– характер загрози: визначення характеру загрози, яка може бути штучною або природною;

– загроза: конкретний вид проблеми для інфраструктури СБФ БПЛА;

– вразливості: ідентифікація слабких місць в системі, які можуть бути використані порушником;

– атака: опис дій, які порушник може виконати, використовуючи вразливості для впливу на систему;

– властивості безпеки: оцінка конфіденційності, цілісності, доступності та спостережності у контексті загрози та вразливостей, які використовує порушник для реалізації атаки на СБФ БПЛА;

– наслідки: потенційні результати атаки на інфраструктуру СБФ БПЛА;

– критичність атаки: оцінка ймовірності, тяжкості та ризику атаки перед застосуванням контрзаходів;

– контрзаходи: сукупність заходів, які призначені для запобігання або пом'якшення наслідків атаки;

– критичність після використання контрзаходів: переоцінка ймовірності, тяжкості та ризику після застосування контрзаходів.

Ці елементи становлять основу для аналізу та оцінки рівня кібербезпеки системи безпілотних літальних апаратів, дозволяючи виявити та вирішити проблеми, пов'язані з потенційними загрозами та атаками на цю систему.

Елементи IMECA таблиці є взаємопов'язаними і взаємозалежними компонентами, що спільно дозволяють оцінити ризики та визначити стратегії контрзаходів в контексті кібербезпеки СБФ БПЛА.

1. Потенціал порушника і характер загрози визначаються конкретними загрозами, які можуть бути штучними або природними. Ці елементи відображають потенційність та тип можливих атак.

2. Загроза і вразливості є основою для подальшого аналізу. Загроза визначає конкретний вид потенційної небезпеки, в той час як вразливості показують слабкі місця в системі, які можуть бути використані порушником для атаки.

3. Атака і властивості безпеки залежать від зазначених загроз і вразливостей. Опис атаки пов'язаний з ідентифікацією потенційних наслідків, тоді як властивості безпеки відображають рівень конфіденційності, цілісності, доступності та спостережності.

4. Наслідки і критичність атаки визначаються атакою та властивостями безпеки. Наслідки вказують потенційні наслідки атаки, а критичність враховує ймовірність і тяжкість наслідків.

5. Контрзаходи і критичність після контрзаходів залежать від критичності атаки. Контрзаходи визначаються для зменшення ризику атаки, тоді як критичність після контрзаходів враховує ефективність застосованих заходів у пониженні наслідків атаки.

3.1.2 Структура IMECA таблиці

Під час аналізу та узагальнення досвіду розробки інфраструктури систем безпілотних літальних апаратів (СБФ БПЛА) та управління її компонентами виявлено необхідність проведення аналізу загроз, уразливостей та атак на систему на ранніх етапах життєвого циклу СБФ БПЛА. Це дозволяє внести відповідні методи та засоби ще на етапі визначення вимог і проектування системи, спрямовані на забезпечення кібербезпеки, оптимізацію контрзаходів та скорочення часу на відновлення після кібератак. Такий підхід відповідає сучасним концепціям розумних технологій і міст, а також політики безпеки цифрової інфраструктури, що сприяє значній економії часу та ресурсів на забезпечення кібербезпеки систем. Пропонується розширити застосування IMECA-аналізу на ранні етапи розробки, щоб вчасно виявляти можливі загрози та їх вплив на систему.

Такий підхід може виявитися неприйнятним для систем моніторингу критичного застосування або військового, оскільки реалізація ефективних методів запобігання кібератакам і зниження тяжкості їхніх наслідків може бути неможлива через ухвалені раніше схемотехнічні рішення, стандартизовану політику або ж потребуватиме додаткових часових і фінансових ресурсів.

Пропонований підхід передбачає виконання аналізу видів, причин і наслідків кібератак на етапах (рис. 3.1): визначення загроз, уразливостей; визначення структури інфраструктури СБФ БПЛА; варіанти реалізації кібератак на ці елементи СБФ БПЛА.

На першому етапі об'єктом аналізу є набір загроз і вразливостей елементів інфраструктури СБФ БПЛА. У цьому випадку, рядками IMECA-таблиці є окремі загрози та вразливості системи, що призводять до виникнення атак на СБФ БПЛА.

Рисунок 3.1 – Етапність застосування IMECA-аналізу

На цьому етапі визначаються варіанти виникнення загроз і вразливостей, які приводять до атак та їхніх наслідків для системи, а також для проєктування оптимізованих кроків застосування контрзаходів для системи, для зменшення можливих наслідків для СБФ БПЛА.

На другому етапі проводиться класичний аналіз IMECA, який охоплює системи, підсистеми та компоненти інфраструктури СБФ БПЛА, що стають об'єктом кібератак через загрози та вразливості. Результати попереднього етапу використовуються для визначення вимог і верифікації наслідків атак. Нарешті, після вибору варіанту атаки на окремі складові системи або інфраструктури СБФ БПЛА, проводиться детальний аналіз відповідних апаратних і програмних засобів, враховуючи особливості загроз та вразливостей. Також уточнюється оцінка критичності атак та вибираються оптимізаційні контрзаходи для відновлення системи.

3.1.3 Ієрархія IMECA таблиць

Ієрархізація аналізу видів причин та наслідків реалізації атак може бути виконана відповідно до природного поділу складних систем на підсистеми, компоненти, апаратні компоненти та програмні модулі. Результати такого аналізу

(далі Hierarchical-IMECA або H-IMECA) будуть ієрархією вкладених IMECA-таблиць. Пропонується використовувати трирівневу ієрархію (рис. 3.2); у кожному даному випадку кількість ієрархічних рівнів може бути уточнено.

Таблиця верхнього рівня розглядає атаки окремих систем інфраструктури СБФ БПЛА. Таблиця першого рівня вкладеності розглядає атаки окремі підсистеми кожної конкретної системи. Таблиця другого рівня вкладеності розглядає атаки на окремі компоненти кожної підсистеми, як це показано на рис. 3.2.

Класична IMECA-таблиця є списком VT, який може бути представлений безліччю V векторів (числом рядків таблиці - елементів системи):

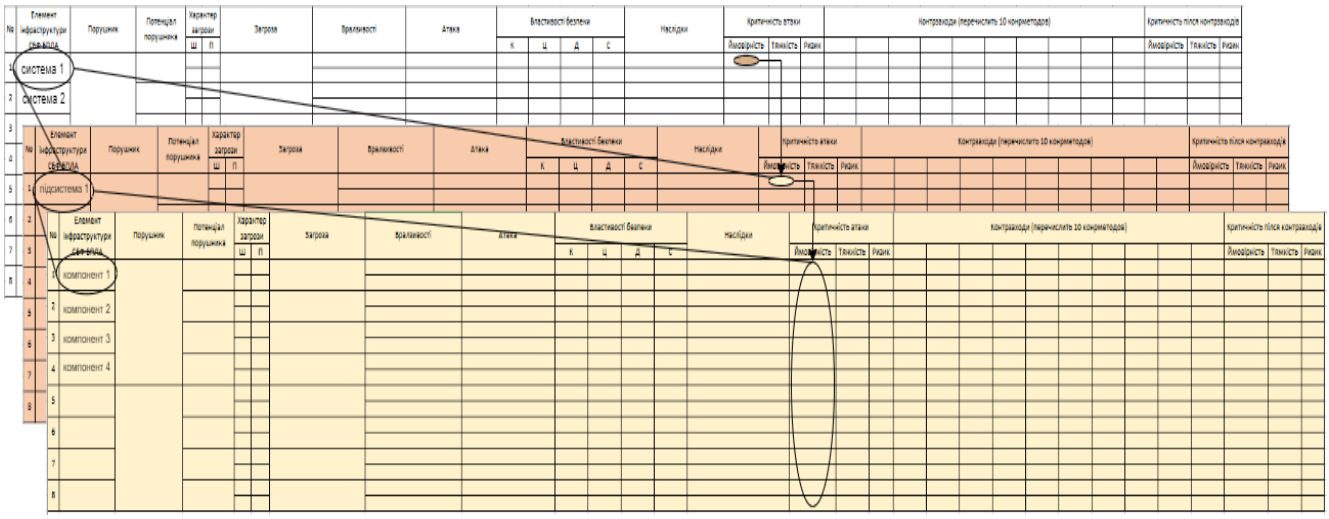


Рисунок 3.2 – Ірархія IMECA-таблиць

$$VT_1 =< I_v, VP_v, Th_v, V_v, A_v, P_v, S_v, X_{r_v} >_{v=1}^{V} \quad (3.1)$$

, де I_v – порушник, VP_v – потенціал порушника, Th_v – загроза, V_v – вразливість, A_v – атака, P_v – ймовірніть (probability) та S_v – тяжкість (severity), які які задаються шкалою за визначенням від високого до низького, та X_r – наслідки системи.

Модернізація моделі VT може бути виконана у частині розширення (уточнення або доповнення):

– оцінюваних – об'єктів (елемент-системи, підсистеми, компоненти);

– потенціал порушника – свідомість та можливості, які може використовувати зловмисник;

– характер загрози – штучна або природна властивість;

– властивості безпеки: оцінка конфіденційності, цілісності, доступності та спостережності;

– наслідки, які відбуваються після атаки відповідно до властивостей кібербезпеки;

– контрзасоби;

– критичніть після контрзаходів, для виявлення наскільки змінилась критичніть після атак.

3.1.4 Особливості побудови IMECA таблиць для властивостей кібербезпеки

IMECA таблиці для властивостей кібербезпеки (конфіденційності, цілісності, доступності та спостережності) відрізняються своєю структурою та специфікою, оскільки вони спрямовані на оцінку та аналіз рівня захищеності системи від різних кіберзагроз. Згідно розділу 2, щоб корректно оцінювати властивості кібербезпеки при різних атаках на системи, підсиситеми, компоненти ірархічної моделі СБФ БПЛА, треба пам’ятати особливості кібербезпеки для IMECA-таблиць.

1. Визначення критеріїв кожної властивості: перш за все, необхідно чітко визначити критерії для кожної з властивостей кібербезпеки: що означає конфіденційність, цілісність, доступність та спостережність для даної системи.

2. Оцінка впливу атак на властивості кібербезпеки: IMECA таблиці мають поля для оцінки впливу кожної атаки на властивості кібербезпеки. Ці показники враховують різні аспекти, для подальшого відображення наслідків та критичності СБФ БПЛА та її елементів.

3. Врахування різноманітності загроз: таблиці IMECA враховують широкий спектр потенційних кіберзагроз, які можуть вплинути на кожну з властивостей. Це також включає аналіз різних вразливостей.

4. Створення підстав для прийняття рішень: однією з головних цілей побудови IMECA таблиць є створення основи для прийняття обгрунтованих рішень

щодо поліпшення кібербезпеки системи. Ці таблиці допомагають ідентифікувати найбільш критичні аспекти та розробляти стратегії для підвищення рівня захисту.

5. Оновлення та адаптація: IMECA таблиці мають бути гнучкими для оновлення та адаптації до нових загроз та вразливостей. Постійний аналіз та оновлення таблиць забезпечують актуальність оцінок і врахування нових викликів кібербезпеки.

3.2 Послідовність аналізу кібербезпеки з використанням ієрархічних IMECA таблиць

Об'єктами аналізу, заснованого на IMECA- методиці, є, у цій роботі зазвичай, компоненти інфарструктури СБФ БПЛА – апаратні і програмні засоби або елементи.

Згідно рисунку 2.2 у розділі 2, таким чином, як об'єкт IMECA-аналізу слід розглядати ієрархічну структуру СБФ БПЛА як "системи в системі" або інфраструктуру – IS (рис. 3.3).

У цьому випадку від одиночної таблиці VT, що описується моделлю (3.1), слід перейти до їх ієрархії VT_{IS}, що описується набором вкладених множин елементів системи:

$$VT_{IS} = \left\{ VT_{Syst_k} = \left\{ VT_{SubSyst_k} = \left\{ VT_{Com_k} = \left\{ VT_{El_k} = \{VT_{PhyEl_k}\}_{i=1}^{nk}, VT_{El_k} = \{VT_{CybEl_k}\}_{j=1}^{mk} \right\} \right\} \right\} \right\}_{k=1}^{K} \quad (3.2)$$

, де VT_{Syst} – модель (таблиця) системи $Syst_k$, k = 1,…, K (K – число систем в інфраструктурі IS), $VT_{SubSyst}$ – модель (таблиця) підсистеми $SubSyst_k$, k = 1,…, K (K – число підсистем в інфраструктурі IS), VT_{Com} – модель (таблиця) компонентів Com_k, k = 1,…, K (K – число компонентів в інфраструктурі IS), VT_{El} – модель (таблиця) елементів El_k, де і-той показано кількість фізичних елементів, а j-той – кількість кібрелементів.

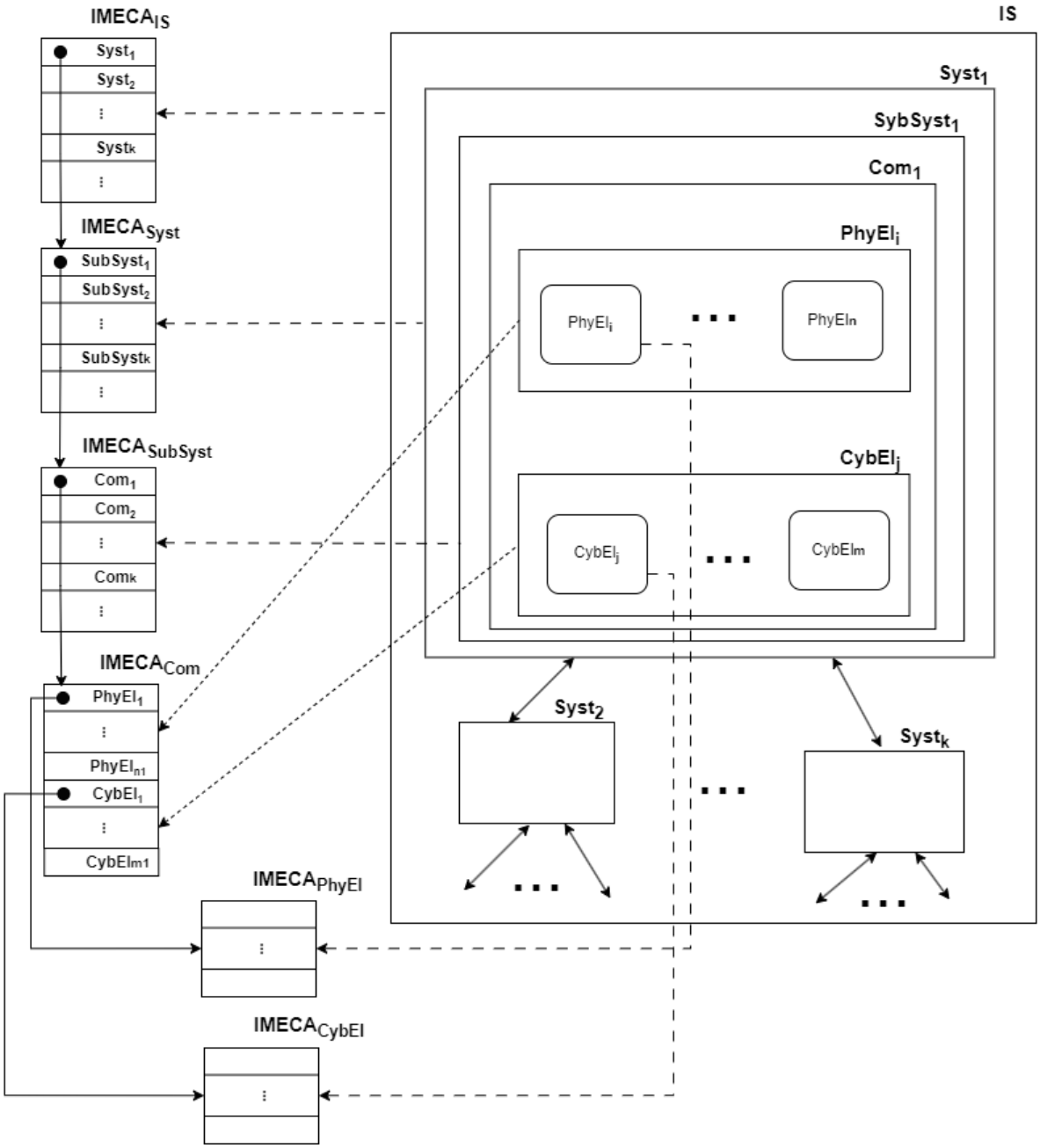


Рисунок 3.3 – Об’єкт H-IMECA-аналізу

3.2.1 Принципи аналізу

Аналіз причин виникнення загроз та вразливостей у СБФ БПЛА вимагає ретельного розгляду факторів, які сприяють цим проблемам. Наприклад, атаки можуть виникати через технічні недоліки програмного забезпечення або апаратного забезпечення, неправильну настройку мережі чи використання непохибних засобів зв'язку. Недостатнє навчання персоналу та недостатня увага

керівництва до кібербезпеки також можуть створювати прогалини в знаннях та розумінні загроз. Відсутність або неправильне виконання оновлень безпеки також може зробити систему вразливою перед новими загрозами. Усі ці аспекти описуються в моделі "I_v" – порушник, "Th_v" – загрози, "V_v" – вразливості, "A_v" – атаки.

Ключовим у такому аналізі є визначення наслідків атаки на СБФ БПЛА і розуміння кроків розробки захисту та підвищення ефективності контрзаходів.

Атаки, зачасту зумовлені зовнішніми або внутрішними впливами, можуть описуватись за допомогою додаткового елемента моделі – характеру загрози (CH_v). До таких впливів належать природні, такі як землетрус, град, повені, біалогічні погрози, або штучні, такі як, ненавмисні (помилки персоналу) або цілеспрямовані (спам, хакерські атаки) інформаційні впливи.

Таким чином, модель (3.1) може бути доповнена таким чином:

$$VT_2 =< I_v, VP_v, \mathrm{C}\boldsymbol{H}_v, Th_v, V_v, A_v, P_v, S_v, X_{r_v} >_{v=1}^{V} \quad (3.3)$$

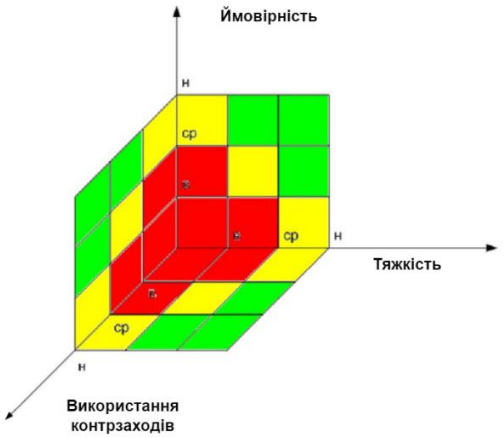
Для повноти розуміння виникнення загроз та уразливостей у СБФ БПЛА, дуже важливими показниками, є елемент інфраструктури СБФ БПЛА (ISv), властивості безпеки (SecPv), які слід додати у вираз (3.3):

$$VT_3 =< I_v, VP_v, \boldsymbol{IS}_v, \mathrm{C}H_v, Th_v, V_v, A_v, \boldsymbol{SecP}_v, P_v, S_v, X_{r_v} >_{v=1}^{V} \quad (3.4)$$

Облік показників зумовлює відображення «квадратної» матриці критичності (рис. 3.4-а), що описує наслідки відмови у двомірному просторі «ймовірність – тяжкість». А додавання такого показника, як - контрзаходи (ContMv) у модель 3.5, зумовлює перехід від матриці («квадрату») критичності (рис. 3.4-а), до «кубу» критичності – тривимірної матриці у просторі «ймовірність – тяжкість – протидія або час відновлення системи (усунення наслідків атаки)» (рис. 3.4-б).

$$VT_4 =< I_v, VP_v, IS_v, \mathrm{C}H_v, Th_v, V_v, A_v, SecP_v, P_v, S_v, X_{r_v}, \boldsymbol{ContM}_v >_{v=1}^{V} \quad (3.5)$$

Ймовірність	***Тяжкість***		
	Низька	*Середня*	*Висока*
Низька	5	4	3
Середня	4	3	2
Висока	3	2	1



а) б)

Рисунок 3.4 – Двох- (а) та тривимірна (б) матриця критичності

На рис. 3.4-б кількість градацій критичності може бути більшою з урахуванням комбінацій значень трьох показників.

Якщо при цьому ввести спеціальний стовпець у таблицю – елемент X_{ContM_V}, який описуватиме можливі наслідки та якість використання контрзаходів для зниження ризиків або парирування атак на систему, то він являтиме собою модель для оцінки критичності системи після використання контрзаходів системи:

$$VT_5 =< I_v, VP_v, IS_v, CH_v, Th_v, V_v, A_v, SecP_v, P_v, S_v, X_{r_v}, ContM_v, \boldsymbol{X_{ContM_v}} >_{v=1}^{V} \quad (3.6)$$

Ця модель включає всі елементи, необхідні проведення аналізу кібербезпеки інфраструктури СБФ БПЛА. Слід зазначити, що введення контрзаходів та визначення критичності після їх застосування призводить до зміни показників тяжкості та ймовірності реалізації атаки повторно або наслідків після неї. Отже, після їх запровадження ці показники мають бути перераховані (перевизначені). Таким чином, вираз (3.6) є розширеною моделлю IMECA-опису СБФ БПЛА.

3.2.2 Етапи аналізу

Згідно підрозділу 3.2.1 для оцінки ризиків загрози для СБФ БПЛА, вони аналізуються з точки зору ймовірності їх виникнення, можливого впливу на окремі елементи системи та наслідки після реалізованих атак, дотримуючись стандартної

методології оцінки. Оцінка проводиться за трьома критеріями ризиків, тобто ознаками критичності: ймовірність, тяжкість та ризик.

Показник ймовірності оцінює можливості того, наскільки ймовірно виникнення конкретної атаки за допомогою загрози через вразливість у системі, враховуючи, що подія відбудеться в певному проміжку часу. Тяжкість характеризує масштаб шкоди чи втрат, які можуть виникнути внаслідок атаки, оцінюється вплив на систему та наслідки для даних, функціональності та безпеки. Показник ризик відображає комплексну оцінку ймовірності та тяжкості наслідків та характеризує загальний ступень потенційного впливу атаки на систему у виді добудка.

Підсумовуючи, у таблиці 3.1 показано оцінки ризиків у відповідних рівнях ризиків.

Таблиця № 3.1– Оцінки ризиків системи

Критерії	Рівень	Обґрунтування	Шкала
1	2	3	4
Ймовірність	Низький	Мінімальна ймовірність виникнення події	1-3
	Середній	Шанси на виникнення події помірні	4-7
	Високий	Велика можливість виникнення події у найближчому майбутньому	8-10
Тяжкість	Низький	Мінімальна шкода або втрати	1-3
	Середній	Помірна шкода або втрати	4-7
	Високий	Серйозна шкода або великі втрати внаслідок події	8-10
Ризик	Низький	Мінімальна загроза	3- 28
	Середній	Середня загроза	29-64
	Високий	Велика загроза для системи або даних	65-100

Оцінюючи загрози для інфраструктури СБФ БПЛА, важливими факторами є оснащення і підготовка порушника. Ці аспекти дозволяють визначити ймовірність та ефективність порушника у подоланні захисних заходів системи. Для числового визначення цих параметрів (високий, середній, низький), а також ймовірності, тяжкості і ризику, була розроблена структура, враховуючи різні характеристики

порушника (таблиця 2.4). У таблиці 3.2 представлені показники для оцінки оснащення і тренувального потенціалу порушника.

Таблиця № 3.2– Показники для виявлення потенціалу порушника

Порушник	Потенціал порушника		
	Характеристика	Оцінка	Рівень
Тип порушника	Технічні навички	1-10	Згідно таблиці 3.3
	Рівень доступу	1-10	
	Мотивація	1-10	
	Рівень освіти	1-10	
	Досвід в реалізації кібератак	1-10	
	Кошти та ресурси	1-10	
	Ступінь організації	1-10	
	Використовувані технічні ресурси	1-10	

Кожна характеристика оцінюватиметься в балах, від 1 до 10, де 1 – дуже низький рівень, 10 – дуже високий рівень. Потім відбувається процес усереднення бала за всіма характеристиками і визначається рівень порушника знову від 1 до 10. Середнє отримане значення характеристик співвідноситься із діапазоном значень, наведеним у табл. 3.3, і, відповідно, визначають потенціал порушника, необхідний для реалізації загрози.

Таблиця № 3.3 – Визначення потенціалу порушника

Діапазон значень	Потенціал порушника
$1 \leq VP < 3,5$	Недостатній потенціал
$3,5 \geq VP < 5,5$	Низький потенціал
$5,5 \geq VP < 8$	Середній потенціал
$8 \geq VP \leq 10$	Високий потенціал

Існує кілька видів експертних оцінок визначення кібербезпеки системи. Оцінка ризиків дозволяє виявити критичність уразливостей та потенційні загрози. Аналіз загроз включає вивчення методів атак та їхнього впливу на систему. Експертна думка досвідчених фахівців дає рекомендації щодо покращення захисту. При систематизації всіх трьох вище методів оцінки, експертна оцінка у вигляді

тестів систематизує знання та досвід, допомагаючи оцінити навички та мотивацію потенційного порушника, його доступ, методи та рівень загрози.

3.3 Інтегральна оцінка кібербезпеки СБФ БПЛА

За підрозділом 3.2, сформована інтегральна оцінка –це комплексна оцінка кібербезпеки СБФ БПЛА, яка відображає загальний рівень кібербезпеки систем для флоту БПЛА, а також це комплексна оцінка, яка складається з підходу до оцінки ризиків, загроз, вразливостей і атак, пов'язаних з цими системами.

Основним завданням є використання розробленої координаційної матриці, розробленої на основі таблиці IMECA, яка охоплює критерії ймовірності, тяжкості та ризику. Ці критерії відображають ймовірність атак через вразливість у сиситемі за допомгоаю загроз, їх потенційну серйозність та загальний ризик для системи.

А також узагальнюються систематичний аналіз отриманих даних, включаючи результати тестів, аудити безпеки, аналіз вразливостей та інші методи, за допомогою яких отримається повна інформація про кібербезпеку у СБФ БПЛА.

На основі цього аналізу створюється інтегрована оцінка кібербезпеки, що відображає загальний стан безпеки системи багатофункційних флотів БПЛА. Ця оцінка дозволяє визначити сфери критичного ризику, визначити найбільш вразливі компоненти системи та дати рекомендації щодо покращення кібербезпеки, побудувати матрицю оптимізаційних заходів підвищення та зменшення ризику реазізації та впровадження атак у системі та пом'якшення загроз.

3.4 IMECA аналіз системи моніторингу критичної інфраструктури за допомогою СБФ БПЛА

Критична інфраструктура України охоплює об'єкти і системи, що мають стратегічне значення для національної безпеки, економіки та суспільства. Ці об'єкти та системи мають бути надійно захищені від цілої низки загроз, включно з

технічними збоями, стихійними лихами та кібератаками [1-6], згідно заканадавсту, яке описано у Додатку В.

3.4.1 Етапи аналізу

Тому багато років розробляються системи моніторингу надзвичайних ситуацій (НС) і критичної інфраструктури (КІ) за допомогою БПЛА. Один із таких проектів був представлений на виставці 2022 року проект Menatir від української компанії [4, 7].

Система моніторингу критичної інфраструктури України за допомогою флоту безпілотних літальних апаратів (БПЛА) є важливою частиною забезпечення безпеки та екології України. Як основу для подальших досліджень розглядається система з детально опрацьованими завданнями та цілями проекту, який був представлений на виставці [7].

Цілями системи є забезпечення безпеки українських атомних електростанцій, раннє виявлення та моніторинг потенційних загроз і надійний контроль параметрів навколишнього середовища. Основними завданнями системи, є:

1. виявлення та класифікація несанкціонованих літаючих об'єктів, таких як БПЛА та літаки, що наближаються до АЕС;

2. моніторинг рівня радіації;

3. візуальне спостереження та аналіз: дозволяє виявляти потенційні проблеми, такі як витоки, пожежі та структурні пошкодження;

4. зв'язок: використовує мережу зв'язку для передачі даних між БПЛА та центром управління;

5. аналіз даних та рекомендації: Центр управління оснащений найсучаснішими системами аналізу даних та штучного інтелекту для обробки інформації, отриманої з БПЛА;

6. створення архіву даних: збиратиме дані про стан та екологічні параметри КІ та створюватиме архів інформації, яка може бути використана для подальшого аналізу та планування.

Система моніторингу НС та КІ України за допомогою інфраструктури СБФ БПЛА, яку було представлено на виставці, наразі є вразливою, щоб розібрати модель загроз та визначити потенціал порушників для такого виду системи, було вирішено поділити її на компоненти для коректнішого розуміння взаємовідносин між елементами інфраструктури цієї системи. Ця система включає кілька ключових компонентів (згідно з розділом 2, підрозділу 2.1 модель інфраструктури системи багатофункціональних флотів БПЛА), що зображені на рисунку 3.5:

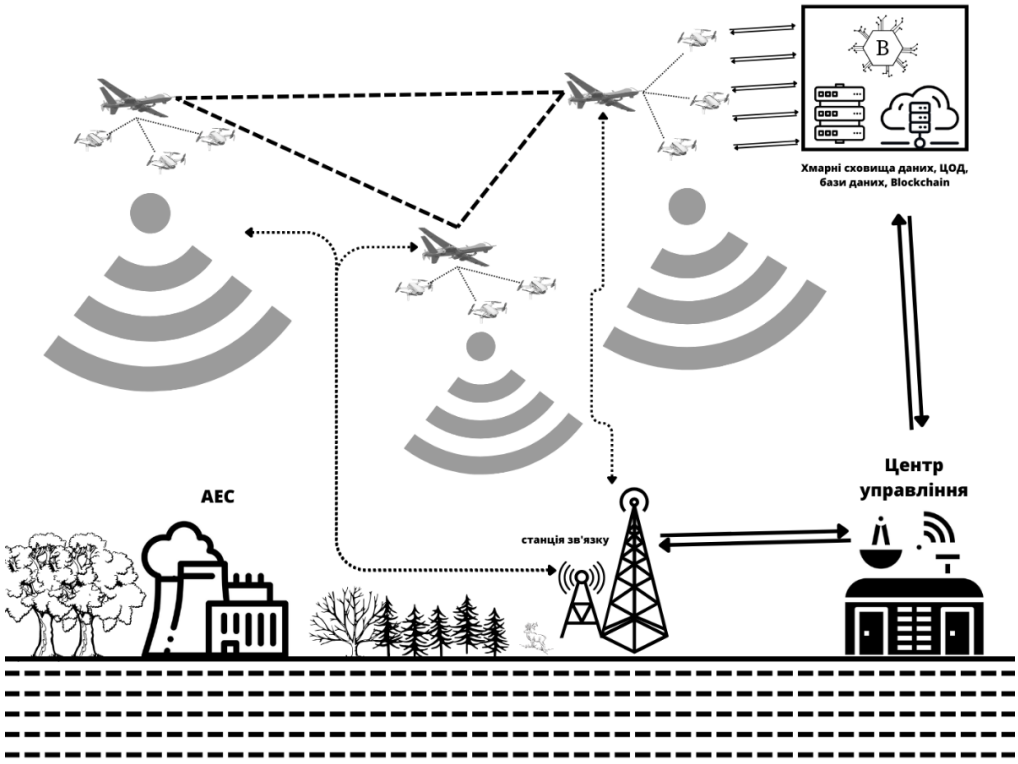


Рисунок 3.5 – Інфраструктура системи моніторингу за допомогою БПЛА

1. флоти БПЛА: система складається з флотів БПЛА, що включають від 4 до 6 БПЛА;

2. оперативний центр: командно-диспетчерський центр виконує функції командного пункту для координації та моніторингу флоту БПЛА, з останніх модифікацій центр автоматизований, не використовує операторів;

3. системи зв'язку: Для забезпечення ефективного зв'язку між БПЛА та оперативними центрами використовуються різні системи зв'язку, включаючи радіо, стільникову та супутникову;

4. датчики та обладнання: БПЛА оснащуються різними датчиками, у тому числі:

– радіаційні детектори вимірювання рівня радіації;
– камери та інфрачервоні датчики для візуальних спостережень;
– датчики вимірювання хімічних параметрів атмосфери;
– геолокаційне обладнання для визначення місцезнаходження БПЛА;
– додаткові датчики для виявлення аномалій та стану інфраструктури.

5. системи зберігання та аналізу даних, які отримані з БПЛА, використовуються спеціалізованими системами, такі як сервери та бази даних, хмарні сховища та інше.

Виходячи з вище проаналізованої та отриманої інформації, було виявлено такі переваги системи:

– система забезпечує швидке реагування на потенційні загрози та підвищує безпеку атомних станцій;

– завдяки екологічному моніторингу мінімізуються ризики для здоров'я людей та природи;

– флот БПЛА забезпечує ширше охоплення та ефективніше використання ресурсів у порівнянні з традиційними методами моніторингу;

– системи дозволяють створювати архів даних, який може бути використаний для майбутнього аналізу та планування;

– використання БПЛА знижує ризик людської помилки та підвищує надійність моніторингу.

Незважаючи на те, що КІ завжди був підданий різноманітним небезпекам, включаючи природні явища, людські помилки, технологічні збої та злочинну поведінку в найширшому сенсі, захист КІ став окремою сферою політики як прямий наслідок подій 11 вересня 2001 року [8]. В останні роки енергетична

інфраструктура зіткнулася з загрозами у вигляді безпілотних літальних апаратів (БПЛА).

Виявлення БПЛА навколо КІ або використання БПЛА для протидії загрозам на КІ також викликає зростаюче занепокоєння, оскільки вони загрожують безпеці людей та інфраструктурі, не кажучи вже про ризики для літаків, станцій та інших об’єктів, яких неможливо уникнути, що призведе до зупинки, поки не буде вирішена ця загроза.

Загрози КІ часто асоціюють із тероризмом, який має кілька аспектів. Такі загрози можна розділити на основі дії порушників (фізичні чи кібернетичні), їх походження (внутрішні чи зовнішні) та контексту, у якому вони виникають (ізольовані чи кількісні цілі). Розуміння типів загроз, з якими стикається КІ, є першим кроком у розробці відповідних стратегій захисту та правильному розумінні моделей загроз і порушників, розглянутих у розділі 2 (підрозділи 2.2-2.5).

Фізичні загрози КІ можуть приймати різні форми. Їхня спільна характеристика полягає в тому, що вони призначені для пошкодження інфраструктури, каліцтва або виведення з ладу повністю або частково шляхом руйнування її фізичної структури, механічних компонентів та інших властивостей. Найбільш очевидні фізичні загрози для КІ включають використання саморобних вибухових або запальних пристроїв, транспортних засобів, ракет, переносних зенітно-ракетних комплексів, гранат або навіть простих інструментів (таких як сірники чи запальнички для підпалів), або, навпаки, проникнення в КІ, як персонал даного об’єкту або маніпулювання працівниками об’єкту.

Кіберзагрози відрізняються за своєю природою від фізичних загроз, але кінцевий результат може бути однаковим , дивитися Додаток Ґ, таблицю 3.4 всі ці приклади систематизовані для даної системи. Кіберзагрози різноманітні, але включають, наприклад, такі типи атак [9]:

– маніпулювання системами передачі даних - наприклад, шкідливе програмне забезпечення, яке використовує вразливості в програмному забезпеченні або апаратних компонентах, необхідних для функціонування КІ;

– зупинка роботи критично важливих систем, наприклад, атаки типу "відмова в обслуговуванні" (DoS);

– обмеження доступу до критично важливих систем та інформації, наприклад, атаки з вимогою викупу.

Захист інформаційних систем від зовнішніх атак отримав значну увагу від національних та міжнародних регуляторів, проте внутрішні загрози залишаються менше уваги. Інсайдери мають перевагу над зовнішніми суб'єктами, бо вони можуть отримати доступ до КІ через своє внутрішнє становище. Інсайдери можуть бути співробітниками або постачальниками компаній, їх можна використовувати як змовників або спільників зовнішніх агентів. Загрози інформаційній інфраструктурі можуть бути ізольованими або частиною ширшого плану нападу. Такі атаки можуть бути спорадичними або скерованими проти інфраструктури, що належить тому самому власнику або оператору в тому ж секторі, або розташована в тій же географічній зоні. Такі дії можуть бути сприйняті як терористичні або промислові шпигунство, а кібератаки можуть виявлятися кампаніями або серіями нападів.

Виявлення закономірностей у таких складних сценаріях вимагає потужних аналітичних інструментів і обробки інформації з різноманітних і різнорідних джерел. Як підкреслює Організація з безпеки і співробітництва в Європі (ОБСЄ) щодо енергетичного сектору, більшість кібератак залишаються невиявленими, оскільки оператори неохоче повідомляють про такі інциденти. У той же час, здатність розпізнавати рушійні сили і технології, що лежать в їх основі, на якомога більш ранній стадії є ключовим фактором для забезпечення обміну відповідною інформацією між органами влади. Це підвищить їхню здатність ефективніше реагувати на поточні атаки і запобігати майбутнім нападам на потенційних жертв. У деяких випадках те, що здається ізольованою атакою на відносно малопомітну ціль, насправді може бути частиною більш амбітної та поетапної злочинної стратегії [10].

Використання моделі з розділу 2 для раннього визначення, чи є атака ізольованим актом або частиною серії запланованих атак на інші об'єкти, може послужити основою для розробки стратегій захисту критичних об'єктів.

Таблиця № 3.4 – Топ-10 загроз критичної інфраструктури (ЗКІ)

№	Загроза	Вразливості
1	2	3
1	Незаконне використання RDP (Remote Desktop Protocol).	Точки доступу до послуг в мережі КІ часто недостатньо захищені і знаходяться зовні.
2	Онлайн-атаки через офісні або корпоративні мережі	Зловмисники можуть отримати доступ до офісних інформаційних технологій через різні способи підключення до мережі.
3	Атаки на стандартні компоненти мережі КІ	Стандартні ІТ-компоненти, як системне програмне забезпечення, сервери та бази даних, часто мають недоліки, що можуть бути використані зловмисниками.
4	DoS-атаки	Атаки типу «відмова в обслуговуванні» можуть спричинити збій систем через порушення мережевих з'єднань і ресурсів.
5	Людська помилка та саботаж	Навмисні і недбалі дії злочинців загрожують всім цілям захисту, включаючи конфіденційність та доступність.
6	Введення шкідливого ПЗ через зовнішні носії і обладнання.	Використання знімних носіїв і мобільних ІТ-компонентів співробітників збільшує ризик зараження шкідливим ПЗ.
7	Зчитування та публікація новин онлайн в мережі КІ	Більшість компонентів керування зараз використовують незахищені протоколи відкритого тексту, що полегшує читання та введення команд.

Продовження таблиці № 3.4

1	2	3
8	Несанкціонований доступ до ресурсів	Зловмисникам легко атакувати систему, якщо вона не використовує надійні методи автентифікації та авторизації після зовнішнього проникнення.
9	Атаки на компоненти мережі	Зловмисники можуть маніпулювати мережевими компонентами для атак типу "людина посередині" і полегшення пошуку.
10	Технічні несправності чи форс-мажор	Збої в роботі через погоду або техніку можуть статися в будь-який момент. Мінімізувати ризик і шкоду важливо в таких випадках.

3.4.2 IMECA-аналіз СБФ БПЛА для критичної інфраструктури

У системі моніторингу КІ існує низка потенційних загроз, які можуть бути реалізовані різними порушниками чи природними явищами.

Система КІ піддається різноманітним природним та штучним загрозам, що можуть призвести до серйозних наслідків. Серед природних загроз найпоширеніші - землетруси, повені, атмосферні та кліматичні явища. Щодо штучних загроз, вони включають диверсії, саботажі, DoS атаки, шпигунство та інші форми атак. Україні не вистачає стандартів для аналізу ризиків, а також узгодженості в концептуальній базі для виявлення загроз та їх протидії. Стандартизація систем безпеки, сертифікація якості та вирішення ефективності проблем є надзвичайно важливими для України, особливо в контексті євроінтеграції. Гармонізація з міжнародними стандартами буде ключовою для забезпечення конкурентоспроможності української продукції на світовому ринку.

Тому далі буде розглянуте варіанти роботи моделей загроз, порушники та їх потенціал, згідно розділу 3.2, виявлення їх потенціалу, наслідків та ймовірність їх існування, на прикладі системи моніторингу КІ, яка була описана вище. Будуть розглянуті атаки, які проводять 4 різні типи порушників (згідно моделі порушників у розділі 2, підрозділі 2.4).

У цій системі було розглянуто такі порушники:

1. Внутрішній адміністратор інформаційної системи та безпеки.

2. Спеціальні служби закордонних держав.

3. Злочинні угруповання (кримінальні структури, хакері).

4. Колишні співробітники організації.

Згідно проведеної оцінки для кожної характеристики та порушника відповідно до таблиці 3.2 та 3.3. Оцінки (у балах) кожної характеристики наведено нижче у таблиці 3.5.

Таблиця № 3.5– Потенціали порушників

Потенціал порушника				
Характеристика	Порушник			
	1	*2*	*3*	*4*
Технічні навички	9	10	7	6
Рівень доступу	8	10	6	5
Мотивація	8	10	8	5
Рівень освіти	9	10	7	6
Досвід в реалізації кібератак	7	10	9	4
Кошти та ресурси	9	10	7	5
Ступінь організації	9	10	7	4
Використовувані технічні ресурси	8	10	8	5
Загальний потенціал	67	80	59	40

Після проведення усереднення балів, отримуємо такий потенціал для кожного порушника:

- внутрішній адміністратор інформаційної системи та безпеки:
  - сума балів: 9 + 8 + 8 + 9 + 7 + 9 + 9 + 8 = 67
  - середнє: 67 / 8 = 8,4
  - потенціал: високий
- спеціальні служби закордонних держав:
  - сума балів: 10 + 10 + 10 + 10 + 10 + 10 + 10 + 10 = 80

- середнє: 80 / 8 = 10
- потенціал: високий

– злочинні угруповання:

- сума балів: 7 + 6 + 8 + 7 + 9 + 7 + 7 + 8 = 59
- середнє: 59 / 8 = 7,4
- потенціал: високий

– колишні співробітники організації:

- сума балів: 6 + 5 + 5 + 6 + 4 + 5 + 4 + 5 = 40
- середнє: 40 / 8 = 5
- потенціал: низький

Таким чином, кожен порушник оцінений за рівнем, ґрунтуючись на усереднених балах характеристик.

Адміністратори безпеки внутрішніх інформаційних систем відіграють ключову роль у забезпеченні кібербезпеки систем екологічного моніторингу та атомних електростанцій. Але водночас, якщо ці адміністратори є зловмисниками, вони можуть використовувати свої права доступу та привілеї для реалізації різних загроз. Було виявлено такі погрози, дивитись таблицю 3.6.

Таблиця № 3.6 – Штучні загрози та вразливості СБФ БПЛА від 1 порушника

№	Загроза	№	Вразливості
1	2	3	4
1	Зміна навігаційних даних БПЛА	1	Використання нешифровані протоколи навігації
		2	Використання слабких паролів
2	Віддалене вимкнення БПЛА	3	Відсутність або слабка сегментація мережі
		4	Несанкціонований доступ до системи через слабку аутентифікацію
3	Зміна даних про стан БПЛА	5	Слабкі механізми аутентифікації та авторизації
		6	Відсутність журналювання та відслідковування доступу
4	Інтерференція із мережею зв'язку	7	Слабке шифрування протоколів комунікацій
		8	Відсутність контролю доступу

Продовження таблиці № 3.6

1	2	3	4
5	Впровадження шкідливого програмного забезпечення в системи керування БПЛА	9	Вразливість в програмному забезпеченні БПЛА
		10	Неправильна настройка прав доступу до системи управління
6	Знищення ідентифікаційних даних БПЛА	11	Низький рівень доступу до ідентифікаційних даних
		12	Відсутність резервного копіювання

Іноземні спецпідрозділи можуть становити серйозну загрозу для систем екологічного моніторингу та атомних електростанцій України. Їхньою метою може бути отримання секретної інформації, порушення роботи системи або потенційна загроза атомній електростанції. Було виявлено такі погрози, дивитись таблицю 3.7.

Таблиця № 3.7 – Штучні загрози та вразливості СБФ БПЛА від 2 порушника

№	Загроза	№	Вразливості
1	2	3	4
1	Зміна програмного забезпечення процесу зарядки	1	Відсутність аутентифікації та авторизації змін у програмному забезпеченні
		2	Відсутність моніторингу програмного забезпечення
2	Захоплення сеансу адміністратора	3	Відсутність механізму шифрування даних
		4	Відсутність механізму автентифікації на рівні передавання
3	Втручання в роботу системи зв'язку	5	Відсутність системи контролю автентифікації та авторизації
		6	Відсутність ефективних заходів захисту від розподілених атак
4	Злам системи управління БПЛА	7	Відсутність шифрування каналів комунікацій
		8	Використання слабких паролів у системі управління БПЛА

Продовження таблиці № 3.7

1	2	3	4
5	Зміна команд і управління БПЛА	9	Відсутність шифрування каналів комунікацій
		10	Відсутність відповідної аутентифікації
6	Впровадження шкідливих датчиків	11	Відсутня перевірка автентичності датчиків
		12	Відсутня системи періодичної перевірки та виявлення шкідливих датчиків

Злочинні групи та хакери представляють серйозну загрозу для систем екологічного моніторингу та атомних електростанцій в Україні. Вони можуть діяти з різних мотивів, включаючи фінансову вигоду та маніпулювання даними, що створює потенційні ризики для безпеки атомних станцій. Можливі атаки включають несанкційний доступ до систем моніторингу, порушення даних та втручання в роботу атомних електростанцій. Враховуючи таблицю 3.8, визначені конкретні загрози, які варто ураховувати при розробці та впровадженні заходів кібербезпеки для екологічних та енергетичних систем. Ефективні контрзаходи є критичними для збереження високого рівня захисту цих систем від кіберзагроз.

Таблиця № 3.8 – Штучні загрози та вразливості СБФ БПЛА від 3 порушника

№	Загроза	№	Вразливості
1	2	3	4
1	Впровадження шкідливого програмного забезпечення в компонент збору відеоданних з БПЛА	1	Відсутня перевірка автентичності під час завантаження програмного забезпечення
		2	Відсутня валідація вхідних даних
2	Впровадження фальшивих команд в управління БПЛА	3	Відсутність шифрування каналів комунікацій
		4	Відсутність відповідної аутентифікації
3	Перехоплення та модифікації даних через бездротові канали зв'язку	5	Використання слабких або стандартних паролів
		6	Відсутність протоколів шифрування данних

Продовження таблиці № 3.8

1	2	3	4
4	Впровадження шкідливих датчиків	7	Слабка політика безпеки та система захищення від фізичного втручання
		8	Вразливість у мережевому протоколі датчиків
5	Віддалене вимкнення БПЛА	9	Слабка аутентифікація при віддаленому доступі до систем керування
		10	Відсутня захищеність протоколів передачі команд
6	Злам серверів і сховищ даних	11	Використання застарілих версій програмного забезпечення на серверах
		12	Використання старі протоколи для захисту даних в сховищах

Колишні співробітники цієї організації можуть становити серйозну загрозу для систем екологічного моніторингу та атомних електростанцій України. Вони можуть мати доступ до внутрішніх ресурсів і системної інформації. Було виявлено такі погрози, дивитись таблицю 3.9.

Таблиця № 3.9 – Штучні загрози та вразливості СБФ БПЛА від 4 порушника

№	Загроза	№	Вразливості
1	2	3	4
1	Захоплення чи модифікація медіа-матеріалів в процесі передачі з БПЛА	1	Відсутність відповідної аутентифікації
		2	Невірне збереження медіа-матеріалів
2	Віддалений вплив на БПЛА	3	Відсутній контроль доступу до системи управління БПЛА
		4	Вразливість в програмному забезпеченні системи управління
3	Витік конфіденційних даних	5	Використання застарілих методів шифрування даних
		6	Використання старих протоколів для доступу к даним

Продовження таблиці № 3.9

1	2	3	4
4	Саботаж і фізичний вплив на БПЛА	7	Слабка політика безпеки та система захищення від фізичного втручання
		8	Вразливість фізичної інфраструктури
5	Перехоплення даних через SQL ін’єкцію	9	Відсутня сиситема фільтрації введених даних
		10	Слабка система автентифікації та контролю доступу
6	Втручання в роботу датчиків і обладнання	11	Відсутність аутентифікації датчиків та обладнання
		12	Відсутність політики безпеки та контролю доступу

Стихійні лиха можуть становити серйозну небезпеку для систем екологічного моніторингу та атомних електростанцій України. Було виявлено такі погрози, дивитись таблицю 3.10.

Таблиця № 3.10– Природні загрози та вразливості системи

№	Загроза	№	Вразливості
1	2	3	4
1	Землетруси	1	Відсутність захисту від землетрусів
		2	Відсутність резервного планування та систем для управління наслідками
2	Паводки	3	Відсутність системи захисту центрів зв'язку та об'єктів оперативного контролю від паводків
		4	Відсутність системи регулярного обслуговування та тестування на випадок паводків
3	Туман	5	Зниження видимості. Низька роздільна здатність оптичних систем
		6	Вплив на комунікації. Переривання радіо- та супутникового зв'язку
4	Грози та блискавки	7	Вразливість радіоелектронного обладнання при ударах блискавки
		8	Недолік у системах захисту від блискавки

Продовження таблиці № 3.10

1	2	3	4
5	Високі температури	9	Недолік у системах охолодження
		10	Вразливість електричної системи при високих температурах
6	Сильні вітри та урагани	11	Відсутність адаптивних аеродинамічних систем при сильних вітрах. Непропорційна реакція на зміни обстановки
		12	Вразливість аеродинаміки при ураганах

Після проведення структурування потенційних загроз та уразливостей для кожного з чотирьох типів порушників, а також розгляду впливу природних катаклізмів, був проведено аналіз типових атак на БПЛА (див. Додаток Г), і наступним кроком після цього було виконане повний IMECA аналіз на СБФ БПЛА. Результати даного аналізу були систематично відображені в таблиці, яка додається до даного документу у Додатку Ґ.

IMECA аналіз включав в себе ідентифікацію всіх можливих загроз та вразливостей, вимірювання їх потенційного впливу на систему, оцінку ймовірності виникнення подій, визначення ефективності контрмер та, нарешті, аналіз ризиків. Цей комплексний підхід дозволяє не лише ідентифікувати потенційні загрози, а й ефективно класифікувати їх за рівнем важливості та можливими наслідками [4].

На підставі результатів аналізу атак у Додатку Ґ за рівнем небезпеки для СБФ БПЛА від дій 4 порушників було побудовано матриці критичності (ризків) цієї системи (табл. 3.11, 3.12, 3.13, 3.14, 3.15 та загальна 3.16) та матрицю критичності після впровадження контрзаходів (табл. 3.17). Зеленим позначено низький рівень ризику, жовтим – середній рівень, червоним – високий [4].

У рамках аналізу безпеки системи багатофункціональних флотів БПЛА виявлено ряд критичних загроз та вразливостей, які можуть призвести до серйозних наслідків для функціонування цієї системи. Зокрема, центри зв'язку, система управління БПЛА, системи моніторингу та бази даних виявлені як ключові елементи, що піддаються різноманітним атакам.

Таблиця № 3.11 – Матриця критичності ризків СБФ БПЛА після атак 1 порушника

	Тяжкість		
Ймовірність появи	Низька	Середня	Висока
Низька			
Середня		3,10	6
Висока		2,4,5,7,8	1,9,11,12

Таблиця № 3.12 – Матриця критичності ризків СБФ БПЛА після атак 2 порушника

	Тяжкість		
Ймовірність появи	Низька	Середня	Висока
Низька			19,20
Середня		23,24	15,16,21,22
Висока		13,14,17,18	

Таблиця № 3.13 – Матриця критичності ризків СБФ БПЛА після атак 3 порушника

	Тяжкість		
Ймовірність появи	Низька	Середня	Висока
Низька			31
Середня		27,33,36,35	28,32,34
Висока		25,26,29,30	

Таблиця № 3.14 – Матриця критичності ризків СБФ БПЛА після атак 4 порушника

	Тяжкість		
Ймовірність появи	Низька	Середня	Висока
Низька			43,46
Середня	47	40,41,42	39,44
Висока	48	45	37,38

Таблиця № 3.15 – Матриця критичності ризків СБФ БПЛА після атак 5 порушника

	Тяжкість		
Ймовірність появи	Низька	Середня	Висока
Низька		49,50,51,52	53,54,55,56
Середня		57,58,59,60	
Висока			

Таблиця № 3.16 – Узагальнююча матриця критичності ризків СБФ БПЛА після атак 5 порушників

	Тяжкість		
Ймовірність появи	Низька	Середня	Висока
Низька		49,50,51,52	19,20,31,43,46, 53,54,55,56
Середня	47	3,10,23,24,27,33,36,35, 40,41,42,57,58,59,60	6,15,16,21,22,28,32, 34,39,44
Висока	48	2,4,5,7,8,13,14,17, 18,25,26,29,30,45	1,9,11,12,37,38

Загрози, пов'язані зі зміною навігаційних даних та впровадженням шкідливого програмного забезпечення, становлять серйозну небезпеку для стійкості та надійності системи. Недоліки у механізмах аутентифікації та авторизації, відсутність шифрування каналів комунікацій та неефективні заходи захисту від розподілених атак створюють умови для реалізації атак та порушення безпеки. Виявлені загрози та вразливості підтверджують необхідність комплексних заходів з підвищення безпеки та захисту інфраструктури системи БПЛА. Акцент слід зробити на підвищенні рівня аутентифікації, шифрування та контролю доступу, а також на вдосконаленні моніторингу та виявлення інцидентів для оперативної реакції на потенційні загрози.

Зниження критичності системи багатофункційних флотів БПЛА від різних атак можна досягти за допомогою різноманітних контрзаходів [4]. Стосовно

захисту СБФ БПЛА доцільно сформулювати такі основні методи забезпечення безпеки ОКІ:

1. Автоматичне повернення або автоматична робота: передбачення системи блокування або автоматичного вимкнення в разі виявлення небажаної поведінки або атаки, а також підсистема самостійного контролю або автоматичної системи управління.

2. Шифрування даних: використання шифрування для захисту конфіденційної інформації та підвищення стійкості передачі даних між БПЛА та центрами управління.

3. Мережева безпека: впровадження ефективних засобів мережевої безпеки для виявлення та блокування небезпечних мережевих атак.

4. Стійке програмне забезпечення: використання стійкого програмного забезпечення, оновлення та патчі для запобігання використанню вразливостей.

5. Фізична безпека: забезпечення фізичної безпеки систем, тобто надійний захист пристроїв та контроль доступу від пошкодження та втручання у апаратні пристрої системи.

6. Автентифікація та авторизація: використання сильних методів автентифікації і авторизації для обмеження доступу до систем управління БПЛА.

7. Моніторинг та реагування: постійний моніторинг систем з метою швидкого виявлення аномальної поведінки або підозрілих активностей.

8. Тренування персоналу: навчання персоналу щодо кібербезпеки, викриття соціального інжинірингу та відповідальності за безпеку інформації.

9. Регулярні аудити безпеки: проведення періодичних аудитів безпеки для ідентифікації слабких місць та вжиття заходів для їх виправлення.

10. Резервна підсистема відновлення: під час аварійних випадків спрацьовує віддалена система відновлення, яка у польоті самовідновлюється.

Отже згідно результатів аналізу атак у Додатку Ґ, а також після побудови матриці відповідності, для даного приклада, матриця критичності після контрзаходів, таблиця 3.17, виглядає так:

Таблиця № 3.17 – Узагальнююча матриця критичності ризків СБФ БПЛА після упровадження контрзаходів після атак 5 порушників

	Тяжкість		
Ймовірність появи	Низька	Середня	Висока
Низька	49	42,50,56,57,58,59,60	43,44,45,51,52,54,55
Середня		1,2,3,4,5,6,7,8,9,10,11, 12,13,14,23,24,25,34, 39,46,47,48,53	15,16,19,20,21,27,31, 32,33
Висока	29,30,35	17,18, 22,26, 28,36,37,38,41	

У процесі оцінки критичності та вибору контрзаходів для системи СБФ БПЛА було враховано різноманітні потенційні загрози та можливі наслідки атак. Аналіз показав, що безпека об'єкта контролю є складною задачею, оскільки йому загрожують як традиційні кібератаки, так і фізичні впливи, такі як природні лиха.

Однією з ключових висновків є необхідність комплексного підходу до захисту системи. Вибір контрзаходів повинен враховувати різноманітні аспекти безпеки, такі як кіберзахист, фізична безпека, інфраструктурна стійкість, та забезпечити ефективний захист в умовах різноманітних загроз.

Автоматичне повернення або автоматична робота (1), шифрування даних (2), стійке програмне забезпечення (4), та резервна підсистема відновлення (10) виявилися важливими контрзаходами для покращення стійкості системи в умовах кібератак та фізичних впливів. Впровадження цих заходів може значно зменшити ризики та наслідки вразливостей системи.

Контрзаходи, такі як мережева безпека (3), автентифікація та авторизація (6), моніторинг та реагування (7), тренування персоналу (8), та регулярні аудити безпеки (9) також відіграють важливу роль у підвищенні рівня захисту системи.

Узагальнюючи, застосування цих комплексних контрзаходів стане невід'ємною частиною стратегії безпеки СБФ БПЛА, забезпечуючи не лише ефективний захист від поточних загроз, але й готовність системи до майбутніх викликів та ризиків.

3.5 Особливості IMECA аналізу кібербезпеки СБФ БПЛА при комбінованих атаках

Аналіз кібербезпеки СБФ БПЛА під час комбінованих атак охоплює декілька ключових аспектів. По-перше, згідно підрозділу 2.4.2, він включає ідентифікацію потенційних загроз і уразливостей, що можуть бути використані для атаки на ці системи, цей процес включає структурований аналіз вразливостей апаратного забезпечення, програмного забезпечення та мережевої інфраструктури. Другий аспект полягає в аналізі сценаріїв комбінованих атак, які можуть комбінувати зазначені вище атаки у Додатках Ґ та Д, що можуть бути використані проти СБФ БПЛА. Це включає в себе розгляд можливих методів атак через різні канали зв'язку та зміни інформації, що передається між БПЛА та Центром управління. Третім етапом є інтегрований підхід до оцінки ризику внаслідок комбінованих атак на системи СБФ БПЛА, включаючи аналіз можливих наслідків для функціональності, конфіденційності, доступності та цілісності даних [4].

На основі цих особливостей проведення IMECA аналізу кібербезпеки СБФ БПЛА при комбінованих атаках надає змогу оцінити загрози та ризики.

3.5.1 Модель оцінювання ризиків комбінованих атак

Систематизація можливих комбінованих кібератак (ККА) включає кілька основних типів. Згідно підрозділу 2.4.2, перший тип - послідовні ідентичні або різні атаки на різні складові системи, впорядковані за методами та цілями, другий - паралельні ідентичні або різні атаки, які одночасно вражають різні частини системи різними виконавцями, третій - послідовно-паралельні атаки, які комбінують паралельні та послідовні втручання на різні компоненти системи, відбуваючись одночасно та послідовно [11].

Для математичного представлення комбінованих атак введемо наступні позначення: A_i, A_j - атаку виду i та j, Com_x - компонента x системи, t – час (використовуємо дискретний час).

Математичне представлення комбінованих атак:

1. Послідовні атаки:

$$A_{comb1}(Com_x)=\{A_i(t, Com_x), A_j(t+1, Com_x)\}, \quad (3.8)$$

де атака A_i відбувається в момент часу t, а атака A_j - в момент часу t+1. Цей тип атак дозволяє зловмисникам поетапно проникати в різні або тіж самі частини системи $Syst_i$, намагаючись уникнути виявлення та реагування. Рисунок 3.6 надає графічне представлення цієї моделі, де $Crit_{comb1}(A_i \rightarrow Com_x, A_j \rightarrow Com_x)$ – підсумкова критичність комбінованої атаки [11].

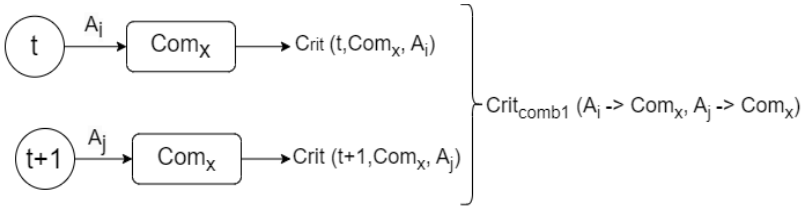


Рисунок 3.6 – Послідовні комбіновані атаки на СБФ БПЛА

2. Паралельні атаки:

$$A_{comb2}(Com_x, Com_y)=\{A_i(t, Com_x), A_j(t, Com_y)\}, \quad (3.9)$$

де A_i представляє атаку, що відбувається в момент часу t на компонент Com_x , тоді як A_j виконується в той же момент часу, впливаючи на компонент Com_y. Модель описує можливість одночасної реалізації атак на різні частини системи, що створює додаткові виклики для виявлення та ефективного реагування (рисунок 3.7 надає графічне представлення цієї моделі, де $Crit_{comb2}(A_i \rightarrow Com_x, A_j \rightarrow Com_y)$ – підсумкова критичність комбінованої атаки) [11].

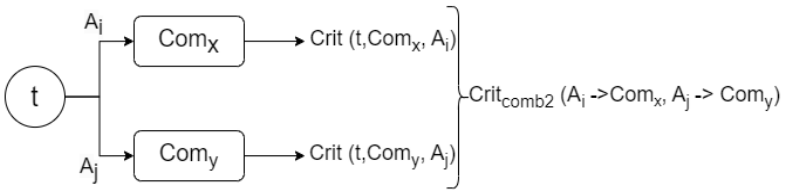


Рисунок 3.7 – Паралельні комбіновані атаки на СБФ БПЛА

3. Послідовно-паралельні атаки:

$$v_{comb3}(t) = \begin{cases} A_i(t) \rightarrow Com_x; \\ A_j(t) \rightarrow Com_y; \end{cases} \quad (3.10)$$

$$v_{comb3}(t+1) = \begin{cases} A_r(t+1) \rightarrow Com_w; \\ A_s(t+1) \rightarrow Com_z; \end{cases} \quad (3.11)$$

$$V_{comb3} = v_{comb3}(t) \times v_{comb3}(t+1), \quad (3.12)$$

Модель послідовно-паралельних атак визначається формулами (3.10), (3.11) та (3.12), відповідно до рисунку 3.8.

Елемент $v_{comb3}(t)$ представляє можливість виконання атак A_i та A_j в момент часу t на компоненти Com_x та Com_y відповідно. Аналогічно, $v_{comb3}(t+1)$ описує можливість атак A_r та A_s в момент часу t+1 на компоненти Com_w, Com_z. Вираз (5) визначає загальну множину варіантів послідовно-паралельних атак, яке є добутком множин атак в моменти часу t та t+1, відповідно до рисунку 3.8 [11].

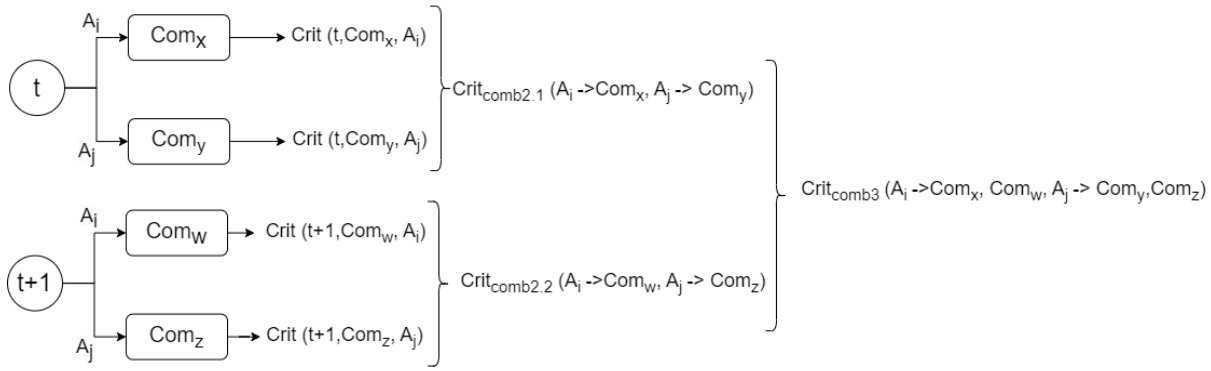


Рисунок 3.8 – Послідовно-паралельні комбіновані атаки на СБФ БПЛА

Визначення ймовірності атак може включати експертні оцінки на підставі аналізу статистичних даних та моделювання сценаріїв атак.

3.5.2 Послідовність IMECA аналізу при комбінованих атаках

Послідовність IMECA-аналізу при комбінованих атаках є наступною:

- виконується IMECA-аналіз кібербезпеки при одиничних кібератаках та оцінюються їх критичність, [11, 12] та Додаток Ґ;

- визначається множина комбінованих атак з використанням розроблених і деталізованих базових моделей послідовно-паралених ККА, притаманних досліджуваній системі;

- будується оновлена IMECA-таблиця з урахуванням множини ККА;

- для кожної ККА оцінюються ризики на підставі різних способів обчислення і операцій над ймовірностями і тяжкістями наслідків одиничних кібератак;

- визначається множина контрзаходів для зменшення ризиків та варіантів покриття ними кожної із загроз та одиничних атак;

- обчислюються ризики при використанні визначених множин контрзаходів та визначається їх вартість;

- визначаються сукупності підмножин «покриваючих» контрзаходів, які забезпечують зменшення ризиків до прийнятного рівня при одиничних кібератаках;

- здійснюється перевірка достатності цих множин при ККА і при необхідності вони доповнюються додатковими контрзаходами;

- вибирається підмножина «покриваючих» контрзаходів з мінімальною вартістю при комбінованих кібератаках.

Розглянемо приклади реалізації елементів даної методики, базуючись на результатах роботи [11, 12] та Додатку Ґ, де розглядалися загрози, уразливості та моделі атак, що виявляють потенційні ризики для складних систем, таких як СБФ БПЛА. Після аналізу атак та загроз від чотирьох різних порушників на критичну інфраструктуру та комбінованих атак, сформовано послідовності для IMECA-аналізу. Ці послідовності дозволяють систематизувати та проводити більш повний аналіз кіберзагроз та кібератак для оцінювання кібербезпеки СБФ БПЛА. Таблиця 3.18, яка сформована на базі результатів аналізу [11, 12], ілюструє варіанти комбінацій порушників та послідовні комбінації атак на систему.

Таблиця № 3.18 – Комбінації порушників та їх послідовні ККА на СБФ БПЛА

№	Комбінація порушників	Послідовність атак
1	1, 2	1, 2, 13, 14, 15
2	1, 3	1, 3, 24, 25, 26
3	1, 4	1, 4, 37, 38, 39
4	2, 3	13, 14, 15, 24, 25
5	2, 4	13, 14, 15, 36, 37
6	3, 4	24, 25, 26, 36, 37
7	1, 2, 3	1, 2, 13, 14
8	1, 2, 4	1, 2, 13, 14, 15, 36
9	1, 3, 4	1, 3, 24, 25, 26
10	2, 3, 4	13, 14, 15, 24, 25, 36

Оберемо для визначення критичності системи багатофункційних флотів БПЛА три методи оцінки впливу комбінованих атак на безпеку системи. Перший метод базується на ймовірності неуспішної атаки, визначаючи ймовірність успішності та тяжкість для кожної послідовної комбінованої атаки. Ймовірність неуспішної атаки розглядається як добуток ймовірностей неуспіху на кожному етапі. Результати наведено у таблиці 3.19.

У роботі [11, 12] та Додатку Д для визначення ймовірності використовувалась шкала від 1 до 10, де 1 відображає найменшу ймовірність, а 10 – найвищу. В контексті послідовних комбінованих атак, де оцінюється ймовірність успішності всіх етапів разом, кожна окрема атака повинна пройти успішно для досягнення загальної мети. Таким чином, ймовірність невдачі будь-якого етапу впливає на загальну ймовірність. В разі невдачі хоча б одного етапу, ймовірність всієї послідовної комбінованої атаки стає 1 (або 100%). Зберігаючи шкалу від 1 до 10, коли всі атаки успішні, ймовірність 1 фактично еквівалентна 10 за шкалою ймовірності. Тоді для такого еквіваленту ймовірності при оцінюванні ризику маємо:

$$P^*_{An} = \left(1 - \left(\left(1\text{-}P_{A_1}\right) \times \left(1\text{-}P_{A_2}\right) \times \left(1\text{-}P_{A_3}\right) \times \ldots \left(1\text{-}P_{A_n}\right)\right)\right) \times 10 \qquad (3.13)$$

$P^*_{A_n}$ використовує шкалу ймовірності від 1 до 10 для визначення цілісного значення успішності послідовної комбінованої атаки. У формулі $P^*_{A_n}$ враховує ймовірність успіху всієї послідовної комбінованої атаки.

$$S^*_{A_n} = \max(S_1,\ldots,S_n) \tag{3.14}$$

$$R^*_{A_n} = P^*_{A_n} \times S^*_{A_n} \tag{3.15}$$

Згідно з результатами в таблиці 3.19, усі розраховані ймовірності та загальний ризик були максимальними (10 або 100%), незалежно від конкретної послідовності атак. Це свідчить про те, що перший метод оцінки критичності системи недостатньо враховує можливі невдачі окремих етапів атак та оптимістично оцінює загальний ризик.

Другий метод використовує фіксовані ймовірності успіху для кожного етапу без врахування можливостей невдачі, що призводить до нереалістичних результатів. Цей підхід спрямований на усунення недоліків першого методу, пропонуючи більш деталізоване визначення ймовірності та тяжкості для кожної атаки. Це дозволяє отримувати більш об'єктивні за певних умов результати при оцінці критичності системи в умовах кібербезпеки (таблиця 3.19).

Таблиця № 3.19 – Критичність СБФ БПЛА після послідовної ККА

№	Послідовність атак	Критичність					
		1 метод			***2 метод***		
		Ймовірність	Тяжкість	Ризик	Ймовірність	Тяжкість	Ризик
1	1, 2, 13, 14, 15	10	10	100	9	10	90
2	1, 3, 24, 25, 26	10	9	90	9	9	81
3	1, 4, 37, 38, 39	10	10	100	9	10	90
4	13, 14, 15, 24, 25	10	10	100	9	10	90
5	13, 14, 15, 36, 37	10	10	100	9	10	90
6	24, 25, 26, 36, 37	10	9	90	9	9	81
7	1, 2, 13, 14	10	9	90	9	9	81
8	1, 2, 13, 14, 15, 36	10	10	100	9	10	90
9	13, 24, 25, 26	10	7	70	9	7	63
10	13, 14, 15, 24, 25, 36	10	10	100	9	10	90

Другий метод не забезпечує повноцінного врахування реалістичності та динаміки кіберзагроз. Ураховуючи це, може бути використано метод, що ґрунтується на максимальному ризику для визначення критичності СБФ БПЛА. Цей метод враховує середнє значення ризику та виокремлює найбільш критичні аспекти та ризики для подальшого підвищення безпеки системи (результати у таблиці 3.20), детальніше Додаток Д [11].

Таблиця № 3.20 – Критичність СБФ БПЛА після послідовної ККА

№	Послідовність атак	Критичність								
		3 метод							***2 метод***	***1 метод***
		R1	R2	R3	R4	R5	R6	Ризик, $R^*_{A_n}$	Ризик	Ризик
1	1, 2, 13, 14, 15	81	48	54	63	60		61,2	90	100
2	1, 3, 24, 25, 26	81	49	42	54	63		57,8	81	90
3	1, 4, 37, 38, 39	81	56	81	72	60		70,0	90	100
4	13, 14, 15, 24, 25	54	63	60	42	54		54,6	90	100
5	13, 14, 15, 36, 37	54	63	60	54	81		62,4	90	100
6	24, 25, 26, 36, 37	42	54	63	54	81		58,8	81	90
7	1, 2, 13, 14	81	48	54	63			61,5	81	90
8	1, 2, 13, 14, 15, 36	81	48	54	63	90	54	65,0	90	100
9	13, 24, 25, 26	54	49	42	63			52,0	63	70
10	13, 14, 15, 24, 25, 36	54	63	60	49	42	54	53,7	90	100

Відповідно до атак у Додатку Д, у таблиці 3.21 відображається комбінація порушників та їх паралельні комбінації атак на систему багатофункційних флотів БПЛА, а таблиця 3.22 містить результати оцінки показників критичності для паралельних ККА на СБФ БПЛА, отримані за третім методом, де бралось максимальне значення ризику та двома іншими.

Результати паралельних комбінованих атак на систему СБФ БПЛА, представлені в таблиці 3.22, детальніше у Додатку Д, дозволяють зробити висновок про можливість реалістичніше враховувати ймовірності та тяжкості кожної атаки, а також їх взаємодію в контексті паралельних комбінацій.

Матриці критичності (МК) СБФ БПЛА при послідовних та паралельних атаках, представлені в таблицях 3.23 – 3.28, відображають результати застосування трьох методів.

Таблиця № 3.21 – Комбінації порушників та їх паралельні ККА на СБФ БПЛА

№	Комб. Поруш.	Паралельні атаки
1	1, 2	13, 14 (спуфінг ідентифікаторів, невиявлене функціонування шпигунського ПЗ)
2	1, 3	24, 25 (підробка ПЗ, впровадження шкідливого коду через вхідні дані)
3	1, 4	36, 37 (SQL ін'єкція, несанкціоноване копіювання або зміна даних)
4	2, 3	18, 19 (розподілена атака на сервіси хмарних сховищ, перехоплення та зміна команд)
5	2, 4	23, 24 (підміна справжніх датчиків, обхід системи виявлення та блокування датчиків)
6	3, 4	32, 33 (підміна авторизованих ідентифікаторів, перехоплення та модифікація команд, що передаються системі управління)

Таблиця № 3.22 – Критичність СБФ БПЛА після паралельних ККА

№	Послідовність атак	Критичність				
		3 метод			***2 метод***	***1 метод***
		R1	R2	Ризик, R^*_{An}	Ризик	Ризик
1	13, 14	54	63	63	63	69
2	24, 25	42	54	54	63	67
3	36, 37	54	81	81	81	89
4	18, 19	63	32	63	72	75
5	23, 24	42	42	42	42	59
6	32. 33	63	56	63	72	85

Таблиця № 3.23 – МК СБФ БПЛА при послідовних ККА за 1 методом

	Тяжкість		
Ймовірність появи	Низька	Середня	Висока
Низька			
Середня			9
Висока			1,2,3,4,5,6,7,8,10

Таблиця № 3.24 – МК СБФ БПЛА для послідовних ККА за 2 методом

	Тяжкість		
Ймовірність появи	Низька	Середня	Висока
Низька			
Середня			9
Висока			1,2,3,4,5,6,7,8,10

Таблиця № 3.25 – МК СБФ БПЛА для послідовних ККА за 3 методом

	Тяжкість		
Ймовірність появи	Низька	Середня	Висока
Низька			7
Середня		2,4,5,6,9	1
Висока	10	8	3

Таблиця № 3.26 – МК СБФ БПЛА для паралельних ККА за 1 методом

	Тяжкість		
Ймовірність появи	Низька	Середня	Висока
Низька			
Середня			
Висока		1,2,5	3,4,6

Таблиця № 3.27 – МК СБФ БПЛА для паралельних ККА за 2 методом

	Тяжкість		
Ймовірність появи	Низька	Середня	Висока
Низька			
Середня		5	
Висока		1,2	3,4,6

Таблиця № 3.28 – МК СБФ БПЛА для паралельних ККА за 3 методом

	Тяжкість		
Ймовірність появи	Низька	Середня	Висока
Низька		2,4	
Середня	5	1,6	
Висока		3	

Слід зауважити, що оцінка критичності системи є складним завданням, залежним від численних факторів, таких як сценарій атак, навички порушника, технічні характеристики системи та експертна оцінка. Критичність може змінюватися в залежності від ситуацій та характеристик обладнання.

3.6 Висновки до розділу

У рамках третього розділу дисертації проведено обґрунтування та реалізацію інтегрованого методу IMECA для аналізу кібербезпеки систем багатофункційних флотів БПЛА.

Розділ розпочинається розгляданням моделі інфраструктури системи багатофункційних флотів БПЛА, включаючи опис елементів IMECA таблиць для аналізу кібербезпеки та структуру цих таблиць. Проведено детальний аналіз ієрархічної структури IMECA таблиць, визначено особливості їх побудови з урахуванням властивостей кібербезпеки.

Далі висвітлено послідовність аналізу кібербезпеки з використанням ієрархічних IMECA таблиць. Наведено принципи та етапи аналізу, що є ключовими для вдосконалення кібербезпеки системи багатофункційних флотів БПЛА.

Досліджено інтегральну оцінку кібербезпеки СБФ БПЛА та визначено особливості IMECA аналізу системи моніторингу критичної інфраструктури за допомогою СБФ БПЛА. Подано етапи аналізу та проведено IMECA-аналіз для критичної інфраструктури.

Окрему увагу приділено особливостям IMECA аналізу кібербезпеки СБФ БПЛА при комбінованих атаках. Розроблено теоретично-математичну модель оцінювання ризиків комбінованих атак та представлено послідовність IMECA аналізу при таких атаках. Результати дослідження можуть слугувати підґрунтям для подальшого вдосконалення та розробки ефективних заходів забезпечення кібербезпеки для систем багатофункційних флотів БПЛА.

Література до розділу

1. Про критичну інфраструктуру: Закон України від 16.11.2021 р. № 1882-IX: станом на 5 груд. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 12.10.2023).

2. Деякі питання об'єктів критичної інфраструктури: Постанова Каб. Міністрів України від 09.10.2020 р. № 1109: станом на 11 трав. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-п#Text (дата звернення: 12.10.2023).

3. Кодекс цивільного захисту України : Кодекс України від 02.10.2012 р. № 5403-VI : станом на 5 жовт. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/5403-17#Text (дата звернення: 12.10.2023).

4. Zemlianko H., Kharchenko V. Cyber Security Systems of Highly Functional Uav Fleets for Monitoring Critical Infrastructure: Analysis of Disruptions, Attacks and Counterapproaches. *Èlektronnoe modelirovanie*. 2024. T. 46, № 1. C. 41–54. URL: https://doi.org/10.15407/emodel.46.01.041.

5. Zheng X., Tan Y., Li D. Navigating Environmental Governance in China's Hog Sector: Unraveling the "Race to the Bottom" Phenomenon and Spatial Dynamics. *Journal of the Knowledge Economy*. 2024. URL: https://doi.org/10.1007/s13132-024-01800-8 (дата звернення: 12.10.2023).

6. Yadin S. The Crowdsourcing of Regulatory Monitoring and Enforcement. *The Law & Ethics of Human Rights*. 2023. T. 17, № 1. C. 95–125. URL: https://doi.org/10.1515/lehr-2023-2006 (дата звернення: 12.10.2023).

7. Нова українська система Menatir для дистанційного моніторингу: базові станції з БПЛА та місії без участі оператора. *ITC.ua*. URL: https://itc.ua/partner-news/novaya-ukraynskaya-systema-menatir-dlya-dystantsyo nnogo-monytorynga-bazovye-stantsyy-s-bpla-y-myssyy-bez-uchastyya-operatora/ (дата звернення: 19.09.2023).

8. Весоловскі Т. Терористична атака 20-річної давності. Як 11 вересня 2001 року змінило світ? *Радіо Свобода*. URL: https://www.radiosvoboda.org/a/terorystychna-ataka-11-veresnya-2001-roku/31452813.html (дата звернення: 22.10.2023).

9. Open-ended working group on developments in the field of information and telecommunications in the context of international security. General Assembly, 2011. 11 с. URL: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (дата звернення: 22.10.2023).

10. Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace. Vienna, Austria: Ueberreuter Print GmbH, 2013. 100 с. URL: https://www.osce.org/files/f/documents/4/b/103500.pdf (дата звернення: 22.10.2023).

11. Землянко Г.А., Харченко В.С. IMECA-аналіз кібербезпеки систем багатофункціональних флотів БПЛА при комбінованих атаках: базові моделі та вибір контрзаходів. *Measuring and computing devices in technological processes*. 2023. № 4. С. 225–233. URL: https://doi.org/10.31891/2219-9365-2023-76-30.

12. Zemlianko H., Kharchenko V. Cybersecurity risk analysis of multifunctional UAV fleet systems: a conceptual model and IMECA-based technique. *Radioelectronic and Computer Systems*. 2023. № 4. С. 152–170. URL: https://doi.org/10.32620/reks.2023.4.11 (дата звернення: 29.01.2024).

РОЗДІЛ 4. РОЗРОБЛЕННЯ ТА ВПРОВАДЖЕННЯ МЕТОДУ І ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СБФ БПЛА

4.1 Постановка задачі та загальна схема методу вибору контрзаходів для забезпечення кібербезпеки СБФ БПЛА за визначеними критеріями

В умовах зростаючої кіберзагрози і з урахуванням багатофункційності безпілотних літальних апаратів, забезпечення кібербезпеки стає пріоритетним завданням. Дане дослідження спрямоване на розробку методу вибору контрзаходів, спрямованих на захист СБФ БПЛА [1-3].

4.1.1 Мета вибору контрзаходів та кількісні показники

У високотехнологічному середовищі систем багатофункціональних флотів безпілотних літальних апаратів (СБФ БПЛА) надзвичайно важливо забезпечити високий рівень кібербезпеки. Ризик-орієнтоване оцінювання кібербезпеки включає в себе аналіз критичних аспектів, таких як ймовірність та тяжкість атак. Перед постановкою завдання вибору контрзаходів для ефективного захисту СБФ БПЛА, важливо визначити оптимальні стратегії та методи захисту, які забезпечать найвищий рівень безпеки та мінімізацію ризиків [4,5].

Згідно 3 розділу, ризик (R) визначається як добуток ймовірності (P) та тяжкості (S) атаки, тобто $R = P * S$. При виборі контрзаходів для забезпечення кібербезпеки СБФ БПЛА, метою вибору контрзаходів полягає в забезпеченні безпеки кіберфізичних систем шляхом зменшення ризику вразливостей та атак. Прийнятний ризик визначається як рівень ризику, який може бути терпимим для організації в контексті її цілей та обмежень. Оцінка прийнятного ризику зазвичай базується на аналізі наслідків можливих загроз та ймовірності їх виникнення [6,7].

Прийнятний ризик - це рівень ризику, який організація або система вважає терпимим у контексті своїх цілей та обмежень. Для оцінки підвищення рівня

кібербезпеки запропоновано використовувати показник відносного зменшення ризиків системи (RDR), який розраховується за формулою:

$$RDR = \left(\frac{IVR-EVR}{IVR}\right) * 100, \quad (4.1)$$

де IVR - інтегральний показник рівня ризиків без застосування контрзаходів, а EVR - інтегральний показник рівня ризиків після впровадження визначеної множини контрзаходів. Показники IVR та EVR розраховуються на основі оцінок критичності кожної атаки.

Для розрахунку показників IVR та EVR необхідно:

– для кожної атаки визначити рівень критичності, використовуючи матрицю критичності;

– розрахувати квантифікований рівень критичності (RVA_i) для кожної атаки;

– сумувати значення RVA_i для отримання IVR та EVR.

Таким чином, IVR - це сума значень RVA_i без застосування контрзаходів, а EVR - сума значень RVA_i після їх впровадження, за формулами 4.2 та 4.3.

$$IVR = \sum IRVA_i \quad (4.2)$$

$$EVR = \sum ERVA_i \quad (4.3)$$

Для ілюстрації обчислення запропонованого показника скористаємося матрицями критичності - таблицями 3.16, 3.17, а також результатами розрахунків квантифікованих значень кіберризиків наданих в Додатку Ґ [7,8].

Показники ризику до і після застосування контрзаходів включають якісні, кількісні і змішані параметри. Якісні показники оцінюються на основі важливості та серйозності загроз для системи. Кількісні показники вимірюються у величинах, таких як ймовірність виникнення атаки та її можливі наслідки. Змішані показники поєднують у собі якісні та кількісні характеристики для комплексної оцінки ризику.

Показники вартості контрзаходів базуються на принципі відносної оцінки, де вартість заходів оцінюється у порівнянні з потенційними збитками від можливої атаки. Цей підхід дозволяє ефективно визначити, які контрзаходи є найбільш

вигідними та ефективними з точки зору витрат та забезпечення безпеки системи, таблиця 4.1 [8].

Таблиця № 4.1 – Шкала оцінки вартості

Критерії	Значення	Шкала
Вартість (Cost)	Безкоштовно	0
	Низька	1-3
	Середня	4-7
	Висока	7-9
	Дуже висока	10

Вартість кожного контрзаходу визначена за шкалою та представлена у таблиці № 4.2.

Таблиця № 4.2 – Вартість 10 контрзаходів для СБФ БПЛА

№	Назва контрзаходу	Вартість (Cost)
1	1. Автоматичне повернення або автоматична робота	7
2	2. Шифрування даних	5
3	3. Мережева безпека	6
4	4. Стійке програмне забезпечення	7
5	5. Фізична безпека	6
6	6. Автентифікація та авторизація	5
7	7. Моніторинг та реагування	6
8	8. Тренування персоналу	4
9	9. Регулярні аудити безпеки	5
10	10. Резервна підсистема відновлення	7

4.1.2 Постановка задачі та критерії вибору контрзаходів

Постановка задачі вибору контрзаходів для забезпечення кібербезпеки включає в себе визначення критеріїв, які допоможуть організації прийняти ефективне рішення.

З огляду на вищесказане, проблема вибору набору контрзаходів за критерієм вартості безпеки виглядає наступним чином: "*Кожному контрзаходу присвоюється рядок у таблиці IMECA, який визначає ймовірність вторгнення та зменшення серйозності (тобто ризик). Необхідно знайти такий набір контрзаходів, для якого залишковий ризик є прийнятним*".

Два основних критерії вибору контрзаходів є:

– прийнятний ризик - мінімальна вартість: Цей критерій передбачає вибір таких контрзаходів, які забезпечують прийнятний рівень ризику за мінімальні можливі витрати. Організація має змогу вибрати найефективніші заходи, які зменшать ризик до прийнятного рівня, при цьому економно використовуючи ресурси.

– прийнятний ризик - мінімальна вартість: Цей критерій передбачає вибір таких контрзаходів, які забезпечують прийнятний рівень ризику за мінімальні можливі витрати. Організація має змогу вибрати найефективніші заходи, які зменшать ризик до прийнятного рівня, при цьому економно використовуючи ресурси.

Особливості постановки задачі при кількісних оцінках ризиків полягають у врахуванні числових значень при оцінці ймовірностей та наслідків кібератак. Використання кількісних методів дозволяє більш точно оцінити ризики та ефективність контрзаходів. При цьому необхідно враховувати якісні аспекти, такі як ступінь критичності імовірних загроз, та об'єктивно оцінювати їх вплив на кібербезпеку системи.

4.1.3 Блок-схема методу вибору контрзаходів

Блок-схема методу вибору контрзаходів за трьома критеріями включає в себе послідовність дій, спрямованих на ефективне забезпечення кібербезпеки системи. Перший критерій, який враховує прийнятний ризик та мінімальну вартість, передбачає аналіз і вибір контрзаходів, які забезпечують прийнятний рівень

безпеки за найменші можливі витрати. Другий критерій, спрямований на обмежену вартість та максимальне зменшення ризику, передбачає вибір заходів, які дозволяють досягти максимального зниження ризику при обмежених фінансових ресурсах.

Третій критерій враховує особливості постановки задачі при кількісних оцінках ризиків, що передбачає використання числових значень для оцінки ймовірностей та наслідків кібератак. Цей критерій вимагає аналізу якісних та кількісних аспектів ризику, зокрема ступеня критичності потенційних загроз та їх впливу на кібербезпеку системи. Блок-схема методу надає структурований підхід до вибору контрзаходів, що сприяє ефективному управлінню ризиками та забезпеченню безпеки кіберфізичних систем, рисунок 4.1.

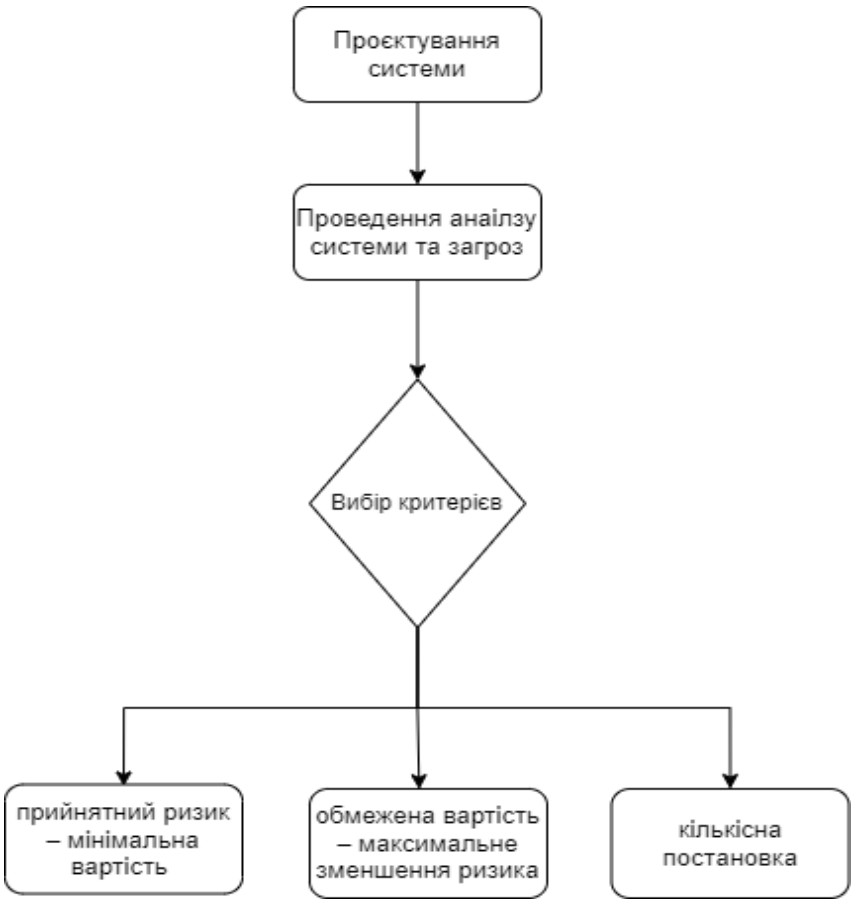


Рисунок 4.1 – Загальна схема методу вибору контрзаходів для забезпечення кібербезпеки СБФ БПЛА за визначеними критеріями

4.1.4 Обґрунтування контрзаходів для забезпечення кібербезпеки СБФ БПЛА

Зниження критичності системи багатофункційних флотів БПЛА від різних атак можна досягти за допомогою різноманітних контрзаходів. Стосовно захисту СБФ БПЛА доцільно сформулювати такі основні методи забезпечення безпеки ОКІ:

1. Автоматичне повернення або автоматична робота: базується на передбаченні системи блокування та автоматичного вимкнення в разі виявлення небажаної поведінки чи атаки. Крім того, він включає підсистему самостійного контролю та автоматичної системи управління. Вибір даного контрзахода обумовлено необхідністю негайного реагування на потенційні загрози та забезпечення безперервності операцій СБФ БПЛА. Типи контрзаходів цієї категорії:

– система блокування: автоматичне призупинення функцій або дій у випадку виявлення аномальних параметрів чи дій;

– автоматичне вимкнення: автоматичне відключення системи або окремих компонентів при виникненні небезпечних ситуацій;

– самостійний контроль: автономна аналізує та оцінює стан безпеки, ініціює заходи у разі виявлення загроз;

– автоматична система управління: механізми, що забезпечують автоматизоване управління СБФ БПЛА в реальному часі на основі аналізу даних та визначених параметрів безпеки.

2. Шифрування даних: передбачає використання шифрування для захисту конфіденційної інформації та підвищення стійкості передачі даних між БПЛА та центрами управління. Обрано з метою запобігання несанкціонованому доступу та збереження конфіденційності даних. Типи контрзаходів цієї категорії:

– шифрування даних в покритті: захист інформації шляхом застосування шифрувальних алгоритмів під час передачі через мережі;

– шифрування в пам'яті: захист конфіденційних даних, збережених у пам'яті пристроїв, використовуючи шифрувальні методи;

– шифрування каналу зв'язку: застосування шифрування для захисту каналів зв'язку між БПЛА та центрами управління.

3. Мережева безпека: передбачає впровадження ефективних засобів мережевої безпеки для виявлення та блокування небезпечних мережевих атак. Вибір обумовлено потребою у захисті від вражень, що виникають в мережевому середовищі, та забезпечення цілісності і доступності інформації. Типи контрзаходів цієї категорії:

– виявлення вторгнень: системи, що аналізують трафік та виявляють невідомі чи аномальні патерни, ініціюючи заходи при необхідності;

– брандмауери та фільтри: засоби, які контролюють та обмежують мережевий трафік для запобігання небажаним з'єднанням чи атакам;

– інтегровані засоби безпеки мережі: використання комплексу технічних та програмних рішень для захисту мережевої інфраструктури.

4. Стійке програмне забезпечення: включає в себе використання стійкого програмного забезпечення, оновлення та патчі для запобігання використанню вразливостей. Цєй контрзаход важлив для усунення можливих слабких місць в програмному коді та запобігання експлуатації атаками. Типи контрзаходів цієї категорії:

– регулярні оновлення: забезпечення своєчасного встановлення оновлень та патчів для програмного забезпечення;

– використання захисних бібліотек: інтеграція захисних бібліотек та фреймворків для зменшення ризиків вразливостей;

– статичний та динамічний аналіз коду: проведення аналізу програмного коду для виявлення та усунення потенційних вразливостей.

5. Фізична безпека: орієнтована на забезпечення фізичного захисту систем, що передбачає надійний захист пристроїв та контроль доступу від пошкодження та втручання у апаратні пристрої системи. Вибір обумовлений необхідністю у

запобіганні фізичним загрозам та втручанням у апаратні компоненти. Типи контрзаходів цієї категорії:

– фізичний контроль доступу: застосування систем контролю доступу та моніторингу для обмеження фізичного доступу до інфраструктури;

– захист обладнання від пошкоджень: використання захисних оболонок та систем охорони для запобігання фізичним пошкодженням пристроїв.

6. Автентифікація та авторизація: передбачає використання сильних методів автентифікації і авторизації для обмеження доступу до систем управління БПЛА. Вибір базується на важливості контролю за доступом до критичних ресурсів. Типи контрзаходів цієї категорії:

– двофакторна аутентифікація: використання двох і більше методів підтвердження ідентичності користувача;

– ролева модель доступу: визначення чітких ролей та прав доступу для кожного користувача чи системи.

7. Моніторинг та реагування: передбачає постійний моніторинг систем з метою швидкого виявлення аномальної поведінки або підозрілих активностей. Цей захід обран для забезпечення оперативного виявлення потенційних загроз і вчасної реакції на них. Типи контрзаходів цієї категорії:

– системи виявлення вторгнень (IDS): використання спеціалізованих систем для виявлення аномальної активності чи зловмисних дій;

– автоматизовані системи реагування: розробка систем, які можуть автоматично реагувати на виявлені загрози без втручання оператора.

8. Тренування персоналу: передбачає навчання персоналу щодо кібербезпеки, викриття соціального інжинірингу та відповідальності за безпеку інформації. Цей контрзахід важлив для забезпечення свідомості та високої кваліфікації персоналу. Типи контрзаходів цієї категорії:

– симуляції атак: проведення тренувань з використанням сценаріїв імітації реальних кібератак;

– освітні програми з кібербезпеки: надання персоналу інформації та навичок у сфері кібербезпеки.

9. Регулярні аудити безпеки: передбачає проведення періодичних аудитів безпеки для ідентифікації слабких місць та вжиття заходів для їх виправлення. Обран для постійного контролю за станом безпеки системи. Типи контрзаходів цієї категорії:

– технічні аудити: перевірка технічних параметрів та конфігурацій для виявлення потенційних вразливостей;

– аудити безпеки коду: перевірка програмного забезпечення на наявність вразливостей та помилок.

10. Резервна підсистема відновлення: передбачає спрацювання локальної системи відновлення під час аварійних випадків. Обран для забезпечення надійності та збереження даних. Типи контрзаходів цієї категорії:

– автоматизована система резервного копіювання: системи, які автоматично створюють резервні копії даних;

– ізольовані резервні системи: використання фізично відокремлених систем для зберігання даних та можливість швидкого відновлення.

Ці контрзаходи обрані для забезпечення комплексного захисту системи багатофункційних флотів БПЛА, враховуючи різноманітність потенційних кіберзагроз та фізичних атак.

4.2 Алгоритми вибору контрзаходів

Алгоритми вибору контрзаходів представляють собою систематичні процедури, спрямовані на забезпечення кібербезпеки системи з урахуванням різних аспектів та обмежень. Перший алгоритм, орієнтований на прийнятний ризик та мінімальну вартість, включає аналіз інфраструктури та оцінку загроз, визначення рівня критичності та формування множини контрзаходів на основі матриць критичності. Другий алгоритм спрямований на обмежену вартість та максимальне

зменшення ризику, що передбачає врахування фінансових обмежень та пошук ефективних контрзаходів, спроможних мінімізувати загрози. Третій алгоритм, зосереджений на особливостях постановки задачі при кількісних оцінках ризиків, включає аналіз якісних та кількісних аспектів ризику та врахування їх у процесі вибору контрзаходів.

4.2.1 Алгоритм пошуку приємного ризику за мінімальною вартістю

Перший алгоритм націлений на досягнення оптимального балансу між прийнятним рівнем ризику та мінімальною вартістю контрзаходів у контексті забезпечення кібербезпеки системи. Початковим етапом процесу є детальний аналіз інфраструктури та оцінка потенційних загроз безпеці системи. Цей аналіз включає ідентифікацію можливих вразливостей, потенційні шляхи їх можливого використання та різноманітні типи можливих кібератак.

Далі, у рамках алгоритму формується IMECA, визначаються критичні елементи системи. Для кожного з цих елементів визначається рівень критичності у контексті можливих загроз та вразливостей, враховуючи їх потенційний вплив на безпеку системи.

Після цього застосовуються матриці критичності для визначення загального рівня критичності системи, що відображає сумарний вплив потенційних атак на безпеку системи. Залежно від цього рівня, формується множина потенційних контрзаходів, які можуть бути використані для зменшення ризику.

Наступним кроком є аналіз кожного потенційного контрзаходу та його впливу на систему, враховуючи вартість впровадження. Після ранжування та оцінки вартості кожного контрзаходу обирається та, яка забезпечує прийнятний ризик за мінімальні витрати. Такий підхід дозволяє раціонально використовувати ресурси та ефективно забезпечувати кібербезпеку системи, зменшуючи можливі ризики та мінімізуючи витрати.

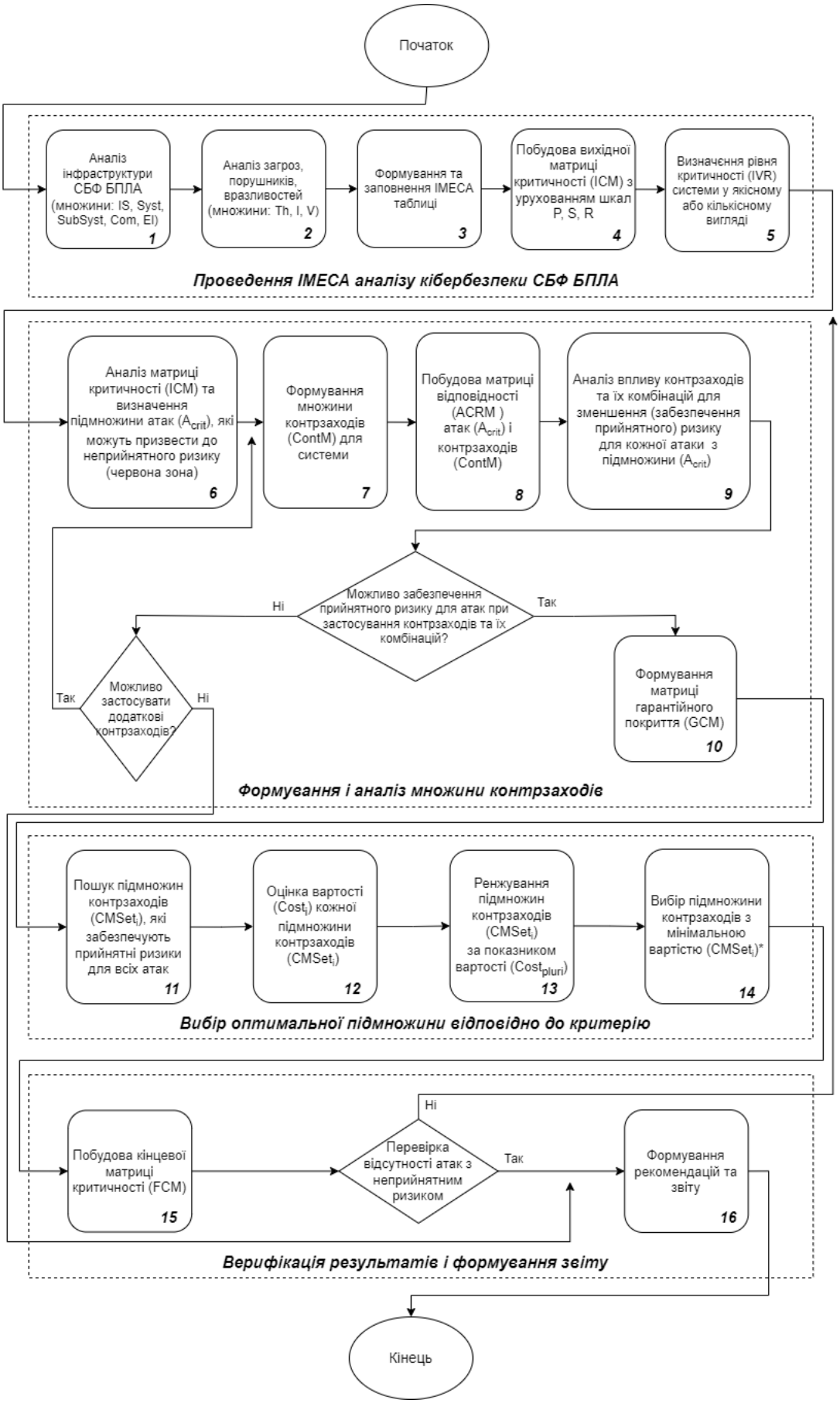


Рисунок 4.2 – Алгоритм пошуку приємного ризику за мінімальною вартістю

4.2.2 Алгоритм пошуку обмежена вартість – максимальне зменшення ризика

Другий алгоритм ставить перед собою завдання забезпечення максимального зменшення ризику для системи при обмежених витратах на контрзаходи. Цей процес починається з аналізу інфраструктури та ідентифікації потенційних загроз, ворожих дій та вразливостей, що можуть вплинути на безпеку системи. На основі цього аналізу формується IMECA, а також створюються матриці критичності, які враховують різні аспекти кібербезпеки.

Після проведення оцінки рівня критичності кожного потенційного ризику та аналізу матриць критичності та їх підмножин надається можливість визначити, які конкретні аспекти безпеки системи є найбільш критичними та вимагають негайних заходів забезпечення безпеки. Цей процес дозволяє ідентифікувати найбільш значущі вразливості та потенційні загрози, які можуть призвести до серйозних наслідків для системи.

На основі отриманих даних формується множина потенційних контрзаходів, які можуть бути використані для максимального зменшення ризику для системи при обмежених витратах. Ці контрзаходи можуть включати технічні, організаційні та процедурні заходи, спрямовані на усунення виявлених вразливостей та запобігання можливим атакам.

Після оцінки ефективності кожного потенційного контрзаходу та їх можливих комбінацій здійснюється вибір підмножини, яка забезпечує максимальне зменшення ризику для системи при заданій обмеженій вартості. Цей підхід дозволяє раціонально використовувати ресурси та забезпечувати оптимальний рівень кібербезпеки системи, уникнувши зайвих витрат та максимізуючи ефективність вжитих заходів. Такий систематичний аналіз допомагає забезпечити ефективний захист системи від кіберзагроз.

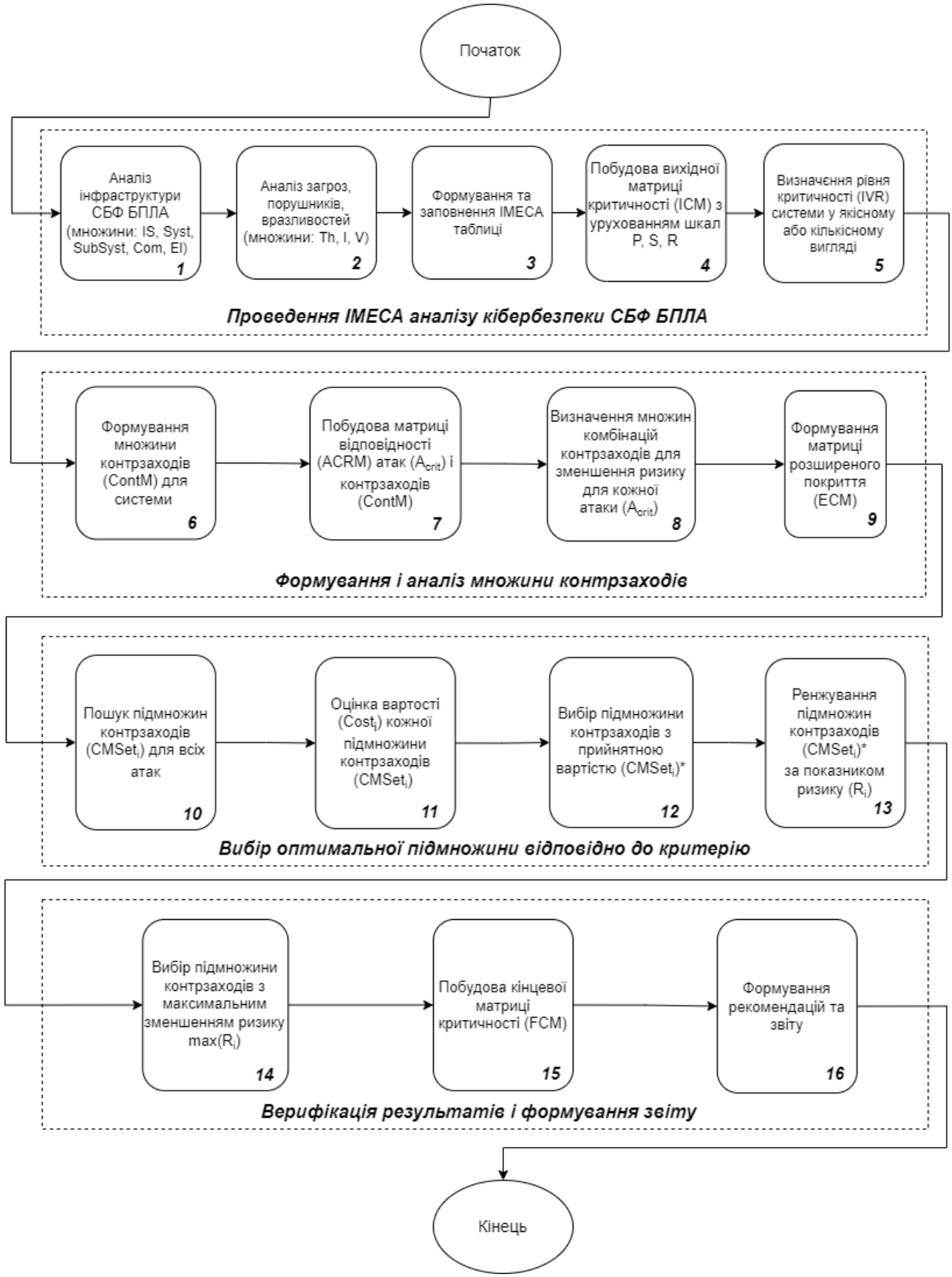


Рисунок 4.3 – Алгоритм пошуку обмежена вартість – максимальне зменшення ризика

4.2.3 Алгоритм пошуку приємного ризику за мінімальною вартістю та кількісного значення прийнятного ризику

Алгоритм, на рисунку 4.4, спрямований на вирішення задач, пов'язаних з кількісним оцінюванням ризиків і врахуванням особливостей цього процесу. Початковим кроком є детальний аналіз структури системи та ідентифікація потенційних загроз, порушників і вразливостей, включаючи вимірювання їхнього впливу на безпеку системи. Зокрема, враховуються різні аспекти кібербезпеки, такі як конфіденційність, цілісність, доступність та спостережність.

Далі проводиться формування IMECA та створення матриць критичності, що відображають рівень ризику для різних атак та вразливостей. Однак, особливістю цього алгоритму є здатність враховувати кількісні показники ризиків, а не лише категоріальні оцінки. Це означає, що для кожної атаки або вразливості проводиться числове оцінювання ризику, що дозволяє точніше визначити його вплив на систему.

Після проведення аналізу матриць критичності та їх підмножин здійснюється цілеспрямована ідентифікація ефективних контрзаходів з урахуванням кількісних оцінок ризиків. Цей етап дозволяє детально вивчити та оцінити рівень потенційних загроз для системи та вибрати оптимальні заходи для її захисту.

Метою такого аналізу є вибір стратегій захисту, які найбільш ефективно зменшать ризики для системи при мінімальних витратах ресурсів. Підходящі контрзаходи обираються з урахуванням їхньої можливої ефективності та вартості реалізації.

Враховуючи кількісні оцінки ризиків, такий підхід дозволяє точніше визначити потреби системи у захисті та забезпечити її оптимальний рівень безпеки. При цьому мінімізуються витрати ресурсів на впровадження контрзаходів, що робить стратегію захисту більш ефективною та економічно обгрунтованою. Такий підхід сприяє підвищенню загального рівня кібербезпеки системи та зменшенню її вразливості перед потенційними загрозами.

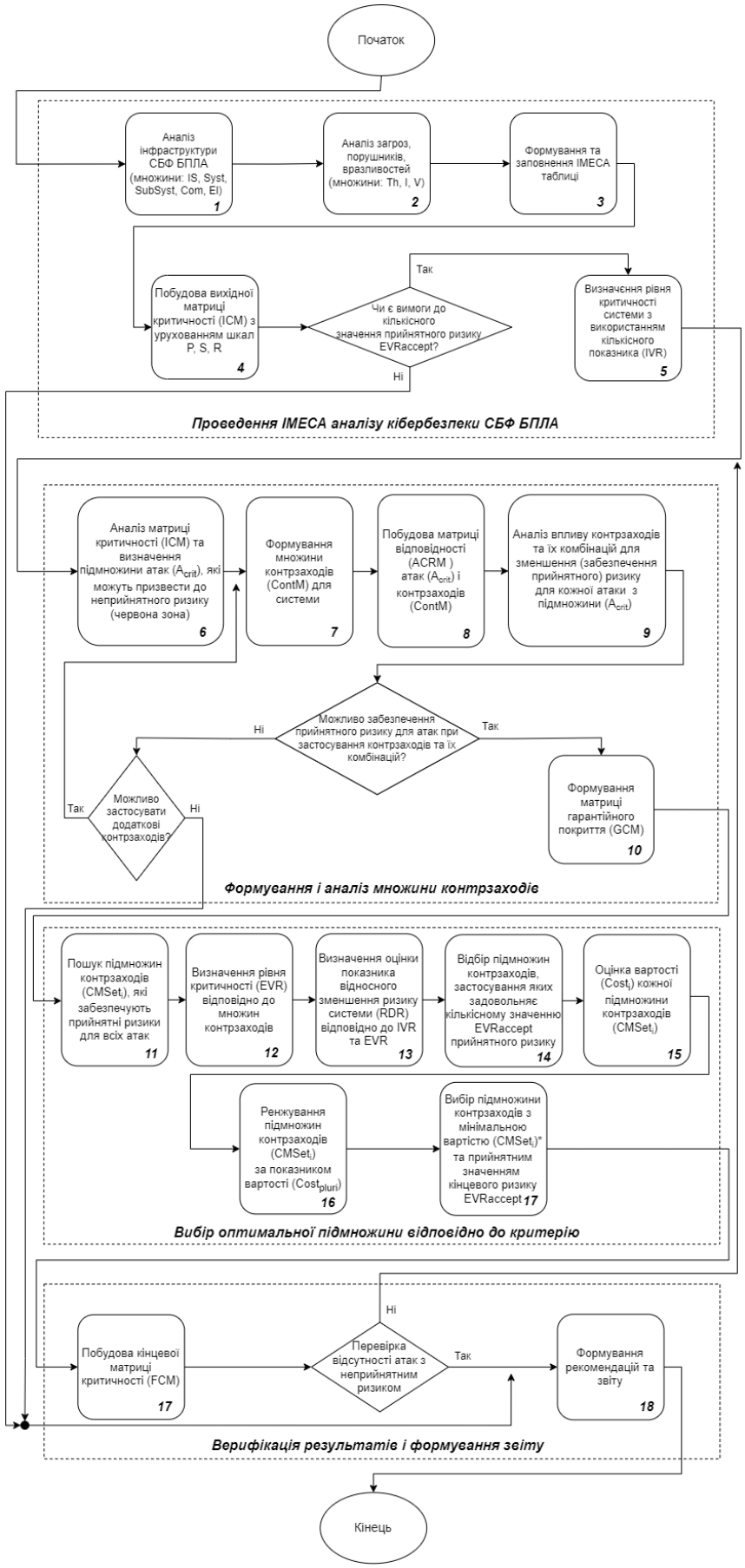


Рисунок 4.4 – Алгоритм пошуку приємного ризику за мінімальною вартістю та кількісного значення прийнятного ризику

4.2.4 Вибір контрзаходів для забезпечення кібербезпеки з використанням алгоритму прийнятний ризик – мінімальна вартість

Починаючи з аналізу інфраструктури та ідентифікації потенційних загроз, атак і вразливостей системи, формується таблиця IMECA, що відображає різні сценарії атак та їх вплив на безпеку, згідно Додатку Ґ [8].

Паралельно створюється матриця відповідності, в якій кожна комірка показує можливість використання певної комбінації контрзаходів для кожної атаки. Це дозволяє систематизувати і відбирати оптимальні заходи захисту для кожного типу загрози, рисунок 4.5.

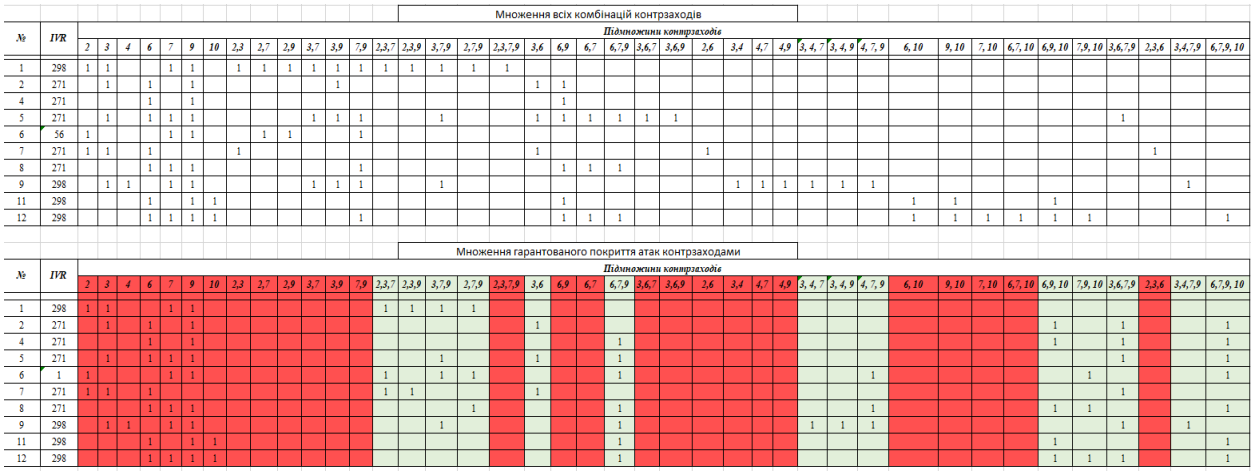


Рисунок 4.5 – Матриця відповідності кожної підмножини контрзаходів

Після цього на основі експертних оцінок і аналітичних даних формується матриця гарантійного покриття, рисунок 4.5, де кожна комірка вказує, чи забезпечує відповідна комбінація контрзаходів прийнятний ризик. Цей етап важливий для відбору ефективних стратегій захисту, які забезпечать найвищий рівень безпеки системи при мінімальних витратах. Після цього було сформовано список комбінацій контрзаходів: 2,3,7; 2,3,9; 3,7,9; 2,7,9; 3,6; 6,7,9; 3,4,7; 3,4,9; 4,7,9; 6,9,10; 7,9,10; 3,6,7,9; 3,4,7,9; 6,7,9,10.

Після проведеного вибору і аналізу, виконується заміна змінних на їх значення. Для цього використовуються наступні значення змінних: a: 2,3,7; b: 2,3,9;

c: 3,7,9; d: 2,7,9; e: 3,6; f: 6,7,9; h: 3,4,7; k: 3,4,9; p: 4,7,9; q: 6,9,10; r: 7,9,10; s: 3,6,7,9; t: 3,4,7,9; z: 6,7,9,10. Після цього ми отримаємо вираз: (fVqVz)Λ(aVbVcVd)Λ(aVbVeVs)Λ(eVqVsVz)Λ(fVqVsVz)Λ(cVeVfVsVz)Λ(fVqVrVsVz)Λ(dVfVpVqVrVz)Λ(aVcVdVfVpVrVz)Λ(cVfVhVkVpVsVt). Для зменшення кількості комбінацій у даному виразі математичної логіки було вирішено використовувати закони дистрибутивності, асоціативності та комутативності логічних операцій.

На наступному етапі переписується вираз з урахуванням цих значень змінних. В результаті отримуємо наступне вираження:

((6,7,9)V(6,9,10)V(6,7,9,10))Λ((2,3,7)V(2,3,9)V(3,7,9)V(2,7,9))Λ((2,3,7)V(2,3,9)V(3,6)V(3,6,7,9))Λ((3,6)V(6,9,10)V(3,6,7,9)V(6,7,9,10))Λ((6,7,9)V(6,9,10)V(3,6,7,9)V(6,7,9,10))Λ((3,7,9)V(3,6)V(6,7,9)V(3,6,7,9)V(6,7,9,10))Λ((6,7,9)V(6,9,10)V(7,9,10)V(3,6,7,9)V(6,7,9,10))Λ((2,7,9)V(6,7,9)V(4,7,9)V(6,9,10)V(7,9,10)V(6,7,9,10))Λ((2,3,7)V(3,7,9)V(2,7,9)V(6,7,9)V(4,7,9)V(7,9,10)V(6,7,9,10))Λ((3,7,9)V(6,7,9)V(3,4,7)V(3,4,9)V(4,7,9)V(3,6)V(3,4,7,9))

Зазначимо, що багато частин виразу повторюються, тому можемо спростити його, об'єднуючи однакові частини:

– (6,7,9)V(6,9,10)V(6,7,9,10) можна записати як (6,7,9,10);

– (2,3,7)V(2,3,9)V(3,7,9)V(2,7,9) можна записати як (2,3,7,9);

– (3,6)V(6,9,10)V(3,6,7,9)V(6,7,9,10) можна записати як (3,6,7,9,10);

– (4,7,9)V(7,9,10)V(3,4,7)V(3,4,9) можна записати як (3,4,7,9,10).

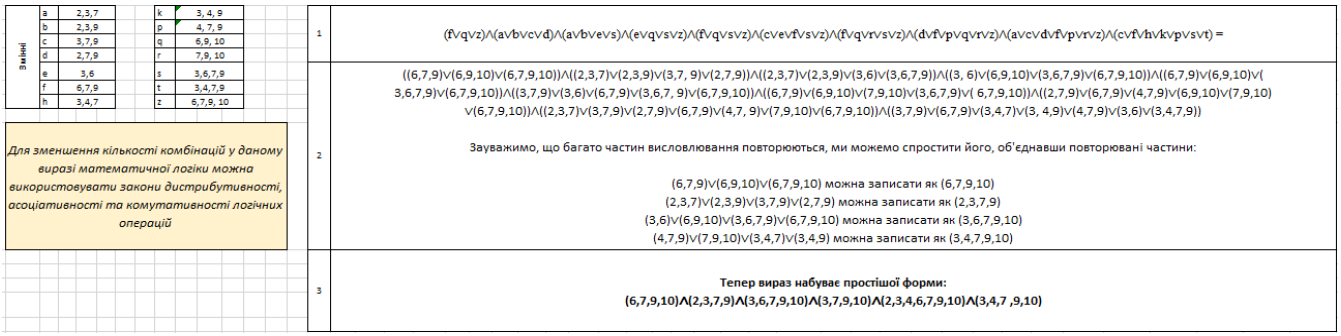
Отримане вираження набуває більш простої форми:

(6,7,9,10)Λ(2,3,7,9)Λ(2,3,7,9)Λ(3,6,7,9,10)Λ(6,7,9,10)Λ(3,7,9,10)Λ(2,3,4,6,7,9,10)Λ(2,3,4,6,7,9,10)Λ(3,4,7,9,10)

Ця спрощена форма дозволяє зменшити кількість комбінацій у виразі, залишаючи його еквівалентним вихідному, як показано на рисунку 4.6.

За отриманами результатами з отриманих підмножин контрзаходів відбувається процес підрахунку вартості з метою виявлення таких, що забезпечують прийнятний рівень ризику з мінімальною вартістю, рисунок 4.7.

Після проведення зведення данних і розрахунків у таблицю, рисунок 4.7, вони ранжуються за критерієм мінімальної вартості. Це дозволяє визначити та впровадити такі стратегії, які забезпечують ефективний захист системи від потенційних загроз з мінімальними витратами ресурсів. Такий підхід допомагає оптимізувати процес забезпечення безпеки та знижує ймовірність виникнення інцидентів або недоліків у роботі системи.



Змінні		
	a	2,3,7
	b	2,3,9
	c	3,7,9
	d	2,7,9
	e	3,6
	f	6,7,9
	h	3,4,7

	k	3, 4, 9
	p	4, 7, 9
	q	6,9, 10
	r	7,9, 10
	s	3,6,7,9
	t	3,4,7,9
	z	6,7,9, 10

Для зменшення кількості комбінацій у даному виразі математичної логіки можна використовувати закони дистрибутивності, асоціативності та комутативності логічних операцій

1	(fVqVz)Λ(aVbVcVd)Λ(aVbVevs)Λ(evqVsVz)Λ(fVqVsVz)Λ(cVevfVsVz)Λ(fVqVrVsVz)Λ(dVfVpVqVrVz)Λ(aVcVdVfVpVrVz)Λ(cVfVhVkVpVsVt) =
2	((6,7,9)V(6,9,10)V(6,7,9,10))Λ((2,3,7)V(2,3,9)V(3,7, 9)V(2,7,9))Λ((2,3,7)V(2,3,9)V(3,6)V(3,6,7,9))Λ((3, 6)V(6,9,10)V(3,6,7,9)V(6,7,9,10))Λ((6,7,9)V(6,9,10)V(3,6,7,9)V(6,7,9,10))Λ((3,7,9)V(3,6)V(6,7,9)V(3,6,7, 9)V(6,7,9,10))Λ((6,7,9)V(6,9,10)V(7,9,10)V(3,6,7,9)V(6,7,9,10))Λ((2,7,9)V(6,7,9)V(4,7,9)V(6,9,10)V(7,9,10) V(6,7,9,10))Λ((2,3,7)V(3,7,9)V(2,7,9)V(6,7,9)V(4,7, 9)V(7,9,10)V(6,7,9,10))Λ((3,7,9)V(6,7,9)V(3,4,7)V(3, 4,9)V(4,7,9)V(3,6)V(3,4,7,9)) Зауважимо, що багато частин висловлювання повторюються, ми можемо спростити його, об'єднавши повторювані частини: (6,7,9)V(6,9,10)V(6,7,9,10) можна записати як (6,7,9,10) (2,3,7)V(2,3,9)V(3,7,9)V(2,7,9) можна записати як (2,3,7,9) (3,6)V(6,9,10)V(3,6,7,9)V(6,7,9,10) можна записати як (3,6,7,9,10) (4,7,9)V(7,9,10)V(3,4,7)V(3,4,9) можна записати як (3,4,7,9,10)
3	**Тепер вираз набуває простішої форми:** **(6,7,9,10)Λ(2,3,7,9)Λ(3,6,7,9,10)Λ(3,7,9,10)Λ(2,3,4,6,7,9,10)Λ(3,4,7 ,9,10)**

Рисунок 4.6 – Процесс пошуку підмножин, які забезпечують прийнятний ризик

№	Комбінация контрзаходів							Вартість кожної							Вартість комбінації
								2	3	4	6	7	9	10	
1	6	7	9	10							5	6	5	7	23
2	2	3	7	9				5	6			6	5		22
3	3	6	7	9	10				6		5	6	5	7	29
4	3	7	9	10					6			6	5	7	24
5	2	3	4	6	7	9	10	5	6	7	5	6	5	7	41
6	3	4	7	9	10				6	7		6	5	7	31

№	Комбінация контрзаходів							Вартість комбінації	
1	6	7	9	10				23	мінімальна
2	2	3	7	9				**22**	мінімальна
3	3	6	7	9	10			29	
4	3	7	9	10				24	
5	2	3	4	6	7	9	10	41	надлишкова
6	3	4	7	9	10			31	надлишкова

Рисунок 4.7 – Ранжування контрзаходів за першим критерієм

Під кінець отримує підмножини або підмножину, яка забезпечує та задовольняє обраний крітерій. За цим прикладом, після отриманих результатов було виявлено, що за критеріям прийнятний ризик - манімальна вартість, підходять 2 комбінації контрзаходів, які зменшать ризик атак від першого порушника: 6,7,9,10 та 2,3,7,9. Такий підхід дозволяє системам ефективно відповідати на загрози кібербезпеки, забезпечуючи оптимальне співвідношення між безпекою та вартістю заходів захисту.

4.3 Інструментальний засіб для оцінювання та забезпечення кібербезпеки СБФ БПЛА

На базі отриманих результатів з аналізу та досліджень кібербезпеки СБФ БПЛА був розроблений засіб, що допомагає експертам з кібербезпеки провести оцінювання інфраструктури СБФ БПЛА, її елементів, розглянути можливі атаки на систему, їх наслідки та побудувати матриці критичності для отриманням загальної структури ймовірності та тяжкості атак на СБФ БПЛА відносно атакам.

4.3.1 Загальний характеристика

Розроблення застосунку виконувалося на мові C# з використанням технологій та бібліотек .Net Framework. Дане рішення надає безліч можливостей і готових рішень стандартних завдань, які виникають при розробці будь-якого програмного забезпечення. Архітектура програми представлена у виді діаграми класів на рисунку 4.8. Це дає можливість більш легко розширювати архітектуру програми і легко змінювати окремі її компоненти.

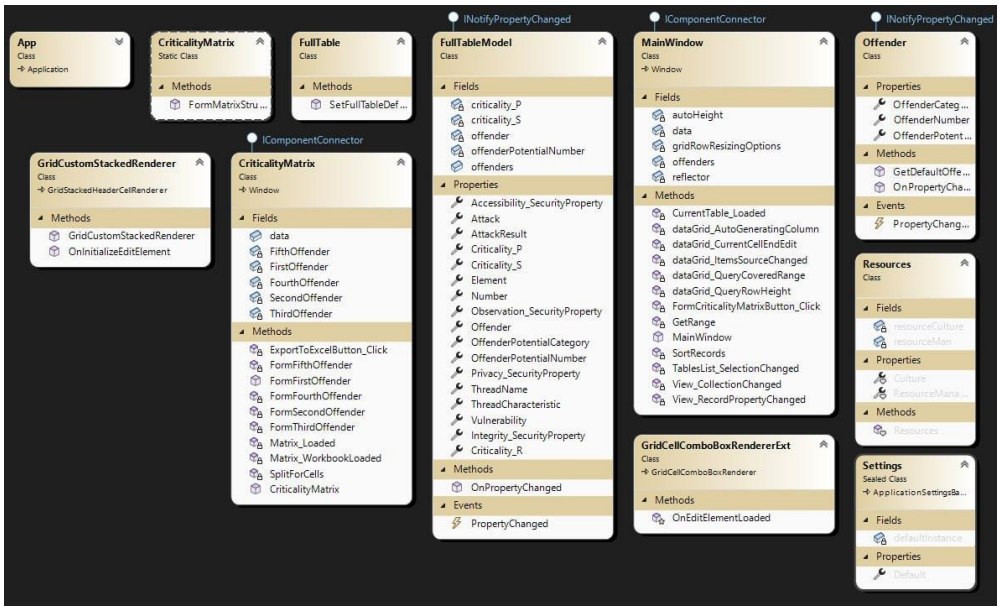


Рисунок 4.8 – Діаграми класів застосунку

Діаграма варіантів використання застосунку представлена на рис. 4.9. Дана діаграма показує, як за допомогою засобу відбувається створення проекту інфраструктури для БПЛА. Основні кроки включають:

1. Формування проекту: додавання відомостей про характеристики системи, включення технічних даних про БПЛА та їх інфраструктуру.

2. Формування таблиці IMEKA: ідентифікація та оцінка інформаційних ризиків, ідентифікація слабких місць у системі, визначення потенційних загроз безпілотним літальним апаратам, визначення можливих наслідків атак.

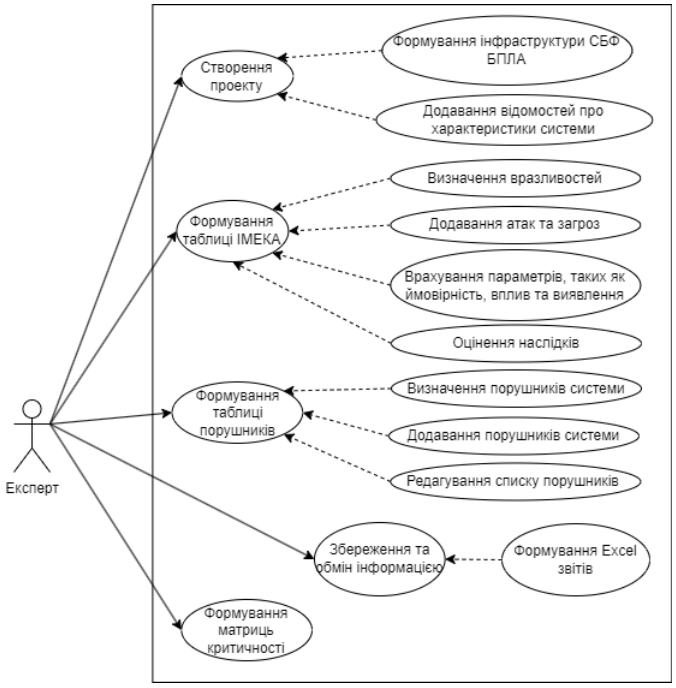


Рисунок 4.9 – Діаграми варіантів використання застосунку

3. Формування таблиці порушників: ідентифікація потенційних порушників системи.

4. Формування матриць критичності: оцінка важливості ризиків та вплив атак на систему.

5. Збереження та обмін інформацією: забезпечення збереження та обміну даними про проект, формування Excel звітів.

Модуль бізнес-логіки був реалізований декількома компонентами, функціональність яких розділена за такими категоріями:

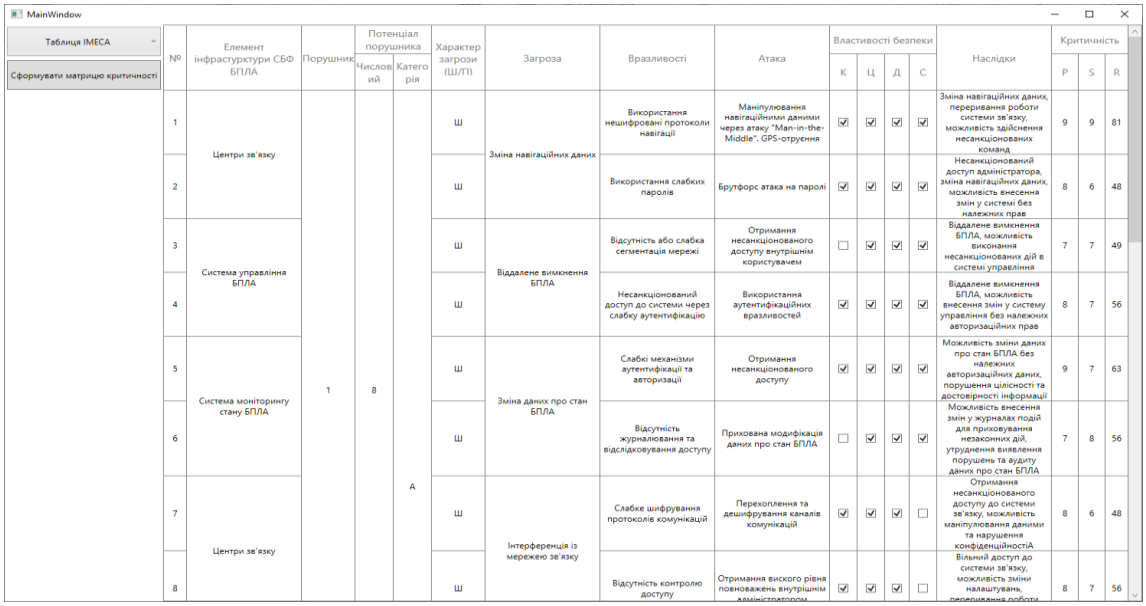
– Реалізація IMECA таблиць і матриць критичності;

– Зберігання даних;

– Інтерфейс бізнес-логіки для графічного інтерфейсу.

4.3.2 Інтерфейс засобу

Інтерфейс програми зображений на рис. 4.10. Для початку роботи програми відкривається екран за замовчуванням с шаблоном IMECA-таблиці. Двома кліками по таблиці відкривається можливість додавання інформації про загрози, вразливості, атаки та іншу інформацію. У експерта з'являється можливість додати всю необхідну інформацію по інфраструктурі СБФ БПЛА.



№	Елемент інфраструктури СБФ БПЛА	Порушник	Потенціал порушника		Характер загрози (Ш/П)	Загроза	Вразливості	Атака	Властивості безпеки				Наслідки	Критичність		
			Числовий	Категорія					К	Ц	Д	С		Р	S	R
1	Центри зв'язку	1	8	А	Ш	Зміна навігаційних даних	Використання нешифровані протоколи навігації	Маніпулювання навігаційними даними через атаку "Man-in-the-Middle", GPS-отруєння	☑	☑	☑	☑	Зміна навігаційних даних, переривання роботи системи зв'язку, можливість здійснення несанкціонованих команд.	9	9	81
2					Ш		Використання слабких паролів	Брутфорс атака на паролі	☑	☑	☑	☑	Несанкціонований доступ адміністратора, зміна навігаційних даних, можливість внесення змін у системі без належних прав	8	6	48
3	Система управління БПЛА				Ш	Віддалене вимкнення БПЛА	Відсутність або слабка сегментація мережі	Отримання несанкціонованого доступу внутрішнім користувачем	☐	☑	☑	☑	Віддалене вимкнення БПЛА, можливість виконання несанкціонованих дій в системі управління	7	7	49
4					Ш		Несанкціонований доступ до системи через слабку аутентифікацію	Використання аутентифікаційних вразливостей	☑	☑	☑	☑	Віддалене вимкнення БПЛА, можливість внесення змін у систему управління без належних авторизаційних прав	8	7	56
5	Система моніторингу стану БПЛА				Ш	Зміна даних про стан БПЛА	Слабкі механізми аутентифікації та авторизації	Отримання несанкціонованого доступу	☑	☑	☑	☑	Можливість зміни даних про стан БПЛА без належних авторизаційних даних, порушення цілісності та достовірності інформації	9	7	63
6					Ш		Відсутність журналювання та відслідковування доступу	Прихована модифікація даних про стан БПЛА	☐	☑	☑	☑	Можливість внесення змін у журналах подій для приховування незаконних дій, утруднення виявлення порушень та аудиту даних про стан БПЛА	7	8	56
7	Центри зв'язку				Ш	Інтерференція із мережею зв'язку	Слабке шифрування протоколів комунікацій	Перехоплення та дешифрування каналів комунікацій	☑	☑	☑	☐	Отримання несанкціонованого доступу до системи зв'язку, можливість маніпулювання даними та нарушення конфіденційностіА	8	6	48
8					Ш		Відсутність контролю доступу	Отримання виского рівня повноважень внутрішнім адміністратором	☑	☑	☑	☐	Вільний доступ до системи зв'язку, можливість зміни налаштувань, переривання роботи	8	7	56

Рисунок 4.10 – Інтерфейс головного вікна застосунку

Для змінення інформації про порушників необхідно в лівій панелі зверху обрати в випадаючому списку таблицю порушників і там експерт знову двома кліками може редагувати та додовати інформацію про порушника та його потенціал. Результат дії зображений на рис. 4.11.

Після цього можна повертатись на головну сторінку. Для визначення допустимих значень критичності в системі СБФ БПЛА необхідно натиснути кнопку «Сформувати матрицю критичності». Результат показаний на рис. 4.12.

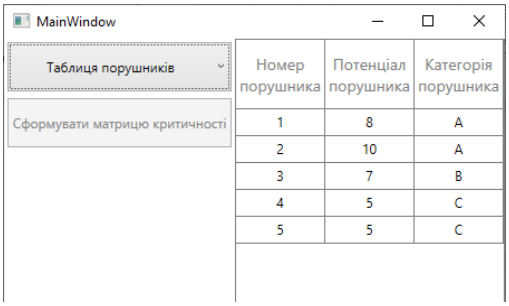


Рисунок 4.11 – Інтерфейс вікна інформації про порушників

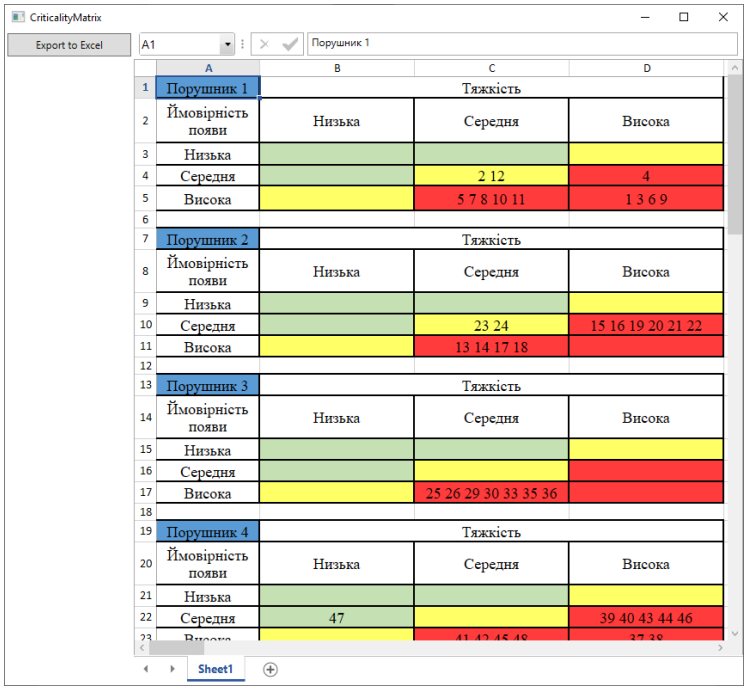


Рисунок 4.12 – Інтерфейс вікна з матрицями критичності

Після цього застосунок з отриманої до цього інформації в IMECA-таблиці сформує матриці, які будуть мати три кольори: зелений, жовтий та червоний, де будуть прописані номери атак, що буде означати прийнятне значення ключових полів таблиці, залежності від ймовірності та тяжкості реалізації їх у СБФ БПЛА. Після закінчення розглядання отриманих результатів, необхідно натиснути кнопку «Export to Excel», щоб загрузити собі на пристрій отриманні результати.

4.4 Технологія оцінювання та забезпечення кібербезпеки СБФ БПЛА

Загальна функціональна модель інформаційної технології, яка базується на запропонованих моделях та методах забезпечення кібербезпеки СБФ БПЛА при комбінованих атаках, наведена на рис. 4.13 у вигляді IDEF0-діаграми.

Після декомпозиція IDEF0-діаграма перейшла на IDEF1-діаграму, рисунок 4.14, яка складається з 4 етапів:

– етап 1: визначення вимог та компонентів системи;

– етап 2: визначення показників кібербезпеки системи при одиночних та комбінованих атаках;

– етап 3: аналіз кіберзагроз, наслідків та критичності одиночних і комбінованих атак на активи кіберфізичної системи;

– етап 4: вибір контрзаходів для забезпечення кібербезпеки активів кіберфізичної системи.

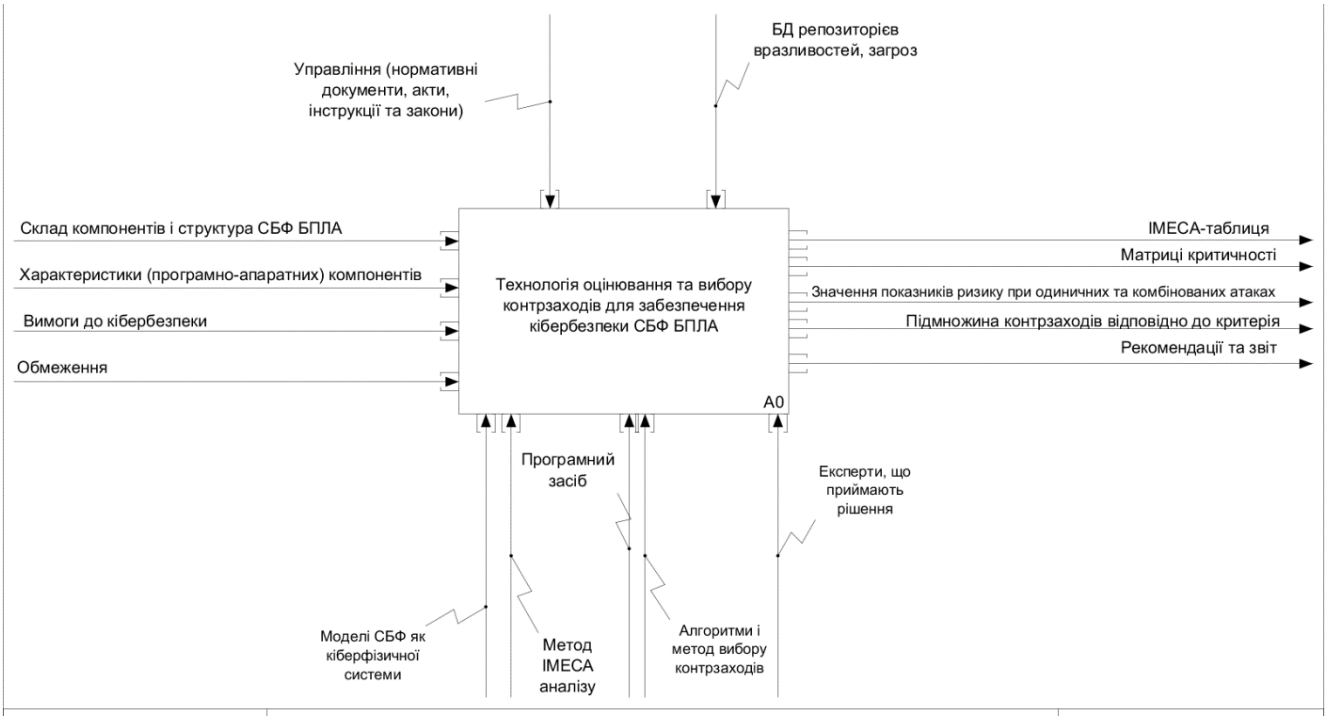


Рисунок 4.13 – IDEF0-діаграма

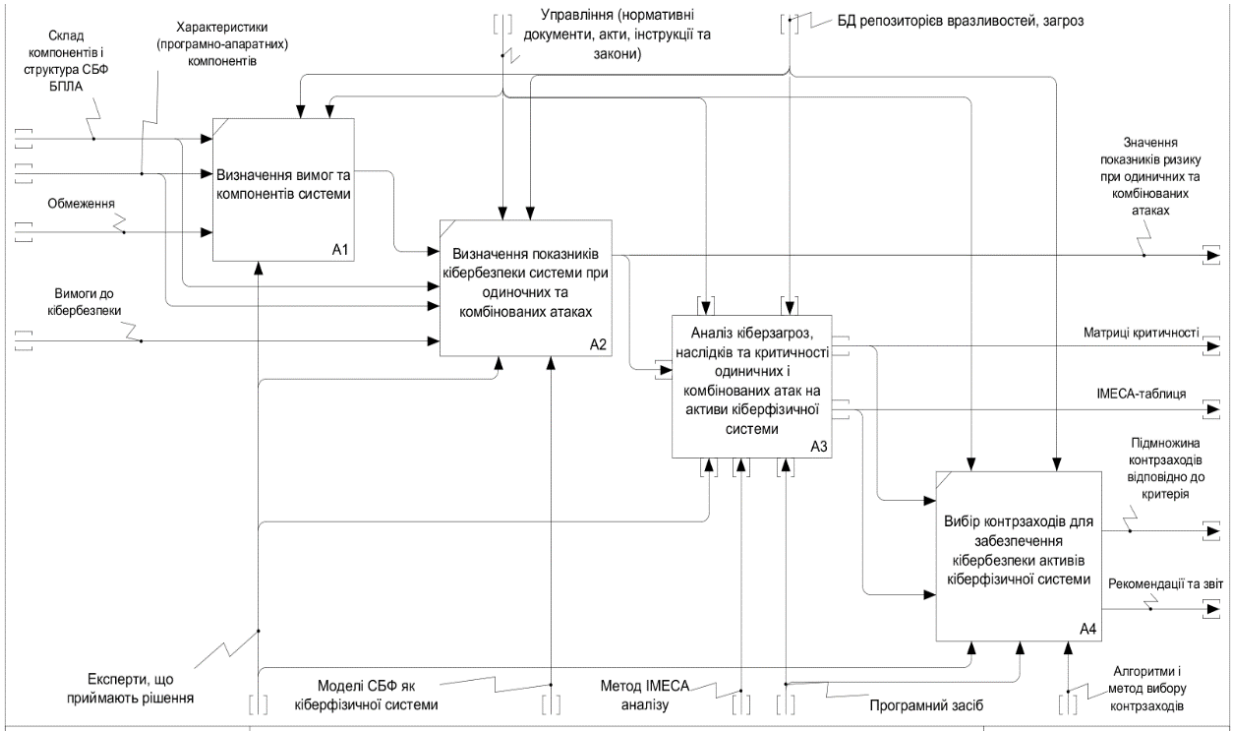


Рисунок 4.14 – IDEF1-діаграма

Метод імека аналізу є комплексним і структурованим підходом, який складається з кількох послідовних етапів для ефективного аналізу та управління кібербезпекою систем, рисунок 4.15. Початковий етап включає аналіз інфраструктури системи безпілотних літальних апаратів (СБФ БПЛА) та формування відповідної множини, що враховує всі аспекти її функціонування та взаємодії. Далі проводиться аналіз загроз, потенційних порушників та вразливостей системи, що дозволяє зрозуміти можливі сценарії атак та їх можливі наслідки. На основі цього аналізу формується відповідна множина контрзаходів, спрямованих на запобігання потенційним загрозам. Далі відбувається формування та заповнення таблиці, що відображає взаємозв'язки між загрозами, атаками та вразливостями системи. Це допомагає усвідомити потенційні ризики та визначити пріоритетні напрямки захисту. На основі цих даних будується початкова матриця критичності, враховуючи різні шкали оцінювання ймовірності та тяжкості атак. В результаті аналізу отримуємо два основних результати: визначення критичних елементів інфраструктури та розроблення оптимальних стратегій захисту системи.

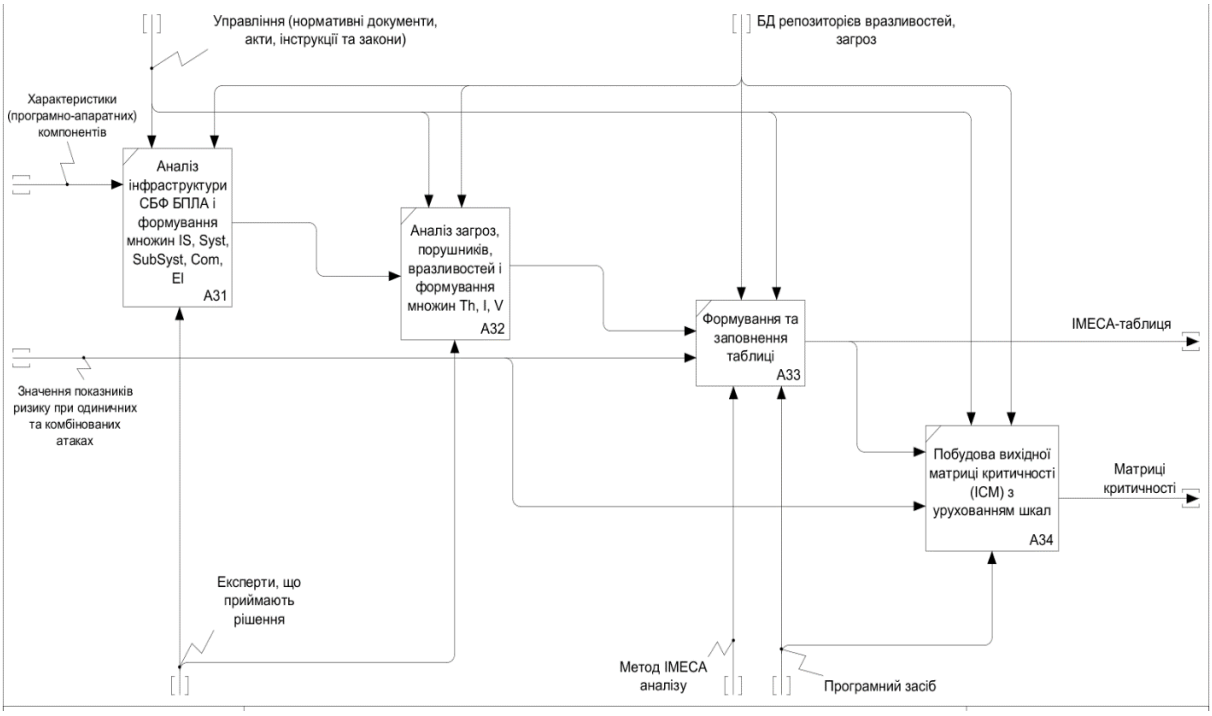


Рисунок 4.15 – IDEF1-діаграма

4.5 Огляд і аналіз результатів впровадження розробленних моделей та методів

Результати наукових досліджень апробовані та впроваджені в наступних організаціях, (див. Додаток Є):

на підприємствах в Україні:

– впроваджені в ТОВ «СІДІ ЛІНК»;

у вищому навчальному закладі України Національному аерокосмічному університету ім. М. Є. Жуковського «Харківський авіаційний інститут»:

– у навчальному процесі кафедри комп'ютерних систем, мереж і кібербезпеки (лекціях та практичних заняттях з навчальних дисциплін «Надійність та функціональна безпека інформаційно-управляючих систем», «Програмування систем IoT», «Захист інформації в інформаційно-комунікаційних системах», «Комплексні системи захисту інформації: проектування, впровадження, супровід») для бакалаврів, магістрів і аспірантів, що навчаються за спеціальністю 125 – Кібербезпека і захист інформації;

– при виконанні міжнародного проекту Internet of Things: Emerging Curriculum for Industry and Human Applications (ALIOT, №573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP) впродовж 2016-2019 рр., за програмою ЄС ERASMUS + [1];

– при виконанні держбюджетної науково-дослідницької роботи «Наукові засади і методи забезпечення гарантоздатності флотів БПЛА інтелектуальних систем моніторингу потенційно небезпечних і військових об’єктів» ДР № 0121U112172 впродовж 2021-2023 рр. [9];

– при виконанні держбюджетної науково-дослідницької роботи «Методи, моделі та інформаційні технології підвищення надійності та безпечності складних ІТ-систем на етапах розроблення та впровадження» ДР № 0121U113842 впродовж 2021-2023 рр. [10];

– при виконанні держбюджетної науково-дослідницької роботи «Методи, програмно-апаратні засоби та інформаційні технології розроблення і модернізації гарантоздатних комп'ютерних систем, мереж та ІТ-інфраструктур» ДР № 0117U05349 впродовж 2018-2020 рр. [11];

– при виконанні держбюджетної науково-дослідницької роботи «Методологія сталого розвитку та інформаційні технології зеленого комп'ютингу та комунікацій» ДР № 0118U003822 впродовж 2018-2020 рр. [12].

Таблиця 4.3 містить систематизацію результатів впровадження наукових досліджень дисертаційної роботи.

Таблиця 4.3 – Систематизація результатів впровадження наукових результатів дисертаційної роботи

Місце впровадження	Наукові результати	Система, процес	Ефект від впровадження
1	2	3	4
ТОВ «СІДІ ЛІНК»	1,2	При оцінюванні безпеки під час розроблення методу вибору контрзаходів за критеріями	Зменшення ризиків порушення кібербезпеки при розробленні та впровадженні методу вибору контрзаходів за трьома критеріями

Продовження таблиці 4.3

1	2	3	4
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»	1,2,3	Навчальний процес (лекції та практичні заняття)	Впровадження та використання інноваційних теорій і методів, пов'язаних з безпекою в навчальних та освітніх ресурсів, покращення наочності, фундаментальності та практичної спрямованості навчального процесу, підвищення якості виконання наукових проектів, покращення підготовки фахівців
		При виконанні держбюджетних НДР	Підвищення якості виконання НДР щодо розроблення та впровадження сучасних методів та засобів забезпечення кібербезпеки СБФ БПЛА
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»	2,3	При виконанні міжнародних проектів за програмами Tempus, Erasmus+	Впровадження у навчальний процес нових науково-технічних досягнень, покращення наочності, фундаментальності та практичної спрямованості навчального процесу, підвищення якості виконання наукових проектів, покращення міжнародних зв’язків університету у галузі підготовки фахівців і наукового співробітництва

4.6 Висновки до розділу

Після виконання розділу, присвяченого розробленню та впровадженню методу та засобів забезпечення кібербезпеки СБФ БПЛА, можна зробити наступні висновки.

1. Удосконалено метод вибору контрзаходів для забезпечення кібербезпеки кіберфізичної системи багатофункційних флотів безпілотних літальних апаратів завдяки формуванню множини контрзаходів з врахуванням впливу на різні складові кібербезпеки, в умовах одиничних та комбінованих кібератак, з використанням процедур спрямованого пошуку варіантів покриття, що забезпечує

прийнятний ризик при мінімальних витратах або мінімальний ризик при обмежених витратах.

2. Основними метою вибору контрзаходів є мінімізація ризиків та максимізація ефективності за мінімальних витрат. Для досягнення цих цілей використовуються ретельно розроблені алгоритми, що дозволяють здійснювати систематичний та обґрунтований підбір контрзаходів.

3. Результатом впровадження методу вибору контрзаходів є підвищення рівня кібербезпеки СБФ БПЛА та зменшення ймовірності виникнення кібератак. Оцінка отриманих результатів показує, що розроблені моделі та методи є ефективними і сприяють покращенню загальної безпеки системи.

Література до розділу

1. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі::Державний університет інформаційно-комунікаційних технологій. *Головна::Державний університет інформаційно-комунікаційних технологій*. URL: https://duikt.edu.ua/ua/lib/1/category/919/view/1057 (дата звернення: 08.03.2024).

2. Типове положення про службу захисту інформації в автоматизованій системі::Державний університет інформаційно-комунікаційних технологій. *Головна::Державний університет інформаційно-комунікаційних технологій*. URL: https://duikt.edu.ua/ua/lib/1/category/2342/view/1023 (дата звернення: 08.03.2024).

3. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі :: Державний університет інформаційно-комунікаційних технологій. *Головна :: Державний університет інформаційно-комунікаційних технологій*. URL: https://duikt.edu.ua/ua/lib/1/category/919/view/1037?lang=ua&act=view&page=1&category=919&id=1037 (дата звернення: 08.04.2024).

4. Anatoly, P., Zemlianko, H., Kharchenko, V. (2020). Prototyping and Rapid Development of IoT Systems in Context of Edge Computing. In: Nechyporuk, M., Pavlikov, V., Kritskiy, D. (eds) Integrated Computer Technologies in Mechanical Engineering. *Advances in Intelligent Systems and Computing*, vol 1113. Springer, Cham. https://doi.org/10.1007/978-3-030-37618-5_23.

5. Pevnev, V., Frolov, A., Tsuranov, M., & Zemlianko, H. (2022). Ensuring the Data Integrity in Infocommunication Systems. *International Journal of Computing*, *21*(2), 228-233. https://doi.org/10.47839/ijc.21.2.2591.

6. Zemlianko H., Kharchenko V. Cybersecurity risk analysis of multifunctional UAV fleet systems: a conceptual model and IMECA-based technique. *Radioelectronic and Computer Systems*. 2023. № 4. С. 152–170. URL: https://doi.org/10.32620/reks. 2023.4.11.

7. Zemlianko H., Kharchenko V. Cyber Security Systems of Highly Functional Uav Fleets for Monitoring Critical Infrastructure: Analysis of Disruptions, Attacks and Counterapproaches. *Èlektronnoe modelirovanie*. 2024. Т. 46, № 1. С. 41–54. URL: https://doi.org/10.15407/emodel.46.01.041.

8. Землянко Г.А., Харченко В.С. IMECA-аналіз кібербезпеки систем багатофункціональних флотів БПЛА при комбінованих атаках: базові моделі та вибір контрзаходів. *Measuring and computing devices in technological processes*. 2023. № 4. С. 225–233. URL: https://doi.org/10.31891/2219-9365-2023-76-30.

9. Оцінка кібербезпеки Інтернету систем дронів з урахуванням радіочастотної вразливості на основі. // Теоретичне обгрунтування методології, структури, моделі, методи оцінювання надійності і живучості інтелектуальних систем моніторингу потенційно небезпечних і військових об'єктів з використанням багатоцільових флотів БПЛА : звіт про НДР (проміж.) : Д503-1/2021-Ф / М-во освіти і науки України, Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харків. авіац. ін-т" ; керівник Харченко В. С. ; викон.: Морозова О. І. [та інш.]. - Харків, 2021. - 230 с. - № ДР 0121U112172.

10. Методи контролю та оцінювання інформаційної безпеки комп’ютерних мереж з використанням пентестингу. // Розроблення засобів тестування та

верифікації вбудованих і розподілених гарантоздатних ІТ-систем та інфраструктур : звіт про НДР (проміж.) / М-во освіти і науки України, Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харків. авіац. ін-т" ; керівник Харченко В. С. ; викон.: Фесенко Г. В. [та інш.]. - Харків, 2021. - 197 с. - № ДР 0121U113842.

11. Розроблення програмно-апаратних засобів для систем розумного міста. // Розробка моделей та засобів кібербезпеки інформаційних і комунікаційних систем. Впровадження запропонованих принципів, моделей та методів оцінювання та розробки гарантоздатних комп'ютерних систем, мереж та ІТ-інфраструктур : звіт про НДР (заключ.) / М-во освіти і науки України, Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харків. авіац. ін-т" ; керівник Харченко В. С. ; викон.: Лисенко І. В. [та інш.]. - Харків, 2020. - 245 с. - № ДР 0117U05349 - Інв. № 0221U000032.

12. Методи і засоби побудови енергоефективних засобів побудови смарт-систем з використанням IoT і Edge комп’ютингу. // Розроблення методів формування вимог, аналізу, оцінювання та зменшення витрат ресурсів протягом життєвого циклу програмного забезпечення, мобільних пристроїв, хмарних обчислень : звіт про НДР (заключ.) : Д503-1/2018-Ф . Т. 1 / М-во освіти і науки України, Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харків. авіац. ін-т" ; керівник Харченко В. С. ; викон.: Колісник М. О. [та інш.]. - Харків, 2020. - 232 с. - № ДР 0118U003822 - Інв. № 0221U000030.

ВИСНОВКИ

У дисертації проведено теоретичне обґрунтування й нове вирішення актуальної наукової задачі розроблення методів і моделей забезпечення кібербезпеки СБФ БПЛА при одиночних та комбінованих атаках. При цьому було отримано наступні наукові та практичні результати.

1) Вперше запропоновано моделі кіберфізичної системи багатофункційних флотів безпілотних апаратів як об’єкта оцінювання кібербезпеки, які, на відміну від відомих, описують концептуальну схему, що об’єднує комплекс мобільних підсистем, а саме безпілотних літальних, наземних і безекіпажних апаратів та інформаційну інфраструктуру, надають теоретико-множинне представлення програмно-апаратних компонентів на різних рівнях ієрархії, порушників, загроз, вразливостей і атак та їх онтологічних зв’язків, і забезпечують повноту аналізу такої системи в умовах зовнішніх впливів, а також надають можливості формування множини контрзаходів для захисту фізичних і кіберактивів.

2) Удосконалено метод (IMECA) аналізу кіберзагроз, наслідків та критичності атак на активи кіберфізичної системи багатофункційних флотів безпілотних літальних апаратів шляхом деталізованого опису впливу на різні властивості безпеки (конфіденційність, цілісність, доступність, спостережність) і різні підсистеми, а також розроблення моделей і послідовностей комбінованих послідовно-паралельних кібератак різними порушниками і засобами, що надає змогу підвищити достовірність оцінювання кібербезпеки та обґрунтувати стратегії захисту та вибір контрзаходів для забезпечення прийнятного ризику.

3) Удосконалено метод вибору контрзаходів для забезпечення кібербезпеки кіберфізичної системи багатофункційних флотів безпілотних літальних апаратів завдяки формуванню множини контрзаходів з врахуванням впливу на різні складові кібербезпеки, в умовах одиничних та комбінованих кібератак, з використанням процедур спрямованого пошуку варіантів покриття, що забезпечує прийнятний ризик при мінімальних витратах або мінімальний ризик при обмежених витратах.

Достовірність отриманих наукових і практичних результатів, підтверджуються результатами оцінювання ризиків успішних атак з використанням якісних і кількісних показників на підставі аналізу матриць критичності без і після запровадження відповідних контрзаходів, прикладами оцінювання показників кібербезпеки та вибору контрзаходів з використанням розроблених методів і алгоритмів при одиничних і комбінованих атаках і результатами практичного основних наукових положень, запропонованих програмних засобів та елементів інформаційної технології в навчальному процесі, наукових проєктах.

Отримані наукові результати, можуть бути використані у науково-дослідних та проектних організаціях, ІТ-компаніях, університетах – при викладанні відповідних дисциплін, та інших організаціях, які спеціалізуються в галузі безпечних інформаційних технологій, зокрема, для побудови та забезпечення кібербезпеки та резильєнтності національної критичної ІТ-інфраструктури та захисту інформаційних активів стратегічних галузей промисловості.

Основні результати дисертації опубліковано 13 наукових публікацій, у тому числі:

– 2 статті опубліковано у наукових фахових виданнях, включених до переліку спеціалізованих видань України;

– 3 статті опубліковані у наукових фахових виданнях, індексовані в базі даних Scopus;

– 2 колективні монографії;

– 6 публікацій у матеріалах національних та міжнародних конференцій, у т.ч. у працях конференції, індексованої у базі даних Scopus.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A Distributed Collaborative Allocation Method of Reconnaissance and Strike Tasks for Heterogeneous UAVs / H. Deng та ін. Drones. 2023. Т. 7, № 2. С. 138. URL: https://doi.org/10.3390/drones7020138 (дата звернення: 16.09.2023).

2. A Flow Feedback Traffic Prediction Based on Visual Quantified Features / J. Chen та ін. IEEE Transactions on Intelligent Transportation Systems. 2023. С. 1-9. URL: https://doi.org/10.1109/tits.2023.3269794 (дата звернення: 04.09.2023).

3. A Guidance System for Tactical Autonomous Unmanned Aerial Vehicles / J. A. Marshall та ін. Journal of Intelligent & Robotic Systems. 2021. Т. 103, № 4. URL: https://doi.org/10.1007/s10846-021-01526-8 (дата звернення: 25.12.2023).

4. A Review on Security Issues and Solutions of the Internet of Drones / W. Yang та ін. IEEE Open Journal of the Computer Society. 2022. С. 1-15. URL: https://doi.org/10.1109/ojcs.2022.3183003 (дата звернення: 04.06.2023).

5. A Survey of Indoor and Outdoor UAV-based Target Tracking Systems: Current Status, Challenges, Technologies, and Future Directions / M. Alhafnawi та ін. IEEE Access. 2023. С. 1. URL: https://doi.org/10.1109/access.2023.3292302 (дата звернення: 08.08.2023).

6. A Survey on Swarming with Micro Air Vehicles: Fundamental Challenges and Constraints / M. Coppola та ін. Frontiers in Robotics and AI. 2020. Т. 7. URL: https://doi.org/10.3389/frobt.2020.00018 (дата звернення: 04.06.2023).

7. Abdulhae O. T., Mandeep J. S., Islam M. Cluster-Based Routing Protocols for Flying Ad Hoc Networks (FANETs). IEEE Access. 2022. Т. 10. С. 32981-33004. URL: https://doi.org/10.1109/access.2022.3161446 (дата звернення: 06.09.2022).

8. Advanced Sensor Systems for Robotics and Autonomous Vehicles / M. Tolani та ін. Artificial Intelligence for Robotics and Autonomous Systems Applications. Cham, 2023. С. 439-459. URL: https://doi.org/10.1007/978-3-031-28715-2_14 (дата звернення: 16.09.2023).

9. Agarwala, N. Integrating UUVs for naval applications. Marit. Technol. Res. 2022, 4, 254470.

10. Ahmad H., Farhan M., Farooq U. Computer Vision Techniques for Military Surveillance Drones. Wasit Journal of Computer and Mathematics Science. 2023. Т. 2, № 2. С. 56-63. URL: https://doi.org/10.31185/wjcms.148 (дата звернення: 16.09.2023).

11. Al-Bkree M. Managing the cyber-physical security for unmanned aerial vehicles used in perimeter surveillance. International Journal of Innovative Research and Scientific Studies. 2023. Т. 6, № 1. С. 164-173. URL: https://doi.org/10.53894/ijirss.v6i1.1173 (дата звернення: 04.06.2023).

12. AL-Dosari K., Hunaiti Z., Balachandran W. Systematic Review on Civilian Drones in Safety and Security Applications. Drones. 2023. Т. 7, № 3. С. 210. URL: https://doi.org/10.3390/drones7030210 (дата звернення: 04.06.2023).

13. Ammari H. M. Spatial Unconditional and Conditional Network Connectivity and Fault-Tolerance Measures for k-Covered Wireless Sensor Networks. Theory and Practice of Wireless Sensor Networks: Cover, Sense, and Inform. Cham, 2022. С. 375-396. URL: https://doi.org/10.1007/978-3-031-07823-1_12 (дата звернення: 16.09.2023).

14. An optimal wsn coverage based on adapted transit search algorithm / T.-K. Dao та ін. International Journal of Software Engineering and Knowledge Engineering. 2023. URL: https://doi.org/10.1142/s0218194023400016 (дата звернення: 16.09.2023).

15. Anatoly, P., Zemlianko, H., Kharchenko, V. (2020). Prototyping and Rapid Development of IoT Systems in Context of Edge Computing. In: Nechyporuk, M., Pavlikov, V., Kritskiy, D. (eds) Integrated Computer Technologies in Mechanical Engineering. Advances in Intelligent Systems and Computing, vol 1113. Springer, Cham. https://doi.org/10.1007/978-3-030-37618-5_23.

16. Anitha A. A., Arockiam L. A Review on Intrusion Detection Systems to Secure IoT Networks. International Journal of Computer Networks and Applications. 2022. Т. 9, № 1. С. 38. URL: https://doi.org/10.22247/ijcna/2022/211599 (дата звернення: 16.09.2023).

17. Austin R. Unmanned aircraft systems: UAVs design, development and deployment. Reston, Va: American Institute of Aeronautics and Astronautics, 2010. 332 p.

18. Autonomous Control Systems and Vehicles: Intelligent Unmanned Systems / K. Nonami et al. Springer, 2016. 324 p.

19. Autonomous Vessels in Maritime Affairs: Law and Governance Implications / A. Pastra et al. Springer International Publishing AG, 2023.

20. Bai, Z.; Feng, Q.; Qiu, Y. Design and research of UAV for campus express delivery. In Proceedings of the 2021 2nd International Conference on Intelligent Design (ICID), Xi'an, China, 19 October 2021; pp. 208-213.

21. Bella, S.; Belbachir, A.; Belalem, G. A Centralized Architecture for Cooperative Air-Sea Vehicles Using UAV-USV. Int. J. Comput. Inf. Eng. 2019, 13, 201-210.

22. Beni, G. From swarm intelligence to swarm robotics. In Swarm Robotics, Proceedings of the SAB 2004 International Workshop, Santa Monica, CA, USA, 17 July 2004; ?ahin, E., Spears, W.M., Eds.; LNCS; Springer: Berlin/Heidelberg, Germany, 2004; Volume 3342, pp. 1-9.

23. Bezpilotniy Letayuschiy Apparat - BPLA. GlobalSecurity.org. URL: https://www.globalsecurity.org/military/world/russia/aircraft-uav.htm (дата звернення: 04.09.2023).

24. Bini, D.; Pamela, D.; Prince, S. Machine vision and machine learning for intelligent agrobots: A review. In Proceedings of the 2020 5th International Conference on Devices, Circuits and Systems (ICDCS), Coimbatore, India, 5-6 March 2020; pp. 12-16.

25. Boyle M. J. Drone Age: How Drone Technology Will Change War and Peace. Oxford University Press, Incorporated, 2020. 336 p.

26. Brantner, G.; Khatib, O. Controlling Ocean One: Human-robot collaboration for deep-sea manipulation. J. Field Robot. 2021, 38, 28-51.

27. Brust, M.R.; Danoy, G.; Bouvry, P.; Gashi, D.; Pathak, H.; Gon?alves, M.P. Defending against intrusion of malicious uavs with networked uav defense swarms. In Proceedings of the 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops), Singapore, 9 October 2017; pp. 103-111.

28. C. Jeon, J. Ha, H. Ko, B. Lee, B. Ryu. Swarmsense: Effective and Resilient Drone Swarm and Search for Disaster Response and Management Application. URL: https://www.wirelessinnovation.org/assets/Proceedings/2019/TS6.2%20Jeon%20presentation.pdf (дата звернення: 04.06.2023).

29. Computational Intelligent Security in Wireless Communications / S. A. Khan та ін. Boca Raton: CRC Press, 2022. URL: https://doi.org/10.1201/9781003323426 (дата звернення: 04.06.2023).

30. Das A., Chowdhury A., Sil R. Third Industrial Revolution: 5G Wireless Systems, Internet of Things, and Beyond. 5G and Beyond. Singapore, 2023. С. 19-43. URL: https://doi.org/10.1007/978-981-99-3668-7_2 (дата звернення: 16.09.2023).

31. De Freitas, E. P., Heimfarth, T., Netto, I. F., Lino, C. E., Pereira, C. E., Ferreira, A. M., Wagner, F. R., & Larsson, T. (2010). UAV relay network to support WSN connectivity. In Proceedings of the International Congress on Ultra Modern Telecommunications and Control Systems 2010, 309-314. IEEE.

32. De Freitas, E. P., Heimfarth, T., Netto, I. F., Lino, C. E., Pereira, C. E., Ferreira, A. M., Wagner, F. R., & Larsson, T. (2010). UAV relay network to support WSN connectivity. In Proceedings of the International Congress on Ultra Modern Telecommunications and Control Systems 2010, 309-314. IEEE.

33. Designers and Manufacturers of Drone Software and Hardware for Enterprise - Sky-Drones Technologies Ltd. Designers and Manufacturers of Drone Software and Hardware for Enterprise - Sky-Drones Technologies Ltd. URL: http://sky-drones.com (дата звернення: 04.09.2023).

34. Development of UAV Tracing and Coordinate Detection Method Using a Dual-Axis Rotary Platform for an Anti-UAV System / B.-H. Sheu та ін. Applied Sciences. 2019. Т. 9, № 13. С. 2583. URL: https://doi.org/10.3390/app9132583 (дата звернення: 04.09.2023).

35. Dey B., Bandyopadhyay S., Nandi S. Mobility Assisted Adaptive Clustering Hierarchy for IoT Based Sensor Networks in 5G and Beyond. Journal of Communications. 2023. С. 346-356. URL: https://doi.org/10.12720/jcm.18.6.346-356 (дата звернення: 16.09.2023).

36. Dias, P.G.F.; Silva, M.C.; Rocha Filho, G.P.; Vargas, P.A.; Cota, L.P.; Pessin, G. Swarm Robotics: A Perspective on the Latest Reviewed Concepts and Applications. Sensors 2021, 21, 2062.

37. Drew J. DARPA selects industry teams for 'Gremlins' UAV project. Flight Global. URL: https://www.flightglobal.com/civil-uavs/darpa-selects-industry-teams-for-gremlins-uav-project/120171.article (дата звернення: 04.09.2023).

38. Dynamic Online Trajectory Planning for a UAV-Enabled Data Collection System / S. Li та ін. IEEE Transactions on Vehicular Technology. 2022. С. 1-12. URL: https://doi.org/10.1109/tvt.2022.3200458 (дата звернення: 16.09.2023).

39. European Union drone regulations explained - AgEagle Aerial Systems Inc. AgEagle Aerial Systems Inc. URL: https://ageagle.com/blog/european-union-drone-regulations-explained/ (дата звернення: 04.09.2023).

40. Ewelina K. Unmanned Aerial Vehicles in the Security Service and as a New Tool in the Hands of Criminals. Safety & Defense. 2018. Т. 4. С. 31-36. URL: https://doi.org/10.37105/sd.6 (дата звернення: 04.09.2023).

41. Falorca J. F., Miraldes J. P. N. D., Lanzinha J. C. G. New trends in visual inspection of buildings and structures: Study for the use of drones. Open Engineering. 2021. Т. 11, № 1. С. 734-743. URL: https://doi.org/10.1515/eng-2021-0071 (дата звернення: 04.06.2023).

42. Flying Sensor Network Optimization Using Bee Intelligence for Internet of Things / A. Salam та ін. Advances in Intelligent Systems and Computing. Cham, 2020. С. 331-339. URL: https://doi.org/10.1007/978-3-030-55190-2_25 (дата звернення: 16.09.2023).

43. Global Drone Regulations Database. Global Drone Regulations Database. URL: https://www.droneregulations.info/index.html (дата звернення: 16.09.2023).

44. Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace. Vienna, Austria: Ueberreuter Print GmbH, 2013. 100 с. URL: https://www.osce.org/files/f/documents/4/b/103500.pdf (дата звернення: 22.10.2023).

45. Group Target Tracking for Highly Maneuverable Unmanned Aerial Vehicles Swarms: A Perspective / Y. Chen та ін. Sensors. 2023. Т. 23, № 9. С. 4465. URL: https://doi.org/10.3390/s23094465 (дата звернення: 16.09.2023).

46. Gupta A., Gupta S. K. A survey on green unmanned aerial vehicles?based fog computing: Challenges and future perspective. Transactions on Emerging Telecommunications Technologies. 2022. URL: https://doi.org/10.1002/ett.4603 (дата звернення: 04.06.2023).

47. Gupta, L., Jain, R., & Vaszkun, G. (2016). Survey of Important Issues in UAV Communication Networks. IEEE Communications Surveys & Tutorials, 18(2), 1123-1152.

48. Hammoud B., Wehn N. Recent Advances in Oil-Spill Monitoring Using Drone-Based Radar Remote Sensing. Environmental Sciences. 2022. URL: https://doi.org/10.5772/intechopen.106942 (дата звернення: 16.09.2023).

49. Harik, E.H.C.; Gu?rin, F.; Guinand, F.; Breth?, J.F.; Pelvillain, H. UAV-UGV cooperation for objects transportation in an industrial area. In Proceedings of the 2015 IEEE International Conference on Industrial Technology (ICIT), Seville, Spain, 17-19 March 2015; pp. 547-552.

50. Hu F. Uav Swarm Networks: Models Protocols and Systems. Taylor & Francis Group, 2020.

51. Hu, C.; Fu, L.; Yang, Y. Cooperative navigation and control for surface-underwater autonomous marine vehicles. In Proceedings of the IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chengdu, China, 15-17 December 2017; pp. 589-592.

52. IEC 61000-2-10:2021. Electromagnetic compatibility (EMC) - Part 2-10: Environment - Description of HEMP environment - Conducted disturbance. На заміну IEC 61000-2-10:1998; чинний від 2021-11-18. Вид. офіц. International Electrotechnical Commission, 2021. 47 с.

53. Impact of Routing Techniques and Mobility Models on Flying Ad Hoc Networks / M. A. Hassan та ін. Studies in Computational Intelligence. Cham, 2022. С.

111-129. URL: https://doi.org/10.1007/978-3-030-97113-7_7 (дата звернення: 16.09.2023).

54. Implementation of the Communication Network for the Multi-Agent Robotic Systems / R. Kirichek та ін. International Journal of Embedded and Real-Time Communication Systems. 2016. Т. 7, № 1. С. 48-63. URL: https://doi.org/10.4018/ijertcs.2016010103 (дата звернення: 16.09.2023).

55. International Civil Aviation Organization (ICAO) Standards. URL: https://www.icao.int/ (дата звернення: 04.02.2022).

56. Internet of Drones: AI Applications for Smart Solutions / A. Solanki et al. Apple Academic Press, Incorporated, 2022.

57. ISO/IEC 27001:2022. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection. На заміну EN ISO/IEC 27001:2017; ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015; чинний від 2022-12-28. Вид. офіц. 3, 2022. 19 с.

58. ISO/IEC/IEEE 15288:2023 Systems and software engineering – System life cycle processes. ISO. URL: https://www.iso.org/ru/standard/81702.html (дата звернення: 22.06.2023).

59. ISO/IEC/IEEE 21450:2010 Information technology – Smart transducer interface for sensors and actuators – Common functions, communication protocols, and Transducer Electronic Data Sheet (TEDS) formats. ISO. URL: https://www.iso.org/ru/standard/54356.html (дата звернення: 06.08.2022).

60. ISO/IEC/IEEE 21839:2019 Systems and software engineering – System of systems (SoS) considerations in life cycle stages of a system. ISO. URL: https://www.iso.org/ru/standard/71955.html. (дата звернення: 05.03.2022).

61. ISO/IEC/IEEE 21840:2019 Systems and software engineering – Guidelines for the utilization of ISO/IEC/IEEE 15288 in the context of system of systems (SoS). ISO. URL: https://www.iso.org/ru/standard/71956.html. (дата звернення: 05.03.2022).

62. ITU-R M.1796-2 Characteristics of and protection criteria for terrestrial radars operating in the radiodetermination service in the frequency band 8 500-10 680 MHz. ITU-R Recommendations. URL: https://extranet.itu.int/brdocsearch/_layouts/15/WopiF

rame.aspx?sourcedoc=%7BA8A0C3D3-2095-4E3A-9AA1-668D4425E469%7D&file=R-REC-M.1796-2-201402-I!!MSW-E.docx&action=default&DefaultItemOpen=1 (дата звернення: 08.08.2023).

63. Ivannikova V. Y., Ayrapetyan A. G. UNMANNED AERIAL VEHICLES (UAVS) OPERATION IN UKRAINE: A REGULATIONS REVIEW. Scientific notes of Taurida National V.I. Vernadsky University. Series: Technical Sciences. 2021. № 6. С. 209-215. URL: https://doi.org/10.32838/2663-5941/2021.6/34 (дата звернення: 16.09.2023).

64. J. Geismann, C. Gerking, and E. Bodden, “Towards ensuring security by design in cyber-physical systems engineering processes // in Proceedings of the 2018 international conference on software and system process, 2018, pp. 123–127. URL: https://www.researchgate.net/publication/325373997_Towards_ensuring_security_by_design_in_cyber-physical_systems_engineering_processes (дата звернення: 08.05.2022).

65. Jobard R. Les drones: La nouvelle r?volution. Paris: Eyrolles, 2014. 175 c.

66. Jongsik Ahn, Min Young Kim, "ICAIIC - Positional estimation of invisible drone using acoustic array with A-shaped neural network", 2021 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), pg. 320, (2021); URL:10.1109/icaiic51459.2021.9415272 (дата звернення: 04.09.2023).

67. Khaldi, B.; Cherif, F. An overview of swarm robotics: Swarm intelligence applied to multi-robotics. Int. J. Comput. Appl. 2015, 126, 2.

68. Kr?likowski H. The Use of Unmanned Aerial Vehicles in Contemporary Armed Conflicts - Selected Issues. Politeja. 2022. T. 19, № 4 (79). URL: https://doi.org/10.12797/politeja.19.2022.79.02 (дата звернення: 04.07.2023).

69. Krishnan S., Murugappan M. Internet of Drones. Boca Raton : CRC Press, 2023. URL: https://doi.org/10.1201/9781003252085 (date of access: 08.04.2024).

70. Krizmancic, M.; Arbanas, B.; Petrovic, T.; Petric, F.; Bogdan, S. Cooperative aerial-ground multi-robot system for automated construction tasks. IEEE Robot. Autom. Lett. 2020, 5, 798-805.

71. L. M. Gladence, V. M. Anu, A. Anderson, I. Stanley, J. A. Fernando J and S. Revathy, "Swarm Intelligence in Disaster Recovery," 2021 5th International Conference

on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2021, pp. 1-8, URL: 10.1109/ICICCS51141.2021.9432146 (дата звернення: 04.06.2023).

72. Lateef S., Rizwan M., Hassan M. A. Security Threats in Flying Ad Hoc Network (FANET). Studies in Computational Intelligence. Cham, 2022. C. 73-96. URL: https://doi.org/10.1007/978-3-030-97113-7_5 (дата звернення: 16.09.2023).

73. Li, N.; Remeikas, C.; Xu, Y.; Jayasuriya, S.; Ehsani, R. Task Assignment and Trajectory Planning Algorithm for a Class of Cooperative Agricultural Robots. J. Dyn. Syst. Meas. Control 2015, 137, 1-9.

74. MahmoudZadeh S., Powers D. M. W., Bairam Zadeh R. Autonomy and Unmanned Vehicles. Singapore : Springer Singapore, 2019. URL: https://doi.org/10.1007/978-981-13-2245-7 (date of access: 12.03.2024).

75. Markus E. D., Fadeyi J. Smart Cities and Spectrum Vulnerabilities in Long-Range Unlicensed Communication Bands: A Review. Applied Soft Computing and Communication Networks. Singapore, 2021. C. 207-220. URL: https://doi.org/10.1007/978-981-33-6173-7_14 (дата звернення: 16.09.2023).

76. Markus E. D., Fadeyi J. Smart Cities and Spectrum Vulnerabilities in Long-Range Unlicensed Communication Bands: A Review. Applied Soft Computing and Communication Networks. Singapore, 2021. C. 207-220. URL: https://doi.org/10.1007/978-981-33-6173-7_14 (дата звернення: 16.09.2023).

77. Mathematical Approaches Transform Cybersecurity from Protoscience to Science / I. Trenchev та ін. Applied Sciences. 2023. Т. 13, № 11. С. 6508. URL: https://doi.org/10.3390/app13116508 (дата звернення: 08.11.2023).

78. McEnroe P., Wang S., Liyanage M. A Survey on the Convergence of Edge Computing and AI for UAVs: Opportunities and Challenges. IEEE Internet of Things Journal. 2022. С. 1. URL: https://doi.org/10.1109/jiot.2022.3176400 (дата звернення: 04.06.2023).

79. McNeal, G.S. Drones and the future of aerial surveillance. George Wash. Law Rev. 2016, 84, 354.

80. Michaelides-Mateou S. Challenges and Trends in the Aviation Industry: Integrating UAVs in Non-segregated Airspace. Unmanned Aerial Vehicles Applications:

Challenges and Trends. Cham, 2023. C. 377-409. URL: https://doi.org/10.1007/978-3-031-32037-8_13 (дата звернення: 16.09.2023).

81. Militants and Drones: A Trend That is Here to Stay. Homepage | Royal United Services Institute. URL: https://www.rusi.org/explore-our-research/publications/commentary/militants-and-drones-trend-here-stay (дата звернення: 04.09.2023).

82. Nedjah, N.; Junior, L.S. Review of methodologies and tasks in swarm robotics towards standardization. Swarm Evol. Comput. 2019, 50, 100565.

83. New Advancements in Cybersecurity: A Comprehensive Survey / M. A. Hassan та ін. Studies in Big Data. Cham, 2022. C. 3-17. URL: https://doi.org/10.1007/978-3-031-05752-6_1 (дата звернення: 08.11.2023).

84. Omolara A. E., Alawida M., Abiodun O. I. Drone cybersecurity issues, solutions, trend insights and future perspectives: a survey. Neural Computing and Applications. 2023. URL: https://doi.org/10.1007/s00521-023-08857-7 (дата звернення: 16.09.2023).

85. Open-ended working group on developments in the field of information and telecommunications in the context of international security. General Assembly, 2011. 11 с. URL: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (дата звернення: 22.10.2023).

86. Optimization of Air Defense System Deployment Against Reconnaissance Drone Swarms / N. Li та ін. Complex System Modeling and Simulation. 2023. Т. 3, № 2. С. 102-117. URL: https://doi.org/10.23919/csms.202 3.0003 (дата звернення: 04.09.2023).

87. Orfanus, D., Eliassen, F., & de Freitas, E. P. (2014). Self-Organizing Relay Network Supporting Remotely Deployed Sensor Nodes in Military Operations. In 6th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 326-333. IEEE.

88. Panchal H., Gajjar S. Fuzzy Logic-Based Cluster Head Selection an Underwater Wireless Sensor Network: A Survey. Communication and Intelligent Systems. Singapore, 2022. C. 661-673. URL: https://doi.org/10.1007/978-981-19-2130-8_51 (дата звернення: 16.09.2023).

89. Pehlivanoglu Y. V., Bekmezci I., Pehlivanoglu P. Efficient Strategy for Multi-UAV Path Planning in Target Coverage Problems. 2022 International Conference on Theoretical and Applied Computer Science and Engineering (ICTASCE), м. Ankara, Turkey, 29 верес. - 1 жовт. 2022 р. 2022. URL: https://doi.org/10.1109/ictacse50438.2022.10009728 (дата звернення: 16.09.2023).

90. Pevnev, V., Frolov, A., Tsuranov, M., & Zemlianko, H. (2022). Ensuring the Data Integrity in Infocommunication Systems. International Journal of Computing, 21(2), 228-233. https://doi.org/10.47839/ijc.21.2.2591.

91. Pevnev, V., Plakhteev, A., Tsuranov, M., Zemlianko, H., Leichenko, K. (2022). "Smart City" Technology: Conception, Security Issues and Cases. In: Nechyporuk, M., Pavlikov, V., Kritskiy, D. (eds) Integrated Computer Technologies in Mechanical Engineering - 2021. ICTM 2021. Lecture Notes in Networks and Systems, vol 367. Springer, Cham. URL: https://doi.org/10.1007/978-3-030-94259-5_19. (дата звернення: 04.06.2023).

92. Pevnev, V., Tsuranov, M., Zemlianko, H., Amelina, O. (2021). Conceptual Model of Information Security. In: Nechyporuk, M., Pavlikov, V., Kritskiy, D. (eds) Integrated Computer Technologies in Mechanical Engineering - 2020. ICTM 2020. Lecture Notes in Networks and Systems, vol 188. Springer, Cham. https://doi.org/10.1007/978-3-030-66717-7_14.

93. Rani P., Gupta N. K. Composite Trust for Secure Routing Strategy through Energy based Clustering in WSN. 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), м. Bhilai, India, 19-20 лют. 2021 р. 2021. URL: https://doi.org/10.1109/icaect49130.2021.9392453 (дата звернення: 16.09.2023).

94. Repository at ChSTU: Методи та інформаційна технологія автоматизованого планування маршрутів польотів безпілотних літальних апаратів для підвищення ефективності пошуку об'єктів. Repository at ChSTU: Home. URL: https://er.chdtu.edu.ua/handle/ChSTU/1144 (дата звернення: 08.04.2024).

95. Rezwan, S.; Choi, W. Artificial intelligence approaches for UAV navigation: Recent advances and future challenges. IEEE Access 2022, 10, 26320-26339.

96. Routing in Flying Ad Hoc Networks: Survey, Constraints, and Future Challenge Perspectives / O. S. Oubbati та ін. IEEE Access. 2019. Т. 7. С. 81057-81105. URL: https://doi.org/10.1109/access.2019.2923840 (дата звернення: 16.09.2023).

97. Singh R., Singh R., Kaur P. Clustering and Securing IoT Wireless Sensor Network. International Journal of Computer Science and Mobile Computing. 2022. Т. 11, № 4. С. 49-60. URL: https://doi.org/10.47760/ijcsmc.2022.v11i04.007 (дата звернення: 16.09.2023).

98. Singh V., Lohani R. B. Mobility Aware Energy Efficient Clustering for Wireless Sensor Network. 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), м. Coimbatore, India, 20-22 лют. 2019 р. 2019. URL: https://doi.org/10.1109/icecct.2019.8869231 (дата звернення: 16.09.2023).

99. STANAG 4586 Ed 4. Standard Interfaces of UAV Control System (UCS) for NATO UAV Interoperability - AEP-84 Edition A. На заміну STANAG 4586; чинний від 2020-02-08. Вид. офіц. NATO, 2017. 13 с.

100. Subbarayalu V., Vensuslaus M. A. An Intrusion Detection System for Drone Swarming Utilizing Timed Probabilistic Automata. Drones. 2023. Т. 7, № 4. С. 248. URL: https://doi.org/10.3390/drones7040248 (дата звернення: 04.06.2023).

101. SumDU Repository: Home. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/93255/1/Дисертація%20М.%20І.%20Мироненко.pdf;jsessionid=705D24C858FA2261FE8AAC2DF0B69DCB (дата звернення: 08.11.2023).

102. The Etiology of Cybersecurity / M. Ambrosi та ін. Lecture Notes in Computer Science. Cham, 2022. С. 299-319. URL: https://doi.org/10.1007/978-3-031-16815-4_17 (дата звернення: 08.11.2023).

103. Towards Security Mechanism in D2D Wireless Communication: A 5G Network Approach / D. Gupta та ін. Wireless Communications and Mobile Computing. 2022. Т. 2022. С. 1-9. URL: https://doi.org/10.1155/2022/6983655 (дата звернення: 16.09.2023).

104. 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. Т. 133. С. 102894. URL: https://doi.org/10.1016/j.adhoc.2022.102894 (дата звернення: 04.09.2023).

105. U.5. URSI Resolution on Criminal Activities using Electromagnetic Tools. URSI Home. URL: https://www.ursi.org/files/GeneralAssemblies/resolutions/1999_U05_Criminal%20Activities%20using%20Electromagnetic%20Tools.pdf (дата звернення: 04.09.2023).

106. U.S. Navy Plans to Fly First Drone Swarm This Summer. Military.com. URL: https://www.military.com/defensetech/2016/01/04/u-s-navy-plans-to-fly-first-drone-swarm-this-summer#:~:text=The%20aim%20is%20to%20have,swarm%20as%20a%20single%20unit. (дата звернення: 04.09.2023).

107. Unmanned Aircraft Systems (UAS). GlobalSecurity.org. URL: https://www.globalsecurity.org/military/world/uav.htm (дата звернення: 04.09.2023).

108. URSI resolution on Criminal activities using electromagnetic tools. - The Radio Science Bulletin. - 1999. - No. 290. - pp. 62-63.

109. Wang J., Wang W., Wu Q. Trajectory Planning of UAV in Unknown Dynamic Environment with Deep Reinforcement Learning. Lecture Notes in Electrical Engineering. Singapore, 2019. С. 470-480. URL: https://doi.org/10.1007/978-981-32-9686-2_54 (дата звернення: 16.09.2023).

110. Wang Y., Liu J. Evaluation methods for the autonomy of unmanned systems. Chinese Science Bulletin. 2012. Т. 57, № 26. С. 3409-3418. URL: https://doi.org/10.1007/s11434-012-5183-2 (дата звернення: 25.12.2023).

111. Yadin S. The Crowdsourcing of Regulatory Monitoring and Enforcement. The Law & Ethics of Human Rights. 2023. Т. 17, № 1. С. 95–125. URL: https://doi.org/10.1515/lehr-2023-2006 (дата звернення: 12.10.2023).

112. Yaqot, M.; Meneze, B.C. Unmanned Aerial Vehicle (UAV) in Precision Agriculture: Business Information Technology towards Farming as a Service. In Proceedings of the 2021 1st International Conference on Emerging Smart Technologies and Applications (eSmarTA), Sana'a, Yemen, 10-12 August 2021; pp. 1-7.

113. Yu, Y.; Shi, C.; Shan, D.; Lippiello, V.; Yang, Y. A hierarchical control scheme for multiple aerial vehicle transportation systems with uncertainties and state/input constraints. Appl. Math. Model. 2022, 109, 651-678.

114. Zemlianko H., Kharchenko V. Cyber Security Systems of Highly Functional Uav Fleets for Monitoring Critical Infrastructure: Analysis of Disruptions, Attacks and Counterapproaches. Èlektronnoe modelirovanie. 2024. T. 46, № 1. C. 41–54. URL: https://doi.org/10.15407/emodel.46.01.041.

115. Zemlianko H., Kharchenko V. Cybersecurity risk analysis of multifunctional UAV fleet systems: a conceptual model and IMECA-based technique. Radioelectronic and Computer Systems. 2023. № 4. C. 152–170. URL: https://doi.org/10.32620/reks. 2023.4.11 (дата звернення: 29.01.2024).

116. Zhang X., Bai Y., He K. On Countermeasures against Cooperative Fly of UAV Swarms. Drones. 2023. T. 7, № 3. C. 172. URL: https://doi.org/10.3390/drones7030172 (дата звернення: 16.09.2023).

117. Zheng X., Tan Y., Li D. Navigating Environmental Governance in China's Hog Sector: Unraveling the "Race to the Bottom" Phenomenon and Spatial Dynamics. Journal of the Knowledge Economy. 2024. URL: https://doi.org/10.1007/s13132-024-01800-8 (дата звернення: 12.10.2023).

118. Алешин Б. С., Суханов В. Л., Шибаев В. М., Шнырев А. Г. Типы беспилотных летательных аппаратов // Межотраслевой альманах. 2014. № 46. URL: http://slaviza.ru/print:page,1,1494-tipy-bespilotnyh-letatelnyh-apparatov.html. (дата звернення: 04.09.2023).

119. Весоловскі Т. Терористична атака 20-річної давності. Як 11 вересня 2001 року змінило світ? Радіо Свобода. URL: https://www.radiosvoboda.org/a/terorystychna-ataka-11-veresnya-2001-roku/31452813.html (дата звернення: 22.10.2023).

120. Деякі питання об'єктів критичної інфраструктури: Постанова Каб. Міністрів України від 09.10.2020 р. № 1109: станом на 11 трав. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-п#Text (дата звернення: 12.10.2023).

121. ДСТУ 9067:2021. Дизайн і ергономіка. Комплекси безпілотних повітряних суден. Правила оцінювання рівня якості. Чинний від 2021-09-01. Наказ про прийняття НД: 2021-02-16 № 54. Вид. офіц. Україна : ДП «УкрНДНЦ», 2021. 7 с.

122. ДСТУ EN ISO/IEC 27001:2022. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. На заміну EN ISO/IEC 27001:2017, IDT; ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015, IDT ; чинний від 2023-12-31. Наказ про прийняття НД: 2022-12-28 № 285. Вид. офіц. Україна : ДП «УкрНДНЦ», 2022. 37 с.

123. ДСТУ ISO/IEC TR 20004:2017 Інформаційні технології. Методи захисту. Уточнений аналіз вразливості програмного забезпечення згідно з ISO/IEC 15408 та ISO/IEC 18045 (ISO/IEC TR 20004:2015, IDT). БУДСТАНДАРТ Online - нормативні документи будівельної галузі України. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=74704 (дата звернення: 08.06.2023).

124. ДСТУ ISO/IEC/IEEE 12207:2018. Інженерія систем і програмних засобів. Процеси життєвого циклу програмних засобів (ISO/IEC/IEEE 12207:2017, IDT). На заміну ДСТУ ISO/IEC 12207:2016 ; чинний від 2018-08-15. Наказ про прийняття НД: 2018-08-06 № 261. Вид. офіц. Україна : ДП «УкрНДНЦ», 2018. 156 с.

125. ДСТУ В 7371:2020. Техніка авіаційна державної авіації. Апарати літальні безпілотні. Основні терміни та визначення понять. Класифікація. На заміну 7371:2013; чинний від 2021-07-01. Вид. офіц. Україна: Стандартизація продукції оборон. призначення, 2020. 16 с.

126. Європейське агентство з безпеки авіації (EASA). URL: https://www.easa.europa.eu/ (дата звернення: 19.08.2022).

127. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: Норм. док. системи техн. зах. інформації від 28.05.1999 р. № НД ТЗІ 1.1-002-99: станом на 28 груд. 2012 р. URL: https://tzi.com.ua/downloads/1.1-002-99.pdf (дата звернення: 03.11.2021).

128. Застосування безпілотних авіаційних систем у сфері цивільного захисту: монографія / Д.В. Бондар, А.В. Гурник, А.О. Литовченко, В.В. Хижняк, В.Л.

Шевченко, Д.М. Ядченко. Київ, 2022, 312 с. URL: eSLU7FcmeJYIEPehdm0Ill3Cn39Bi1BMIl3IedcX.pdf (dsns.gov.ua)

129. Землянко Г.А., Харченко В.С. IMECA-аналіз кібербезпеки систем багатофункціональних флотів БПЛА при комбінованих атаках: базові моделі та вибір контрзаходів. Measuring and computing devices in technological processes. 2023. № 4. С. 225–233. URL: https://doi.org/10.31891/2219-9365-2023-76-30.

130. Кодекс цивільного захисту України : Кодекс України від 02.10.2012 р. № 5403-VI : станом на 5 жовт. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/5403-17#Text (дата звернення: 12.10.2023).

131. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: Норм. док. системи техн. зах. інформації від 28.05.1999 р. № НД ТЗІ 2.5-004-99: станом на 28 груд. 2012 р. URL: https://tzi.com.ua/downloads/2.5-004-99.pdf (дата звернення: 10.04.2022).

132. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі :: Державний університет інформаційно-комунікаційних технологій. Головна :: Державний університет інформаційно-комунікаційних технологій. URL: https://duikt.edu.ua/ua/lib/1/category/919/view/1037?lang=ua&act=view&page=1&category=919&id=1037 (дата звернення: 08.04.2024).

133. Міжнародні стандарти цивільної авіації (МКАО). URL: https://www.icao.int/ (дата звернення: 19.08.2022).

134. Нова українська система Menatir для дистанційного моніторингу: базові станції з БПЛА та місії без участі оператора. ITC.ua. URL: https://itc.ua/partner-news/novaya-ukraynskaya-systema-menatir-dlya-dystantsyo nnogo-monytorynga-bazovye-stantsyy-s-bpla-y-myssyy-bez-uchastyya-operatora/ (дата звернення: 19.09.2023).

135. Повітряний кодекс України: Кодекс України від 19.05.2011 р. № 3393-VI: станом на 2 серп. 2023 р. URL: https://zakon.rada.gov.ua/laws/show /3393-17#Text (дата звернення: 05.09.2023).

136. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі::Державний університет інформаційно-комунікаційних технологій. Головна::Державний університет інформаційно-комунікаційних технологій. URL: https://duikt.edu.ua/ua/lib/1/category/919/view/1057 (дата звернення: 08.03.2024).

137. Про затвердження Авіаційних правил України "Правила використання повітряного простору України": Наказ Держ. авіац. служби України від 11.05.2018 р. № 430/210. URL: https://zakon.rada.gov.ua/laws/show/z1056-18#Text (дата звернення: 05.09.2023).

138. Про затвердження Змін до Правил інженерно-авіаційного забезпечення державної авіації України: Наказ М-ва оборони України від 03.08.2021 р. № 223. URL: https://zakon.rada.gov.ua/laws/show/z1221-21#Text (дата звернення: 05.09.2023).

139. Про затвердження Положення про використання повітряного простору України: Постанова Каб. Міністрів України від 06.12.2017 р. № 954: станом на 5 січ. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/954-2017-п#Text (дата звернення: 05.09.2023).

140. Про затвердження Правил технічної експлуатації безпілотних авіаційних комплексів І класу державної авіації України : Наказ М-ва оборони України від 10.08.2018 р. № 401. URL: https://zakon.rada.gov.ua/laws/show/z1062-18#Text (дата звернення: 05.09.2023).

141. Про критичну інфраструктуру: Закон України від 16.11.2021 р. № 1882-IX: станом на 5 груд. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 12.10.2023).

142. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2469-19 (дата звернення: 08.08.2023).

143. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2163-19. (дата звернення: 08.08.2023)

144. Розділ 1. Підрозділ 1.2 Методи контролю та оцінювання інформаційної безпеки комп’ютерних мереж з використанням пентестингу. // Розроблення засобів тестування та верифікації вбудованих і розподілених гарантоздатних ІТ-систем та інфраструктур : звіт про НДР (проміж.) / М-во освіти і науки України, Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харків. авіац. ін-т" ; керівник Харченко В. С. ; викон.: Фесенко Г. В. [та інш.]. - Харків, 2021. - 197 с. - № ДР 0121U113842.

145. Розділ 3. Підрозділ 3.1 Методи і засоби побудови енергоефективних засобів побудови смарт-систем з використанням IoT і Edge комп’ютингу. // Розроблення методів формування вимог, аналізу, оцінювання та зменшення витрат ресурсів протягом життєвого циклу програмного забезпечення, мобільних пристроїв, хмарних обчислень : звіт про НДР (заключ.) : Д503-1/2018-Ф . Т. 1 / М-во освіти і науки України, Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харків. авіац. ін-т" ; керівник Харченко В. С. ; викон.: Колісник М. О. [та інш.]. - Харків, 2020. - 232 с. - № ДР 0118U003822 - Інв. № 0221U000030.

146. Розділ 3. Підрозділ 3.2 Оцінка кібербезпеки Інтернету систем дронів з урахуванням радіочастотної вразливості на основі. // Теоретичне обгрунтування методології, структури, моделі, методи оцінювання надійності і живучості інтелектуальних систем моніторингу потенційно небезпечних і військових об'єктів з використанням багатоцільових флотів БПЛА : звіт про НДР (проміж.) : Д503-1/2021-Ф / М-во освіти і науки України, Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харків. авіац. ін-т" ; керівник Харченко В. С. ; викон.: Морозова О. І. [та інш.]. - Харків, 2021. - 230 с. - № ДР 0121U112172.

147. Розділ 3. Підрозділ 3.5 Розроблення програмно-апаратних засобів для систем розумного міста. // Розробка моделей та засобів кібербезпеки інформаційних і комунікаційних систем. Впровадження запропонованих принципів, моделей та методів оцінювання та розробки гарантоздатних комп'ютерних систем, мереж та ІТ-інфраструктур : звіт про НДР (заключ.) / М-во освіти і науки України, Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харків. авіац. ін-т" ; керівник Харченко В. С. ; викон.: Лисенко І. В. [та інш.]. - Харків, 2020. - 245 с. - № ДР 0117U05349 - Інв. № 0221U000032.

148. Ростопчин В. В. Ударні безпілотні літальні апарати та протиповітряна оборона - проблеми та перспективи протистояння // Безпілотна авіація. 2019. URL: https://www.researchgate.net/publication/331772628_Udarnye_bespilotnye_letatelnye_apparaty_i_protivovozdusnaa_oborona_-problemy_i_perspektivy_protivostoania (дата звернення: 04.09.2023).

149. Сігорський В. П. Математичний апарат інженера. - Київ: Техніка, 1975. - 768 с.

150. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: Норм. док. системи техн. зах. інформації від 28.05.1999 р. № НД ТЗІ 1.1-003-99. URL: https://tzi.ua/assets/files/1.1_003_99.pdf (дата звернення: 03.11.2021).

151. Типове положення про службу захисту інформації в автоматизованій системі::Державний університет інформаційно-комунікаційних технологій. Головна::Державний університет інформаційно-комунікаційних технологій. URL: https://duikt.edu.ua/ua/lib/1/category/2342/view/1023 (дата звернення: 08.03.2024).

152. Хусити вдарили з дрона по нафтосховищу в Саудівській Аравії - DW - 08.03.2021. dw.com. URL: https://www.dw.com/ru/husity-nanesli-udar-s-drona-po-neftehranilishhu-v-portu-saudovskoj-aravii/a-56801618 (дата звернення: 04.09.2023).

ДОДАТОК А. СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

1. Anatoly, P., Zemlianko, H., Kharchenko, V. (2020). Prototyping and Rapid Development of IoT Systems in Context of Edge Computing. In: Nechyporuk, M., Pavlikov, V., Kritskiy, D. (eds) Integrated Computer Technologies in Mechanical Engineering. *Advances in Intelligent Systems and Computing*, vol 1113. Springer, Cham. https://doi.org/10.1007/978-3-030-37618-5_23.

2. Assoc. Prof., Dr A. P. Plakhteyev, MSc student H. Zemlianko (KhAI). Section 31. Prototyping and rapid development of IoT systems. //Drozd A. et al. Internet of Things for Industry and Human Application //Volumes 1–3. Volume 2. Modelling and Development. – 2019.

3. Torianyk V., Kharchenko V., Zemlianko H. IMECA based assessment of internet of drones systems cyber security considering radio frequency vulnerabilities //IntelITSIS //CEUR Workshop Proceedings. – 2021. – С. 460-470.

4. Pevnev, V., Tsuranov, M., Zemlianko, H., Amelina, O. (2021). Conceptual Model of Information Security. In: Nechyporuk, M., Pavlikov, V., Kritskiy, D. (eds) Integrated Computer Technologies in Mechanical Engineering - 2020. ICTM 2020. *Lecture Notes in Networks and Systems*, vol 188. Springer, Cham. https://doi.org/10.1007/978-3-030-66717-7_14.

5. Pevnev, V., Plakhteev, A., Tsuranov, M., Zemlianko, H., Leichenko, K. (2022). “Smart City” Technology: Conception, Security Issues and Cases. In: Nechyporuk, M., Pavlikov, V., Kritskiy, D. (eds) Integrated Computer Technologies in Mechanical Engineering - 2021. ICTM 2021. *Lecture Notes in Networks and Systems*, vol 367. Springer, Cham. https://doi.org/10.1007/978-3-030-94259-5_19.

6. Pevnev, V., Frolov, A., Tsuranov, M., & Zemlianko, H. (2022). Ensuring the Data Integrity in Infocommunication Systems. *International Journal of Computing*, *21*(2), 228-233. URL:https://doi.org/10.47839/ijc.21.2.2591.

7. Zemlianko H., Kharchenko V. Cybersecurity risk analysis of multifunctional UAV fleet systems: a conceptual model and IMECA-based technique. *Radioelectronic*

and Computer Systems. 2023. № 4. С. 152–170. URL: https://doi.org/10.32620/reks.2023.4.11.

8. Zemlianko H., Kharchenko V. Cyber Security Systems of Highly Functional Uav Fleets for Monitoring Critical Infrastructure: Analysis of Disruptions, Attacks and Counterapproaches. *Èlektronnoe modelirovanie*. 2024. Т. 46, № 1. С. 41–54. URL: https://doi.org/10.15407/emodel.46.01.041.

9. Землянко Г.А., Харченко В.С. IMECA-аналіз кібербезпеки систем багатофункціональних флотів БПЛА при комбінованих атаках: базові моделі та вибір контрзаходів. *Measuring and computing devices in technological processes*. 2023. № 4. С. 225–233. URL: https://doi.org/10.31891/2219-9365-2023-76-30.

10. Землянко Г.А., Пєвнєв В.Я., Ніколас Бардис, Харченко В. С., Розділ 9. Розробка моделі загроз для безпілотних літальних апарптів. 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. 159–177. ISBN 978-617-8335-01-4. URL:https://dspace. library.khai.edu/xmlui/handle/123456789/5307.

11. Heorhii Zemlianko, Kyrylo Leichenko, "Smart City" technology: conception, security issues and cases. Book of abstracts of the International Workshop on Reliability Engineering and Computational Intelligence 2020 (RECI 2020), Zilina, Slovakia, 27-29 October 2020. P. 41. URL: https://ki.fri.uniza.sk/RECI2020/Abstracts%20of%20RECI%202020.pdf

12. Землянко Г.А. Implementation of smart grid technologies in the power system of Ukraine. Матеріали III НТК «Інформаційна, функційна і кібербезпека» (СКІФіК-2023), 30 лист.– 1 груд. 2023 р. Харків, Україна. Харків: НАКУ «ХАІ», 2023. С. 105–106.

13. Землянко Г.А. Ensuring cybersecurity of the cyber physical system of combined fleets of unmanned aerial, ground and sea vehicles. Всеукраїнська науково-технічна конференція «Інтегровані комп’ютерні технології в машинобудуванні» ІКТМ 2023, Харьків, 2023.

ДОДАТОК Б. СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Таблиця № Б.1 – Американська класифікація БПЛА

Класифікаційний тип	Маса, кг	Висота польоту, км	Швидкість, км/год	Приклади
I	0 - 9	до 0,365	до 185	RQ-11 Raven, RQ-20 Puma, Wasp III, RQ-16 T-Hawk
II	9,5 - 25	до 1,07	до 460	ScanEagle
III	понад 600	до 5,5	не визначено	RQ-2 Pioneer, RQ-5 Hunter, RQ-7 Shadow, RQ-21 Blackjack
IV	понад 600	до 5,5	не визначено	RQ-1/MQ-1 Predator, MQ-1C Grey Eagle, X-47, YMQ-18 Hummingbird, MQ-8 Fire Scout
V	понад 600	понад 5,5	не визначено	RQ-4 Global Hawk, MQ-9 Reaper

Таблиця № Б.2 – Західноєвропейська класифікація БПЛА

Класифікаційний тип	Середня висота польоту, км	Середній радіус дії, км	Середня тривалість польоту, год	Приклади
1	2	3	4	5
Micro-UAV (мікро-БПЛА)	0,6	2	до 1	EMTAIadin (Германія)
Mini-UAV або Close-Range UAV (міні-БПЛА або БПЛА ближнього радіусу дії)	до 2	до 10	до 2	Bird Eye 400 (Ізраіль)
Short-range UAV (БПЛА малого радіусу)	до 3	50 – 150	до 6	Speiwer (Франція)
Medium-range UAV (БПЛА середнього радіусу)	до 6	100 - 300	до 12	Hermes 450 (Ізраіль)
HALE (High-altitude, long-endurance) (висотний БПЛА тривалого польоту)	понад 9,1	глобальний	понад 24	Global Hawk (США)

Продовження таблиці Б.2

1	2	3	4	5
MALE (Medium-altitude, long-endurance) (середньовисотний БПЛА тривалого польоту)	5 - 15	200 - 500	до 24	Patroller (Франція)

Примітка: класи Short-range UAV та Medium-range UAV часто поєднують у загальний клас TUAV (Tactical unmanned aerial vehicle) – тактичні БПЛА.

Таблиця № Б.3 – Російська класифікація БПЛА

Класифікаційний тип	Злітна маса, кг	Дальність дії, км
Нано-БПЛА ближнього радіусу дії	до 0,25	до 2
Мікро- та міні-БПЛА ближнього радіусу	до 5	25 - 40
Легкі БПЛА малого радіусу дії	5 - 50	10 - 70
Легкі БПЛА середнього радіусу дії	50 - 100	70 – 150 (250)
Середні БПЛА	100 - 300	150 - 1000
Середньо-важкі БПЛА	300 - 500	70 - 300
Важкі БПЛА середнього радіусу дії	500	70 - 300
Тяжкі БПЛА великої тривалості польоту	1500	1500
Безпілотні бойові літаки (ББЛ)	500	1500

Таблиця № Б.4 – Гармонізована класифікація БПЛА

Клас БПЛА	Категорія	Міжнародне позначення	Позначення	Назва	Вага, кг	Радіус дії, км	Практична межа, км	Тривалість польоту, год
1	2	3	4	5	6	7	8	9
Малі	I	η	η	нано	до 0,025	до 1	0,1	≤ 1
		μ	μ	мікро	до 5	до 10	3	1
		mini	mini	міні	до 25	10 - 40	3	≤ 4
Легкі	II	CR	БлД	Ближньої дії класа 1	25 - 50	25 - 75	3	2-4
				Ближньої дії класа 2	50 - 100	50 - 100	3	≤ 6
Середні	III	SR	МД	Малої дальності	до 200	до 150	4	6-8

Продовження таблиці Б.4

1	2	3	4	5	6	7	8	9
Середні	III	MR	СД	Середньої дальності	до 500	200	5	10-12
	IV	MRE		Середньої дальності з великою тривалість польота	500	500	8	10-18
		LADP	БД	Маловисотний великої дальності	до 250	більше 250	до 4	1,5-2
Тяжкі	V	LALE		Маловисотний з великою тривалість польота	до 250	більше 500	4	18
	V-VI	MALE		Середньовисотний з великою тривалість польота	до 100	більше 1000	8	24
	VII	HALE		Висотний з великою тривалість польота	до 2500	більше 4000	20	більше 24
Бойові	VIII	UCAV	Б	Безпілотний ударний	більше 1000	більше 500	12	1,5 - 2
		DEG		Помилкова ціль	150 - 500	0 - 500	0,05 - 5	до 4
		TGT		Повітряна ціль	10 - 1000	5 - 200	0,05 - 10	більше 0,5
Змішані	IX	OPA	ОП	Пілотований по вибору (опційно) ЛА	до 200			
		CMA	ПП	Переобладнений пілотований ЛА				

Таблиця № Б.5 – Світові вимоги та норми функціонування БПЛА

Країни	Початковий регламент		Експлуатаційні вимоги					Шлях польоту			
	Вага (<25 кг)	Вимоги	Просторове обмеження	Радіозв'язок	Візуальна лінія зору	Особливості безпеки	Конфіденційність	Юрисдикція	Реєстрація та маркування	Подробиці дозволу польоту	Кваліфікація оператора
1	2	3	4	5	6	7	8	9	10	11	12
Україна	Якщо застосовується	Відсутність реєстрації	Військові об'єкти, аеропорти, в'язниці, атомні електростанції	2.4-5 ГГц	В межах прямої видимості	Невстановлений	Жодних твердих обмежень	Місцевий уряд	Ім'я, адреса, номер телефону, призначення	Мета використання	Національний, дорослий
Німеччина	Якщо застосовується	Конкретний дозвіл на дозвіл на політ	Військові об'єкти, аеропорти, в'язниці, атомні електростанції	2.4-5 ГГц	100 м – 1 км	Сертифікат проекту, виклик на базу	Обмежений запис осіб	Місцевий уряд	Ім'я, адреса, дата народження, мета	Попередньо визначений шлях, мета використання та деталі	Підтвердження досвіду, знань та тренінгів

Кінець таблиці Б.5

1	2	3	4	5	6	7	8	9	10	11	12
Китай	Якщо застосовується	Не вимагається	Військові об’єкти, аеропорти, в’язниці, атомні електростанції	2.4-5 ГГц	В межах прямої видимості	Не застосовується	Все ще дискусійне	Китайське законодавство щодо цивільних польотів	Назва, адреса, номер телефону польоту	Призначення польоту, місця зйомки, шлях	Національний, дорослий, ліцензований
США	Якщо застосовується	Ліцензія / дозвіл	Військові об’єкти, аеропорти, в’язниці, атомні електростанції	2.4-5 ГГц	В межах прямої видимості	Сертифікат проекту, виклик на базу, безпечна посадка	Федеральної авіаційної адміністрації	Обмежений запис осіб	Ім’я, адреса, дата народження, мета	Попередньо визначений шлях, мета використання та деталі	Дорослий, посвідчення польоту

ДОДАТОК В. СУЧАСНА СИСТЕМА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

На сьогодні існують два основні нормативно-правові документи, які контролюють і визначають, що таке критична інфраструктура в Україні:

– Закон України "Про критичну інфраструктуру" (1882-IX від 16.11.2021), розроблений 15.12.2021, але який набрав чинності лише 15.06.2022.

– Постанова КМУ № 1109 від 09.10.2020 "Деякі питання об'єктів критичної інфраструктури" зі змінами від 29.12.2021, яка набула чинності 31.12.2021.

Згідно з цими документами, критична інфраструктура (КІ) - об'єкти інфраструктури, системи, їхні частини та їхня сукупність, що є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєва важливим національним інтересам.

Водночас, нещодавно Постановою Кабінету Міністрів № 787 від 12 липня 2022 року "Про утворення Державної служби України з питань захисту критичної інфраструктури та забезпечення національної стійкості систем" Державну службу (ДССЗІ) було визначено компетентним органом у сфері КІП. Рішення також набуде чинності після внесення змін до Закону про Державний бюджет України на 2022 рік, які передбачатимуть фінансування ДССЗЗІ.

Таким чином, наразі реєстр об'єктів критичної інфраструктури ще не створений і не функціонує. Порядок ведення реєстру ще не затверджений Радою Міністрів, а компетентний орган, який має створювати та вести такий реєстр у сфері КІП, ще не функціонує.

На рівні держави це створює багато проблем і не юридично обґрунтованих дефектів і не повноцінно працюючих механізмів величезної системи, але на даний момент згідно з Кодексом цивільного захисту України, статтею 43, моніторинг здійснюється різними організаціями або представниками міської адміністрації, свого регіону і території. Це викликає як фінансові так і політичні питання.

Якщо розглядати що таке моніторинг загалом згідно з нормативно-правовими актами, то:

– сучасний термін "моніторинг" позначає систему регулярного контролю та постійних спостережень, що проводяться за певною програмою для оцінки поточного стану НС, аналізу всіх процесів, що відбуваються в ній на цей період, а також можливого завчасного виявлення негативних тенденцій її змін;

– найбільш інформативним і достовірним є комплексний екологічний моніторинг НС. Комплексний екологічний моніторинг НС - це організація системи спостережень за станом об'єктів НС для оцінювання їхнього фактичного рівня забруднення та попередження про критичні ситуації, які виникають, шкідливі для здоров'я людей та інших живих організмів. здоров'я людей та інших живих організмів;

– моніторинг надзвичайних ситуацій - це система безперервних спостережень, лабораторного та іншого контролю для оцінювання стану захисту населення і територій та небезпечних процесів, що можуть призвести до загрози або виникнення надзвичайних ситуацій, а також своєчасне виявлення тенденцій до їх зміни.

ДОДАТОК Г. КІБЕРАТАКИ НА БЕЗПІЛОТНІ ЛІТАЛЬНІ АПАРАТИ

Інформаційна взаємодія між БПЛА і контролером наземної станції зазвичай здійснюється через мережу Wi-Fi, відповідну стандарту IEEE 802.11. Ця мережа вразлива для порушень безпеки: відсутність шифрування на бортових чіпах безпілотників або атака "людина-всередині" може дозволити захопити управління БПЛА на великій відстані. Незахищений Wi-Fi зв'язок додатково збільшує ризик злому. Існує кілька рішень, таких як SkyJack, які використовують node.js та клієнт node-ar-drone, здатні автономно знаходити та захоплювати управління іншими БПЛА в межах мережі чи навіть на дальності польоту, створюючи армію "зомбі-БПЛА". Профілактика такої загрози можлива, наприклад, з використанням програмного рішення Wi-Fi Protected Access, що забезпечує аутентифікацію пароля для БПЛА, що ускладнює доступ зловмисника. У цьому роздері були розглянуті типові атаки на флоти БПЛА і самі БПЛА з відкритим Wi-Fi, до яких може підключитися кілька пристроїв. Після підключення до БПЛА, можна визначити його IP-адресу та провести додаткове дослідження. Використання інструмента сканування Nmap допоможе виявити відкриті порти на БПЛА та вивчити їхню безпеку. Безкоштовна утиліта з відкритим кодом для аналізу мережевих об'єктів може надати список відкритих портів на цільовому об'єкті.

Атака "отказ в обслуживании" (DoS) представляет ряд видів нападів, що можуть призвести до втрати доступу між оператором базової станції та БПЛА. Ця атака спрямована на перешкоджання законним користувачам у доступі до системи, як зображено на рисунку Г.1. Флуд-атаки є найпоширенішим типом DoS-атак, коли зловмисник перенавантажує мережу інформацією. Один з простих інструментів для здійснення DoS-атаки - це мережевий сканер hping3, що функціонує як генератор та аналізатор пакетів для протоколу TCP/IP (Hping - Активний Інструмент Мережевої Безпеки, один з інструментів для тестування мережевої безпеки). Цей інструмент може запустити простий пінг-флуд, відправляючи ICMP-пакети з високою швидкістю, не очікуючи відповідей. Така атака перенавантажує цільову систему запитами, що робить її недоступною для іншого спілкування.

Використовуючи різні прапорці, такі як fast або faster, можна вказати швидкість передачі пакетів.

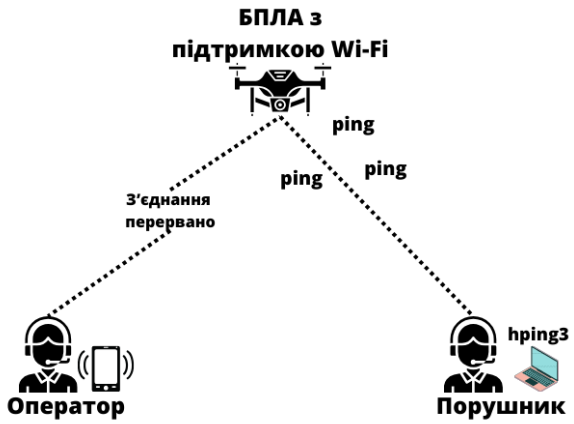


Рисунок В.1 – Атака відмови в обслуговуванні під час втрати з'єднання через переповнення повідомленнями

Друга атака, показана на рисунку Г.2, спрямована на деаутентифікацію БПЛА, що дозволить зловмиснику захопити контроль над ним. Він може відключити пілота від зв'язку з БПЛА, що змусить безпілотник зупинитися у повітрі. Якщо у зловмисника є інший контролер (наприклад, смартфон) із додатком для керування БПЛА, він може моментально підключитися та отримати повний контроль. Атакуючий ноутбук намагатиметься підключитися до БПЛА, доки залишається зв'язок із справжнім пілотом. Зловмисник, що знаходиться в тій же мережі, легко дізнатися MAC-адресу контролера БПЛА. Це необхідно для атаки, проте для швидшого захоплення управління зловмиснику слід зберегти зв'язок. Для таких атак використовують Aircrack-ng, набір інструментів для оцінки безпеки Wi-Fi [12]. Процес починається з пасивного сканування бездротової мережі, потім за допомогою airodump-ng (частина Aircrack-ng) фільтруються та зберігаються пакети лише з цієї мережі. Потім складається список клієнтів, підключених до мережі, для деаутентифікації. Модуль Aireplay-ng, впроваджений Aircrack-ng, посилає роз'єднувальні пакети клієнтам, щоб відключити їхню відмінність від точки доступу, включаючи БПЛА і, за необхідності, певного клієнта.

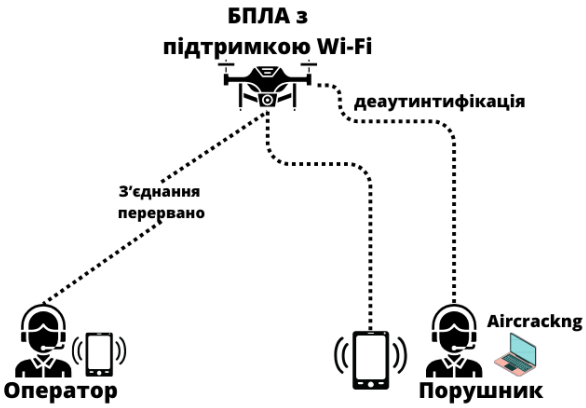


Рисунок В.2 – Схема атаки деаутентифікації для перехоплення керування БПЛА зловмисником

Це відбувається шляхом відправки 128 пакетів, по 64 на клієнта та БПЛА. Це призведе до деаутентифікації з'єднання між БПЛА та його контролером. Подальша поведінка безпілотних апаратів після деаутентифікації може бути різною – від посадки до краха.

Атака «людина посередині» (MitM), зображена на рисунку Г.3, передбачає наявність зловмисника між оператором БПЛА і самим пристроєм. Для здійснення такої атаки може використовуватись, наприклад, пристрій WiFi Pineapple. Після налаштування воно може бути запущене в режимі розвідки для відстеження та відображення доступних точок доступу та клієнтів, які до них підключені. Як тільки режим Recon виявить цільову точку доступу – вибраний безпілотник, його можна додати до PineAP SSID. Пристрій почне емулювати SSID БПЛА, що дозволить оператору БПЛА автоматично підключитися до Pineapple. Мета цієї атаки полягає у перевірці працездатності безпілотника під час підключення контролера через WiFi Pineapple. Не знайдено жодних загальнодоступних досліджень щодо використання WiFi Pineapple у таких ситуаціях з безпілотниками, тому результат залишається незрозумілим. Передбачається, що безпілотник продовжуватиме функціонувати як завжди, не виявляючи зловмисника, що знаходиться між БПЛА і оператором.

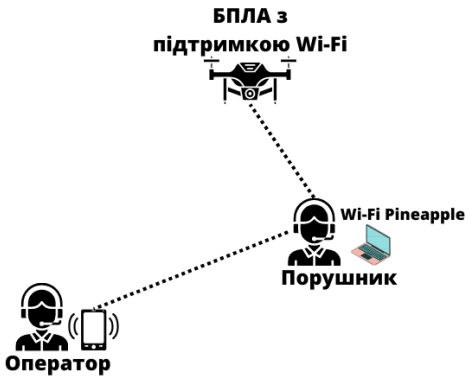


Рисунок В.3 – Схема атаки "людина-посередині" за допомогою WiFi Pineapple

Атака несанкціонованого доступу з привілеєвим користувачем (root-доступ) полягає у прямому підключенні зловмисника до БПЛА та отриманні доступу до ресурсів, виявлених після етапу розвідки. Наприклад, використання утиліти Nmap дозволяє сканувати IP-мережі для знаходження відкритих портів, до яких можна потенційно отримати доступ через протоколи, такі як Telnet та FTP. Якщо Telnet доступний без будь-яких додаткових облікових даних, зловмисник може отримати root-доступ. Це надасть йому повний контроль над пристроєм, даними на ньому та будь-якими виконуваними сценаріями, як показано на рисунку Г.4. Очікуваний результат такої атаки полягає у доступності портів та можливості встановлення з'єднань без необхідності будь-яких облікових даних.

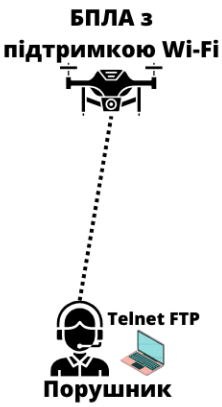


Рисунок В.4 – Підключення до дрона через Telnet

Тип атаки, відомий як заміна пакетів, включає створення IP-пакетів з метою маскування під іншу систему, наприклад, контролер БПЛА, як показано на рсиунку Г.5. Для цієї атаки початковим кроком є моніторинг трафіку між БПЛА та його контролером, використовуючи інструмент, такий як Wireshark. Він перехоплює мережевий трафік, що дозволяє проаналізувати протоколи та зрозуміти, як системи взаємодіють.

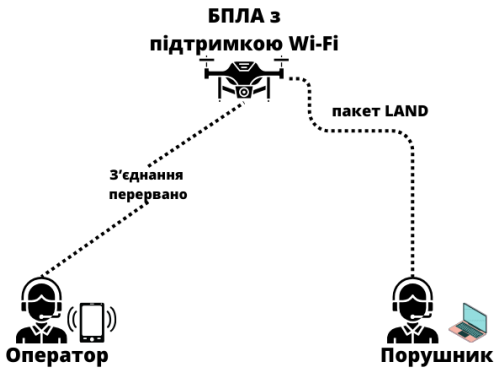


Рисунок В.5 – Підміна пакетів зловмисником, який видає себе за пілота безпілотника

Кожна захоплена команда має свій порядковий номер, щоб запобігти використанню застарілих пакетів, але скидається, якщо дві секунди не надходить керуючий пакет на БПЛА. Це дозволяє фальсифікувати ці пакети, скидаючи лічильник або використовуючи більш високий порядковий номер. Крім того, існує клієнт node.js для керування БПЛА без мобільного додатка. З його допомогою можна написати скрипти, які керують БПЛА через функції, такі як take off() або land(). Передбачається, що пакет відправки буде підроблений, що в результаті успішно призведе до посадки безпілотника.

Всі вище описані атаки, які можна провести через блокувальник БПЛА, можно розробити на контролері Raspberry Pi. Цей пристрій автоматизує атаки через скрипти bash, що ілюструються на рисунку Г.6. Raspberry Pi може бути налаштований так, що зловмисник не обов'язково повинен мати ноутбук для атаки - він може використовувати цей пристрій, готовий до проведення атак у будь-який

час. Підключення до контролера можливо віддалено через SSH, що дозволяє керувати системою та тунелювати TCP-з'єднання. Атаки реалізуються за допомогою скриптів bash залежно від типу атаки. Наприклад, коли Raspberry Pi виявляє SSID, що починається з рядка "ardrone2", воно підключається до Wi-Fi і через Telnet вимикає БПЛА. Результат - відключення безпілотника, навіть якщо зловмисник знаходиться поряд з Raspberry Pi та БПЛА.

У цьому розділі розглянуті найчастіше використовувані зловмисниками різні вразливості, з допомогою яких може бути перехоплено управління флоти БПЛА, і сам БПЛА: відмова у обслуговуванні, деаутентифікація, людина-посередині, несанкціонований доступ із повноваженнями суперкористувача і заміна пакетів. Крім того, у розділі описано можливість реалізації блокувальника БПЛА на основі контролера Raspberry Pi, який запускає скрипти bash.

ДОДАТОК Ґ. IMECA АНАЛІЗ СБФ БПЛА

Позначення та роз’яснення для стовпчиків IMECA таблиці:

- нумерація;
- елемент інфраструктури СБФ БПЛА;
- номер порушника (1 - внутрішній адміністратор інформаційної системи та безпеки, 2 - спеціальні служби закордонних держав, 3 - злочинні угруповання, 4 - колишні співробітники організації, 5 - природа);
- потенціал порушника (перший стовпчик у виді числа, другий стовпчик у виді букви);
- характер загрози, ХЗ (Ш – штучно, зроблено людиною, П – зроблено природою);
- загрози;
- вразливості системи;
- атаки, які реалізовані через вразливість у системі;
- властивості безпеки, на які спрямована атака (К - конфіденційність, Ц - цілісність, Д - доступність, С - спостережність);
- наслідки, після реалізованої атаки;
- критичність системи (P_1 – ймовірність, S_1 – тяжкість, R_1 - ризик);
- контрзаходи системи;
- критичність системи після контр заходів (P_2 – ймовірність, S_2 – тяжкість, R_2 - ризик).

Таблиця Ґ.1 – IMECA аналіз системи багатофункційних флотів БПЛА

№	Елемент інфраструктури СБФ БПЛА	Порушник	Потенціал порушника		ХЗ	Загроза	Вразливості	Атака	Властивості безпеки				Наслідки	Критичність			Контрзаходи										Критичність після контрзаходів		
					Ш/П				К	Ц	Д	С		Р	S	R	1	2	3	4	5	6	7	8	9	10	Р	S	R
1	2	3	4		5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
1	Центри зв'язку	1	8,4	А	Ш	Зміна навігаційних даних БПЛА	Використання нешифровані протоколи навігації	Маніпулювання навігаційними даними через атаку "Man-in-the-Middle". GPS-отруєння	Так	Так	Так	Так	Зміна навігаційних даних, переривання роботи системи зв'язку, можливість здійснення несанкціонованих команд	9	9	81		+	+				+		+		6	9	54
2							Використання слабких паролів	Брутфорс атака на паролі	Так	Так	Так	Так	Несанкціонований доступ адміністратора, зміна навігаційних даних, можливість внесення змін у системі без належних прав	8	6	48			+			+			+		5	6	30
3	Система управління БПЛА				Ш	Віддалене вимкнення БПЛА	Відсутність або слабка сегментація мережі	Отримання несанкціонованого доступу внутрішнім користувачем	Ні	Так	Так	Так	Віддалене вимкнення БПЛА, можливість виконання несанкціонованих дій в системі управління.	7	7	49			+			+			+		4	7	28
4							Несанкціонований доступ до системи через слабку аутентифікацію	Використання аутентифікаційних вразливостей	Так	Так	Так	Так	Віддалене вимкнення БПЛА, можливість внесення змін у систему управління без належних авторизаційних прав	8	7	56						+			+		5	7	35

Продовження таблиці Г.1

1	2	3	4		5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
5	Система моніторингу стану БПЛА	1	8,4	А	Ш	Зміна даних про стан БПЛА	Слабкі механізми аутентифікації та авторизації	Отримання несанкціонованого доступу	Так	Так	Так	Так	Можливість зміни даних про стан БПЛА без належних авторизаційних даних, порушення цілісності та достовірності інформації	9	7	63			+			+	+		+		5	7	35
6							Відсутність журналювання та відслідковування доступу	Прихована модифікація даних про стан БПЛА	Ні	Так	Так	Так	Можливість внесення змін у журналах подій для приховування незаконних дій, утруднення виявлення порушень та аудиту даних про стан БПЛА	7	8	56		+					+		+		4	8	32
7	Центри зв'язку				Ш	Заглушення каналу зв'язку	Слабке шифрування протоколів комунікацій	Перехоплення та дешифрування каналів комунікацій	Так	Так	Так	Ні	Отримання несанкціонованого доступу до системи зв'язку, можливість маніпулювання даними та нарушення конфіденційності	8	6	48		+	+			+					5	6	30
8							Відсутність контролю доступу	Отримання виского рівня повноважень внутрішнім адміністратором	Ні	Так	Так	Так	Вільний доступ до системи зв'язку, можливість зміни налаштувань, переривання роботи мережі та можливість втрати даних	8	7	56						+	+		+		5	7	35
9	Системи управління БПЛА				Ш	Впровадження шкідливого програмного забезпечення в системи керування БПЛА	Вразливість в програмному забезпеченні БПЛА	Внедрення шкідливого ПЗ через програмну вразливість	Так	Ні	Так	Так	Можливе втручання в роботу серверів управління, порушення працездатності систем та можливість втрати даних	8	8	64			+	+			+		+		4	8	32

Продовження таблиці Ґ.1

1	2	3	4		5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
10		1	8,4	А		Впровадження шкідливого програмного забезпечення в системи керування БПЛА	Неправильна настройка прав доступу до системи управління	Перехоплення ідентифікаторів та паролів для отримання несанкціонованого доступу	Так	Так	Так	Так	Можливе фізичне пошкодження серверів, призведення до втрати даних та перерв у роботі систем управління БПЛА	7	5	35		+	+			+	+				5	5	25
11	Бази даних				Ш	Знищення ідентифікаційних даних БПЛА	Низький рівень доступу до ідентифікаційних даних	Несанкціоноване отримання ідентифікаційних даних	Ні	Так	Так	Так	Можливе втручання в бази даних, їх негайне видалення та неможливість відновлення інформації	9	9	81						+			+	+	6	9	54
12							Відсутність резервного копіювання	Привласнення привілеїв	Так	Так	Так	Ні	Потенційна втрата даних без можливості відновлення через відсутність резервних копій	9	8	72						+	+		+	+	5	8	40
13	Зарядні станції	2	10	А	Ш	Зміна програмного забезпечення процесу зарядки	Відсутність аутентифікації та авторизації змін у програмному забезпеченні	Спуфінг ідентифікаторів або атака методом брутфорсу	Так	Так	Так	Так	Потенційне зібрання та передача конфіденційних даних про зарядку на станції	9	6	54			+			+			+		6	6	36
14							Відсутність моніторингу програмного забезпечення	Невиявлене функціонування шпигунського ПЗ через відсутність моніторингу	Так	Так	Так	Так	Потенційне збирання та трансляція даних без виявлення та блокування	9	7	63				+			+		+		5	7	35
15	Бази даних				Ш	Захоплення сеансу адміністратора	Відсутність механізму шифрування даних	Атака на перехоплення даних в процесі передавання	Ні	Так	Так	Так	Можливе читання та використання конфіденційних даних	6	10	60		+	+				+		+		4	10	40

Продовження таблиці Ґ.1

1	2	3	4		5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
16		2	10	А		Захоплення сеансу адміністратора	Відсутність механізму автентифікації на рівні передавання	Брутфорс або використання стандартних паролів	Так	Так	Так	Так	Потенційна можливість модифікації, видалення або зміни даних	7	9	63			+			+	+		+		7	9	63
17	Хмарні сховища				Ш	Втручання в роботу системи зв'язку	Відсутність системи контролю автентифікації та авторизації	Перехоплення або підміна ідентифікаційних даних	Так	Так	Так	Так	Можливе перехоплення даних або модифікація інформації у хмарних сховищах	8	7	56		+				+	+				6	7	42
18							Відсутність ефективних заходів захисту від розподілених атак	Розподілена атака на доступність сервісів хмарних сховищ	Ні	Так	Так	Так	Можливі перебої у роботі хмарних сховищ, що призведе до обмеження доступу або перерв у роботі	9	7	63	+		+						+		6	7	42
19	Центри зв'язку				Ш	Злам системи управління БПЛА	Відсутність шифрування каналів комунікацій	Перехоплення та зміна команд, аналіз трафіку	Так	Так	Так	Ні	Можливість злому та незаконному контролю над центрами зв'язку, що може призвести до перерв у роботі або маніпулювання системою управління	4	8	32		+	+			+	+				4	8	32
20							Використання слабких паролів у системі управління БПЛА	Брутфорс атака для злому паролів у системі управління	Ні	Так	Так	Так	Несанкціонований доступ до системи управління, що може призвести до втрати контролю над БПЛА або маніпуляції їх функціоналом	4	9	36			+			+					4	9	36

Продовження таблиці Г.1

1	2	3	4		5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
21	Системи управління БПЛА	2	10	А	Ш	Зміна команд і управління БПЛА	Відсутність шифрування каналів комунікацій	Перехоплення та модифікація незашифрованих команд для керування БПЛА	Так	Ні	Так	Так	Можливість зміни маршрутів, функціоналу або навігації БПЛА, що може призвести до непередбачуваних дій та ризиків	6	8	48		+	+			+	+				6	8	48
22							Відсутність відповідної аутентифікації	Злам аутентифікаційних механізмів для отримання несанкціонованого доступу до системи управління БПЛА	Так	Так	Так	Так	Несанкціонований доступ до системи управління, що може викликати контроль над функціоналом та даними БПЛА	7	9	63			+	+		+		+		7	9	63
23	Системи управління БПЛА				Ш	Впровадження шкідливих датчиків	Відсутня перевірка автентичності датчиків	Підміна справжніх датчиків на шкідливі	Ні	Так	Так	Так	Система управління буде отримувати від шкідливих датчиків некоректні або спотворені дані, що може викликати неправильне прийняття рішень	6	7	42					+		+		+		5	7	35
24							Відсутня системи періодичної перевірки та виявлення шкідливих датчиків	Обхід системи виявлення та блокування шкідливих датчиків	Так	Так	Так	Ні	Шкідливі датчики можуть продовжувати функціонувати невиявленими, що дозволяє їм надавати системі управління невірні або контрольовані дані	6	7	42			+	+	+			+		5	7	35

Продовження таблиці Г.1

1	2	3	4		5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
25	Програмне забезпечення БПЛА	3	7,4	В	Ш	Впровадження шкідливого програмного забезпечення в компонент збору відеоданних з БПЛА	Відсутня перевірка автентичності під час завантаження програмного забезпечення	Підробка або зміна програмного забезпечення під час завантаження	Так	Так	Так	Так	Можливість модифікувати або підробити програмне забезпечення, що може призвести до некоректної роботи системи або навіть до її неконтрольованої поведінки	9	6	54				+					+	+	6	6	36
26							Відсутня валідація вхідних даних	Впровадження шкідливого коду через вхідні дані	Так	Так	Так	Так	Використання вхідних даних для впровадження шкідливого коду може призвести до виконання несанкціонованих операцій в системі	9	7	63				+		+				+	7	7	49
27	Системи управління БПЛА				Ш	Впровадження фальшивих команд в управління БПЛА	Відсутність шифрування каналів комунікацій	Перехоплення та модифікація команд	Ні	Так	Так	Так	Інтерцепція та зміна команд може призвести до неправильних дій літального апарату, включаючи його втрату чи використання у несанкціонованих цілях	6	10	60		+				+	+		+		6	10	60
28							Відсутність відповідної аутентифікації	Отримання несанкціонованого доступу до системи	Так	Так	Так	Так	Несанкціонований доступ до системи управління може дозволити зловмисникам здійснювати дії, які можуть загрожувати безпеці та функціонуванню БПЛА	7	9	63			+			+			+		7	9	63

Продовження таблиці Ґ.1

1	2	3	4		5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
29	Канал передачі даних між БПЛА та оперативним центром	3	7,4	В	Ш	Перехоплення та модифікації даних через бездротові канали зв'язку	Використання слабких або стандартних паролів	Брутфорс атака на паролі	Так	Так	Так	Так	Це може призвести до розкриття конфіденційної інформації або зміни команд, що надходять до БПЛА	8	7	56						+			+		7	7	49
30							Відсутність протоколів шифрування данних	Сніфінг та аналіз трафіку	Ні	Так	Так	Так	Ця атака може дозволити несанкціонованим користувачам отримувати доступ до переданих даних між БПЛА та оперативним центром	9	7	63		+	+								9	7	63
31	Датчики, що використовуються в системі				Ш	Впровадження шкідливих датчиків	Слабка політика безпеки та система захищення від фізичного втручання	Маніпулювання фізичною структурою датчиків	Так	Так	Так	Ні	Ця атака може призвести до спотворення інформації, що надходить від датчиків, що вплине на точність та надійність системи управління	4	8	32					+						4	8	32
32							Вразливість у мережевому протоколі датчиків	Впровадження шкідливого програмного забезпечення через мережевий протокол датчиків	Ні	Так	Так	Так	Ця атака може дозволити несанкціонованим особам впроваджувати шкідливі програми в систему через мережеві підключення датчиків, загрожуючи цілісності та безпеці функціонування системи	7	9	63			+	+			+				7	9	63

Продовження таблиці Г.1

1	2	3	4		5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
33	Системи керування та управління віддаленими командами	3	7,4	В	Ш	Віддалене вимкнення БПЛА	Слабка аутентифікація при віддаленому доступі до систем керування	Підміна авторизованих ідентифікаторів для отримання доступу до системи	Так	Ні	Так	Так	Здійснення такої атаки може дозволити зловмиснику отримати доступ до системи керування та нанести шкоду або взяти під контроль віддалене управління БПЛА	8	7	56						+			+		4	7	28
34							Відсутня захищеність протоколів передачі команд	Перехоплення та модифікація команд, що передаються системі управління	Так	Так	Так	Так	Ця атака може призвести до неконтрольованого втручання в роботу системи керування, що може призвести до втрати контролю над БПЛА або навіть втрати даних	7	9	63		+				+	+				7	9	63
35	Сервери та сховища даних				Ш	Злам серверів і сховищ даних	Використання застарілих версій програмного забезпечення на серверах	Атака через використання незапатченого програмного забезпечення	Ні	Так	Так	Так	Зламання серверів може призвести до втрати контролю над цими серверами, можливого крадіжку чутливої інформації та перешкоджання нормальному функціонуванню систем	8	7	56				+				+	+		7	7	49
36							Використання старі протоколи для захисту даних в сховищах	SQL-ін'єкція або атака на сервери та сховища даних	Так	Так	Так	Ні	Ця атака може призвести до крадіжки чутливої інформації або втрати конфіденційності даних, що може вплинути на безпеку, репутацію та відповідність законодавству	9	6	54			+	+		+		+	+		7	6	42

Продовження таблиці Г.1

1	2	3	4		5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
37	Система збору та обробки медіа матеріалу	4	5	С	Ш	Захоплення чи модифікація медіа-матеріалів в процесі передачі з БПЛА	Відсутність відповідної аутентифікації	SQL ін'єкція	Так	Так	Так	Так	Ця атака може дозволити колишнім співробітникам отримати доступ до конфіденційної інформації або навіть змінити або знищити дані, що загрожує конфіденційності та доступності даних	9	9	81			+	+		+			+		6	9	54
38							Невірне збереження медіа-матеріалів	Несанкціоноване копіювання або зміна даних	Так	Так	Так	Так	Несанкціонований доступ до нешифрованих даних може призвести до розголошення чутливої інформації, що загрожує конфіденційності даних та може порушити вимоги щодо захисту конфіденційної інформації	9	8	72		+				+	+				6	8	48
39	Система управління БПЛА				Ш	Віддалений вплив на БПЛА	Відсутній контроль доступу до системи управління БПЛА	Використання несанкціонованого доступу до системи управління БПЛА	Ні	Так	Так	Так	Ця атака може призвести до можливості неправомірного втручання в процеси керування БПЛА, зміни маршрутів польоту або навіть вимкнення засобів безпеки, що загрожує безпеці польоту	6	10	60			+			+			+		7	10	70

Продовження таблиці Ґ.1

1	2	3	4		5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
40	Система управління БПЛА	4	5	С	Ш	Віддалений вплив на БПЛА	Вразливість в програмному забезпеченні системи управління	Використання вразливостей програмного забезпечення для впливу на систему управління БПЛА	Так	Так	Так	Так	Ця атака може спричинити втрату контролю над БПЛА, можливість перехоплення або зміни команд управління, що загрожує безпеці та надійності польоту	7	9	63			+	+					+		7	9	63
41	Засоби зберігання і передачі даних				Ш	Витік конфіденційних даних	Використання застарілих методів шифрування даних	Розшифрування даних через використання застарілих методів шифрування	Так	Так	Так	Так	Ця атака може призвести до витоку конфіденційних даних, порушення конфіденційності та недовіри до системи зберігання	8	7	56		+							+	+		6	7	42
42							Використання старих протоколів для доступу к даним	Отримання несанкціонованого доступу до даних через недостатнє обмеження прав доступу	Ні	Так	Так	Так	Ця атака може спричинити несанкціоноване отримання конфіденційної інформації, порушення конфіденційності та можливість використання цієї інформації проти системи чи організації	9	7	63							+		+	+		7	7	49
43	Фізична безпека, датчики				Ш	Саботаж і фізичний вплив на БПЛА	Слабка політика безпеки та система захищення від фізичного втручання	Фізичне пошкодження або модифікація датчиків	Так	Так	Так	Ні	Ця атака може спричинити недостовірність зібраних даних або взагалі припинення роботи датчиків, що може вплинути на точність збору інформації	4	8	32					+				+	+		5	8	40

Продовження таблиці Г.1

1	2	3	4		5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
44	Фізична безпека, датчики	4	5	С	Ш	Саботаж і фізичний вплив на БПЛА	Вразливість фізичної інфраструктури	Неправомірний доступ до фізичної інфраструктури БПЛА або датчиків	Ні	Так	Так	Так	Ця атака може призвести до неправомірного доступу до системи або фізичних ресурсів, що може бути використане для саботажу, витоку конфіденційної інформації або модифікації системи	7	9	63					+		+				4	9	36
45	Серверні системи, сховища даних				Ш	Перехоплення даних через SQL ін’єкцію	Відсутня сиситема фільтрації введених даних	SQL Ін’єкція для отримання конфіденційних даних	Так	Ні	Так	Так	Несанкціонований доступ може призвести до витоку конфіденційної інформації або втрати цінних даних	8	7	56				+			+		+		7	7	49
46							Слабка система автентифікації та контролю доступу	Імперсонація колишнього співробітника	Так	Так	Так	Так	Злам системи через відомі вразливості може викликати витік конфіденційної інформації або може бути використаний для встановлення шкідливого програмного забезпечення	4	9	36						+	+		+		7	9	63
47	Датчики, обладнання				Ш	Втручання в роботу датчиків і обладнання	Відсутність аутентифікації датчиків та обладнання	Отримання несанкціонованого доступу до датчиків і обладнання	Ні	Так	Так	Так	Несанкціонований доступ може призвести до фальсифікації даних, порушення їх правильної роботи або втрати збережених даних	7	3	21					+	+					4	3	12

Продовження таблиці Ґ.1

1	2	3	4		5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
48	Датчики, обладнання	4	5	С	Ш	Втручання в роботу датчиків і обладнання	Відсутність політики безпеки та контролю доступу	Фізичне втручання або небажані зміни в роботі датчиків та обладнання	Так	Так	Так	Ні	Фізичні втручання можуть викликати пошкодження або зміну роботи датчиків, що може призвести до несправності системи або втрати даних	9	4	36					+			+	+		5	4	20
49	Обладнання та інфраструктура системи флотів БПЛА	5	5	С	П	Землетруси	Відсутність захисту від землетрусів	Пошкодження системи в результаті землетрусу	Ні	Так	Так	Ні	Може призвести до пошкодження чутливого обладнання та інфраструктури, що використовується для управління БПЛА	4	6	24					+					+	4	6	24
50							Відсутність резервного планування та систем для управління наслідками	Фізичні пошкодження серверних систем	Ні	Так	Так	Ні	Затримка у відновленні системи, можливість втрати даних та функціональності через відсутність систем управління наслідками події	5	7	35					+					+	5	7	28
51	Центри зв'язку та об'єкти оперативного контролю				П	Паводки	Відсутність системи захисту центрів зв'язку та об'єктів оперативного контролю від паводків	Затоплення центрів зв'язку та об'єктів оперативного контролю під час паводку	Ні	Так	Так	Ні	Великі збитки через втрату обладнання, неможливість ведення оперативного контролю та зв'язку	3	7	21					+					+	3	7	21
52					П		Відсутність системи регулярного обслуговування та тестування на випадок паводків	Затоплення комунікаційних ліній. Пошкодження систем зберігання	Ні	Так	Так	Ні	Повільне або неефективне відновлення після паводку, великі збитки через втрату часу та можливої додаткової шкоди	2	7	14					+					+	2	7	14

Продовження таблиці Ґ.1

1	2	3	4		5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
53	Частини літального апарату, сенсори, системи виявлення пожеж	5	5	С	П	Туман	Зниження видимості. Низька роздільна здатність оптичних систем	Модифікація або блокування сигналів з датчиків видимості	Ні	Так	Так	Ні	Затримка або неспроможність виявлення пожеж, можливість поширення пожежі до великих розмірів до втручання людей	4	9	36	+		+		+					+	4	9	36
54							Вплив на комунікації. Переривання радіо- та супутникового зв'язку	Перешкоджання сигналів зв'язку	Ні	Так	Так	Ні	Втрата функціональності деяких частин літального апарату, можливість аварійної посадки або втрата БПЛА	3	9	27	+		+		+					+	3	9	27
55	Радіоелектронне обладнання, системи захисту від блискавки				П	Грози та блискавки	Вразливість радіоелектронного обладнання при ударах блискавки	Пошкодження радіоелектронного обладнання під час удару блискавки	Ні	Так	Так	Ні	Втрата функціональності обладнання або його часткове пошкодження, що може вплинути на здатність БПЛА працювати коректно	3	9	27	+				+					+	2	9	18
56							Недолік у системах захисту від блискавки	Несправність систем відводу блискавки, що призводить до прямого удару	Ні	Так	Так	Ні	Пошкодження систем захисту, які призначені захищати радіоелектронне обладнання від блискавки, зменшення захисту та збільшення ймовірності пошкодження обладнання під час грози	4	9	36	+				+						4	9	36
57	Електрична система живлення, системи охолодження				П	Високі температури	Недолік у системах охолодження	Перегрів системи охолодження через екстремальні температури	Ні	Так	Так	Ні	Несправність систем охолодження, що може призвести до перегріву електроніки або систем живлення, тим самим може збільшити ризик відмови чи пошкодження обладнання	5	6	30	+				+					+	4	6	24

Продовження таблиці Ґ.*1*

1	2	3	4		5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
58	Електрична система живлення, системи охолодження	5	5	С	П	Високі температури	Вразливість електричної системи при високих температурах	Перегрів електричної системи через високі температури	Ні	Так	Так	Ні	Збільшення опору в електричних системах, можливість перегріву проводів та їхньої деформації, що може призвести до несправності або відмови системи живлення	4	6	24	+				+					+	4	6	24
59	Системи авіаційної безпеки та аеродинаміка				П	Сильні вітри та урагани	Відсутність адаптивних аеродинамічних систем при сильних вітрах. Непропорційна реакція на зміни обстановки	Втрата керованості. Екстремальні аеродинамічні обтічники	Ні	Так	Так	Ні	Втрата стабільності або складнощі в управлінні, що може призвести до аварійних ситуацій або втрати контролю над апаратом	3	6	18	+				+						3	6	18
60							Вразливість аеродинаміки при ураганах	Маніпуляція аеродинамікою апарату для втрати контролю при ураганах.	Ні	Так	Так	Ні	Потеря контролю над БПЛА через втрату стійкості під час урагану, що може призвести до аварії або втрати апарату	4	7	28	+				+						4	7	28

ДОДАТОК Д. IMECA АНАЛІЗ СБФ БПЛА ПІД ЧАС КОМБІНОВАНИХ АТАК

Таблиця Д.1 – IMECA аналіз системи багатофункційних флотів БПЛА під час комбінованих атак

№	№ за Додаток Ґ	Порушник	Загроза	Вразливості	Тип комбінованої атаки	Атака	Наслідки	Критичність кожної атаки			Критичність 1 метод			Критичність 2 метод			Критичність3 метод
								P	S	R	P	S	R	P	S	R	R
1	1	1,2	Зміна навігаційних даних БПЛА	Використання нешифровані протоколи навігації	Послідов.	Маніпулювання навігаційними даними через атаку "Man-in-the-Middle". GPS-отруєння	Зміни маршрутів та локацій БПЛА може призвести до введення в оману та втрати контролю над апаратом	9	9	81	10	10	100	9	10	90	61,2
2	2			Використання слабких паролів		Брутфорс атака на паролі	Може викликати виток чутливої інформації та неправомірне керування БПЛА	8	6	48							
3	13		Зміна програмного забезпечення процесу зарядки	Відсутність аутентифікації та авторизації змін у програмному забезпеченні		Спуфінг ідентифікаторів або атака методом брутфорсу	Може призвести до введення в обман системи автентифікації, порушуючи ідентифікацію користувачів та забезпечення доступу для несанкціонованих осіб	9	6	54							
4	14			Відсутність моніторингу програмного забезпечення		Невиявлене функціонування шпигунського ПЗ через відсутність моніторингу	Може призвести до стеження та збору конфіденційної інформації без відома власників системи	9	7	63							
5	15		Захоплення сеансу адміністратора	Відсутність механізму шифрування даних		Атака на перехоплення даних в процесі передавання	Може викликати виток конфіденційної інформації та втрату цілісності даних	6	10	60							

Продовження таблиці Д.1

№	№ за Додаток Ґ	Порушник	Загроза	Вразливості	Тип комбінованої атаки	Атака	Наслідки	Критичність кожної атаки			Критичність 1 метод			Критичність 2 метод			Критичність3 метод
								P	S	R	P	S	R	P	S	R	R
6	1	1,3	Зміна навігаційних даних БПЛА	Використання нешифровані протоколи навігації	Послідов.	Маніпулювання навігаційними даними через атаку "Man-in-the-Middle". GPS-отруєння	Може викликати серйозні проблеми в управлінні та навігації, наприклад, вибір неправильного маршруту чи введення в оману щодо точності координат	9	9	81	10	9	90	9	9	81	57,8
7	3		Віддалене вимкнення БПЛА	Відсутність або слабка сегментація мережі		Отримання несанкціонованого доступу внутрішнім користувачем	Може призвести до неправомірного доступу до обмежених ресурсів та навіть зміни конфігурації системи, що вплине на її нормальне функціонування	7	7	49							
8	24		Впровадження шкідливих датчиків	Відсутня системи періодичної перевірки та виявлення шкідливих датчиків		Обхід системи виявлення та блокування шкідливих датчиків	Створює можливість для невиявленого функціонування шкідливого програмного забезпечення та сприяє подальшим етапам атаки	6	7	42							
9	25		Впровадження шкідливого програмного забезпечення в компонент збору відеоданних з БПЛА	Відсутня перевірка автентичності під час завантаження програмного забезпечення		Підробка або зміна програмного забезпечення під час завантаження	Можуть призвести до серйозних порушень цілісності та безпеки системи, оскільки дозволяють втручання в програмне забезпечення та використання вразливостей для запуску шкідливого коду	9	6	54							
10	26			Відсутня валідація вхідних даних		Впровадження шкідливого коду через вхідні дані		9	7	63							

Продовження таблиці Д.1

№	№ за Додаток Ґ	Порушник	Загроза	Вразливості	Тип комбінованої атаки	Атака	Наслідки	Критичність кожної атаки			Критичність 1 метод			Критичність 2 метод			Критичність3 метод
								P	S	R	P	S	R	P	S	R	R
11	1	1,4	Зміна навігаційних даних БПЛА	Використання нешифровані протоколи навігації	Послідов.	Маніпулювання навігаційними даними через атаку "Man-in-the-Middle". GPS-отруєння	Може виникнути порушення точності та достовірності інформації, що може призвести до помилок в навігації та керуванні БПЛА, а також можливих аварій	9	9	81	10	10	100	9	10	90	70,0
12	4		Віддалене вимкнення БПЛА	Несанкціонований доступ до системи через слабку аутентифікацію		Використання аутентифікаційних вразливостей	Може призвести до незаконного доступу та маніпулювання критичними системними параметрами	8	7	56							
13	37		Захоплення чи модифікація медіа-матеріалів в процесі передачі з БПЛА	Відсутність відповідної аутентифікації		SQL ін'єкція	Може викликати порушення цілісності бази даних, що в свою чергу може вплинути на нормальне функціонування системи	9	9	81							
14	38			Невірне збереження медіа-матеріалів		Несанкціоноване копіювання або зміна даних	Може порушити конфіденційність та викликати викрадення важливої інформації	9	8	72							
15	39		Віддалений вплив на БПЛА	Відсутній контроль доступу до системи управління БПЛА		Використання несанкціонованого доступу до системи управління БПЛА	Може дозволити атакуючому виконувати команди та отримувати конфіденційну інформацію	6	10	60							

Загалом, об'єднання цих атак може призвести до втрати контролю над безпілотним літальним апаратом, розголошення конфіденційної інформації, а також може мати серйозні наслідки для військової, комерційної чи громадської безпеки.

Продовження таблиці Д.1

№	№ за Додаток Ґ	Порушник	Загроза	Вразливості	Тип комбінованої атаки	Атака	Наслідки	Критичність кожної атаки			Критичність 1 метод			Критичність 2 метод			Критичність3 метод
								P	S	R	P	S	R	P	S	R	R
16	13	1,2	Зміна програмного забезпечення процесу зарядки	Відсутність аутентифікації та авторизації змін у програмному забезпеченні	Парарлел.	Спуфінг ідентифікаторів або атака методом брутфорсу	Можливе перехоплення індивідуальних облікових записів, в тому числі конфіденційних інформаційних даних.	9	6	54	9,9	7	69	9	7	63	63
17	14			Відсутність моніторингу програмного забезпечення		Невиявлене функціонування шпигунського ПЗ через відсутність моніторингу	Може призвести до довготривалого збору та витоку конфіденційних даних без відома власника системи	9	7	63							
18	24	1,3	Впровадження шкідливих датчиків	Відсутня системи періодичної перевірки та виявлення шкідливих датчиків	Парарлел.	Обхід системи виявлення та блокування шкідливих датчиків	Може призвести до введення шкідливих компонентів у систему, не сприйнятих або неперехоплених існуючими засобами виявлення	6	7	42	9,6	7	67	9	7	63	54
19	25		Впровадження шкідливого програмного забезпечення в компонент збору відеоданних з БПЛА	Відсутня перевірка автентичності під час завантаження програмного забезпечення		Підробка або зміна програмного забезпечення під час завантаження	Може вивести з системи засоби перевірки автентичності програм та завдати шкоди їхній інтегрітету	9	6	54							

Зловмисники можуть отримати непомічений доступ, змінити чи використовувати програми від імені автентичних джерел, що призводить до збитку важливих даних та операцій системи. Такі атаки також можуть викликати велику шкоду репутації та витрати на відновлення системи.

Продовження таблиці Д.1

№	№ за Додаток Ґ	Порушник	Загроза	Вразливості	Тип комбінованої атаки	Атака	Наслідки	Критичність кожної атаки			Критичність 1 метод			Критичність 2 метод			Критичність3 метод
								P	S	R	P	S	R	P	S	R	R
20	36	1,4	Злам серверів і сховищ даних	Використання старі протоколи для захисту даних в сховищах	Парарлел.	Атака на сервери та сховища даних	Зловмисники можуть здійснювати несанкціоновані операції, видаляти, змінювати чи вивчати конфіденційні дані, що загрожує конфіденційності та цілісності інформації.	9	6	54	9,9	9	89	9	9	81	81
21	37		Захоплення чи модифікація медіа-матеріалів в процесі передачі з БПЛА	Відсутність відповідної аутентифікації		SQL ін'єкція	Може викликати пошкодження чи втрату даних у базі, а також недостачу доступу до критично важливих функціональностей. Зловмисники можуть зловживати структурою запитів SQL, отримуючи непередбачені результати та наносячи шкоду системі.	9	9	81							

ДОДАТОК Е. КОД ЗАСТОСУНКУ

Код класу MainWindow:

```
using Syncfusion.UI.Xaml.Grid;
using System.Collections.Generic;
using System.Windows;
using UAVSecurity.Models;
using Syncfusion.UI.Xaml.Grid.Helpers;
using UAVSecurity.Views;
using UAVSecurity.Renderer;
using Syncfusion.Data;
using UAVSecurity.Windows;

namespace UAVSecurity
{
    /// <summary>
    /// Interaction logic for MainWindow.xaml
    /// </summary>
    public partial class MainWindow : Window
    {
        GridRowSizingOptions gridRowResizingOptions = new GridRowSizingOptions();

        List<FullTableModel> data = new List<FullTableModel>();
        List<Offender> offenders= new List<Offender>();

        IPropertyAccessProvider reflector = null;

        double autoHeight;
        public MainWindow()
        {
            InitializeComponent();

            TablesList.ItemsSource = new string[] { "Таблиця IMECA", "Таблиця порушників" };
            if (TablesList.Items.Count !=0)
            {
                TablesList.SelectedItem = TablesList.Items[0];
            }

            CurrentTable.ItemsSource = data;
            CurrentTable.AllowEditing= true;

            CurrentTable.AllowSorting= false;
            CurrentTable.AllowFiltering= false;
            CurrentTable.ColumnSizer = GridLengthUnitType.Auto;

            this.CurrentTable.AutoGeneratingColumn += dataGrid_AutoGeneratingColumn;
            this.CurrentTable.QueryRowHeight += dataGrid_QueryRowHeight;
            this.CurrentTable.CurrentCellEndEdit += dataGrid_CurrentCellEndEdit;
            this.CurrentTable.ItemsSourceChanged += dataGrid_ItemsSourceChanged;
            this.CurrentTable.QueryCoveredRange += dataGrid_QueryCoveredRange;

            this.CurrentTable.CellRenderers.Remove("StackedHeader");

            this.CurrentTable.CellRenderers.Add("StackedHeader", new GridCustomStackedRenderer());

            this.CurrentTable.CellRenderers.Remove("ComboBox");
            this.CurrentTable.CellRenderers.Add("ComboBox", new GridCellComboBoxRendererExt());

            Offender.GetDefaultOffendersList(offenders);
            FullTable.SetFullTableDefaultView(data, offenders);
        }

        private void View_RecordPropertyChanged(object sender, System.ComponentModel.PropertyChangedEventArgs e)
```

```
{
    for (int i = 0; i < data.Count; i++)
    {
        data[i].Number = i + 1;
    }
    CurrentTable.View.Refresh();

    if (e.PropertyName == "Offender")
    {
        SortRecords();
    }
}
private void View_CollectionChanged(object sender, System.Collections.Specialized.NotifyCollectionChangedEventArgs e)
{
}
void dataGrid_CurrentCellEndEdit(object sender, CurrentCellEndEditEventArgs args)
{
    CurrentTable.InvalidateRowHeight(args.RowColumnIndex.RowIndex);
    CurrentTable.GetVisualContainer().InvalidateMeasureInfo();
}
void dataGrid_ItemsSourceChanged(object sender, GridItemsSourceChangedEventArgs e)
{
    if (CurrentTable.View != null)
        reflector = CurrentTable.View.GetPropertyAccessProvider();
    else
        reflector = null;
    this.CurrentTable.View.RecordPropertyChanged += View_RecordPropertyChanged;
}
void dataGrid_AutoGeneratingColumn(object sender, AutoGeneratingColumnArgs e)
{
    if (e.Column.MappingName == "OffenderNumber")
    {
        e.Column.IsReadOnly= true;
        e.Column.MaximumWidth = 80;
        e.Column.TextAlignment= TextAlignment.Center;
        return;
    }
    if (e.Column.MappingName == "OffenderPotentialNum")
    {
        e.Column = new GridComboBoxColumn()
        {
            TextAlignment = TextAlignment.Center,
            HeaderText = e.Column.HeaderText,
            ValueBinding = e.Column.ValueBinding,
            MappingName = e.Column.MappingName,
            MinimumWidth = 35,
            MaximumWidth = 80,
            ItemsSource = new int[] { 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 }
        };
        return; }
    if (e.Column.MappingName == "OffenderCategory")
    {
        e.Column = new GridComboBoxColumn()
        {
            TextAlignment = TextAlignment.Center,
            HeaderText = e.Column.HeaderText,
            ValueBinding = e.Column.ValueBinding,
            MappingName = e.Column.MappingName,
            MinimumWidth = 35,
            MaximumWidth = 80,
            ItemsSource = new string[] { "A","B","C" }
        };
        return;
    }
    if (e.Column.MappingName == "OffenderPotentialNumber")
    {
```

```
    e.Column = new GridNumericColumn()
    {
        TextAlignment = TextAlignment.Center,
        HeaderText = e.Column.HeaderText,
        ValueBinding = e.Column.ValueBinding,
        MappingName = e.Column.MappingName,
        MaximumWidth = 50,
        IsReadOnly = true,
        AllowEditing = false
    };
    return; }
if (e.Column.MappingName == "OffenderPotentialCategory")
{
    e.Column = new GridTextColumn()
    {
        TextAlignment = TextAlignment.Center,
        HeaderText = e.Column.HeaderText,
        ValueBinding = e.Column.ValueBinding,
        MappingName = e.Column.MappingName,
        MaximumWidth = 50,
        IsReadOnly = true,
        AllowEditing =false
    };
    return; }
if (e.Column.MappingName == "ThreadCharacteristic")
{
    e.Column = new GridComboBoxColumn()
    {
        TextAlignment = TextAlignment.Center,
        HeaderText = e.Column.HeaderText,
        ValueBinding = e.Column.ValueBinding,
        MappingName = e.Column.MappingName,
        MaximumWidth = 70,
        ItemsSource = new string[] { "Ш","П" }
    };
    return; }
if (e.Column.MappingName == "Criticality_S" || e.Column.MappingName == "Criticality_P")
{
    e.Column = new GridComboBoxColumn()
    {
        TextAlignment = TextAlignment.Center,
        HeaderText = e.Column.HeaderText,
        ValueBinding = e.Column.ValueBinding,
        MappingName = e.Column.MappingName,
        MinimumWidth = 35,              MaximumWidth = 70,
        ItemsSource = new int[] { 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 }
    };
    return; }
if (e.Column.MappingName == "Criticality_R")
{
    e.Column = new GridNumericColumn()
    {
        TextWrapping = TextWrapping.Wrap,
        TextAlignment = TextAlignment.Center,
        ValueBinding = e.Column.ValueBinding,
        MappingName = e.Column.MappingName,
        HeaderText = e.Column.HeaderText,
        MaximumWidth = 70,
        MinimumWidth = 35,
        IsReadOnly = true,
    };
    return; }
if (e.Column.MappingName == "Offender")
{
    e.Column = new GridComboBoxColumn()
    {
```

```
            TextAlignment = TextAlignment.Center,
            HeaderText = e.Column.HeaderText,
            ValueBinding = e.Column.ValueBinding,
            MappingName = e.Column.MappingName,
            MinimumWidth = 35,
            MaximumWidth = 70,
            ItemsSource = new int[] { 1, 2, 3, 4, 5 }
        }; }
    if (e.Column is GridTextColumn)
    {
        e.Column = new GridTextColumn()
        {
            TextWrapping = TextWrapping.Wrap,
            TextAlignment = TextAlignment.Center,
            ValueBinding = e.Column.ValueBinding,
            MappingName = e.Column.MappingName,
            HeaderText = e.Column.HeaderText,
            MaximumWidth = 150,
            MinimumWidth = 15,
        }; }
    if (e.Column is GridNumericColumn)
    {
        e.Column = new GridNumericColumn()
        {
            TextAlignment= TextAlignment.Center,
            TextWrapping = TextWrapping.Wrap,
            ValueBinding = e.Column.ValueBinding,
            MappingName = e.Column.MappingName,
            HeaderText = e.Column.HeaderText,
            MaximumWidth = 150,
            MinimumWidth = 30,
        }; } }
void dataGrid_QueryRowHeight(object sender, QueryRowHeightEventArgs e)
{
    if (this.CurrentTable.GridColumnSizer.GetAutoRowHeight(e.RowIndex, gridRowResizingOptions, out autoHeight))
    {
        if (autoHeight > 24)
        {
            e.Height = autoHeight;
            e.Handled = true;
        }
    }
    if (this.CurrentTable.GetHeaderIndex() == e.RowIndex)
    {
        if (this.CurrentTable.GridColumnSizer.GetAutoRowHeight(e.RowIndex, gridRowResizingOptions, out autoHeight))
        {
            if (autoHeight > 24)
            {
                e.Height = autoHeight;
                e.Handled = true;
            } } }
}
void dataGrid_QueryCoveredRange(object sender, GridQueryCoveredRangeEventArgs e)
{
    var range = GetRange(e.GridColumn, e.RowColumnIndex.RowIndex, e.RowColumnIndex.ColumnIndex, e.Record);

    if (range == null)
        return;
    // You can know that the range is already exist in Covered Cells by IsInRange method.
    foreach (CoveredCellInfo c in range)
    {
        if (!CurrentTable.CoveredCells.IsInRange(c))
        {
            e.Range = c;
            e.Handled = true;
        }
```

```
        }
        //If the calculated range is already exist in CoveredCells, you can get the range using SfDataGrid.GetConflictRange
(CoveredCellInfo coveredCellInfo) extension method.
    }

    private List<CoveredCellInfo> GetRange(GridColumn column, int rowIndex, int columnIndex, object rowData)
    {
        var range = new CoveredCellInfo(columnIndex, columnIndex, rowIndex, rowIndex);
        object data1 = reflector.GetFormattedValue(rowData, column.MappingName);
        // total rows count.
        int recordsCount = this.CurrentTable.GroupColumnDescriptions.Count != 0 ?
        (this.CurrentTable.View.TopLevelGroup.DisplayElements.Count + this.CurrentTable.TableSummaryRows.Count +
this.CurrentTable.UnBoundRows.Count + (this.CurrentTable.AddNewRowPosition == AddNewRowPosition.Top ? +1 : 0)) :
        (this.CurrentTable.View.Records.Count + this.CurrentTable.TableSummaryRows.Count +
this.CurrentTable.UnBoundRows.Count + (this.CurrentTable.AddNewRowPosition == AddNewRowPosition.Top ? +1 : 0));

        if (!(column.MappingName == "Element" || column.MappingName == "Offender" || column.MappingName ==
"OffenderPotentialNumber" || column.MappingName == "OffenderPotentialCategory" || column.MappingName ==
"ThreadName"))
        {
            return null;
        }
        // Merge Vertically from the row index.
        int previousRowIndex = -1;
        int nextRowIndex = -1;
        // Get previous row data.
        var startIndex = CurrentTable.ResolveStartIndexBasedOnPosition();
        for (int i = rowIndex-1; i >= startIndex; i--)
        {
            var previousData = this.CurrentTable.GetRecordEntryAtRowIndex(i);
            if (previousData == null || !previousData.IsRecords)
                break;
            var compareData = reflector.GetFormattedValue((previousData as RecordEntry).Data, column.MappingName);
            if (compareData == null)
                break;
            if (!compareData.Equals(data1))
                break;
            previousRowIndex = i;
        }
        // get next row data.
        for (int i = rowIndex + 1; i <= recordsCount + 1; i++)
        {
            var nextData = this.CurrentTable.GetRecordEntryAtRowIndex(i);

            if (nextData == null || !nextData.IsRecords)
                break;
            var compareData = reflector.GetFormattedValue((nextData as RecordEntry).Data, column.MappingName);
            if (compareData == null)
                break;
            if (!compareData.Equals(data1))
                break;
            nextRowIndex = i;
        }
        if (previousRowIndex != -1 || nextRowIndex != -1)
        {
            if (previousRowIndex != -1)
                range = new CoveredCellInfo(range.Left, range.Right, previousRowIndex, range.Bottom);
            if (nextRowIndex != -1)
                range = new CoveredCellInfo(range.Left, range.Right, range.Top, nextRowIndex);
            return new List<CoveredCellInfo>() { range};
        }
        return null;
    }
    void SortRecords()
    {
        data.Sort((x, y) =>x.Offender.CompareTo(y.Offender));
```

```
    }
    private void CurrentTable_Loaded(object sender, RoutedEventArgs e)
    {
        this.SizeToContent = SizeToContent.Width;
        this.CurrentTable.View.RecordPropertyChanged += View_RecordPropertyChanged;
        this.CurrentTable.View.CollectionChanged += View_CollectionChanged;
    }
    private void TablesList_SelectionChanged(object sender, System.Windows.Controls.SelectionChangedEventArgs e)
    {
        if (TablesList.SelectedItem.ToString() == "Таблиця IMECA")
        {
            CurrentTable.ItemsSource = data;
            foreach (FullTableModel f in data)
            {
                f.Offender = f.Offender;
            }
            FormCriticalityMatrixButton.IsEnabled = true;
            //this.CurrentTable.View.RecordPropertyChanged += View_RecordPropertyChanged;
        }
        if (TablesList.SelectedItem.ToString() == "Таблиця порушників")
        {
            CurrentTable.ItemsSource = offenders;
            FormCriticalityMatrixButton.IsEnabled= false;
            //this.CurrentTable.View.RecordPropertyChanged += View_RecordPropertyChanged;
        }
    }
    private void FormCriticalityMatrixButton_Click(object sender, RoutedEventArgs e)
    {
        var matrix = new CriticalityMatrix(data);
        matrix.Show();
    }
  }
}
```

ДОДАТОК Є. АКТИ ВПРОВАДЖЕННЯ

Затверджую
Проректор з науково-педагогічної роботи
Національного аерокосмічного університету
ім. М.Є. Жуковського
«Харківський авіаційний інститут»
к.т.н., доцент
_____ Андрій ГУМЕННИЙ
« 15 » 05 2024 року

АКТ ВПРОВАДЖЕННЯ

наукових результатів дисертаційної роботи
Землянко Георгія Андрійовича, виконаної на здобуття наукового ступеня доктора філософії, у навчальному процесі кафедри комп'ютерних систем, мереж і кібербезпеки

Комісія у складі: голови комісії - декана факультету радіоелектроніки, комп'ютерних систем та інфокомунікацій к.т.н. Олексія Одокієнка, і членів - професора кафедри комп'ютерних систем, мереж і кібербезпеки, к.т.н. Клайда Фурманова, професора кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н. Володимира Пєвнєва, доцента кафедри комп'ютерних систем, мереж і кібербезпеки, к.т.н. Ігоря Клюшнікова встановила, що наукові результати, а саме:

– метод (IMECA) аналізу кіберзагроз, наслідків та критичності атак на активи кіберфізичної системи багатофункційних флотів безпілотних літальних апаратів;

– метод вибору контрзаходів для забезпечення кібербезпеки кіберфізичної системи багатофункційних флотів безпілотних літальних апаратів;

реалізовані у навчальному процесі кафедри комп'ютерних систем, мереж і кібербезпеки у вигляді:

- лекційного матеріалу і практичних занять з використання інструментальних засобів та методів при розробленні, аналізі та оцінці кібербезпеки кіберфізичних систем, зокрема, системи багатофункційних флотів безпілотних апаратів, ризик-орієнтованого оцінювання та вибору контрзаходів для забезпечення безпеки відповідно до вимог у навчальних дисциплінах «Надійність та функціональна безпека інформаційно-керуючих систем» (6 годин), «Програмування систем IoT» (4 години), «Захист інформації в інформаційно-комунікаційних системах» (4 години), «Комплексні системи захисту інформації: проектування, впровадження, супровід» (4 години).

Це дозволило покращити фундаментальність викладання матеріалу з кібербезпеки сучасних технологій, а саме, мобільних систем, інтернету речей, літаючих сенсорних мереж, наочність та практичну спрямованість навчального процесу, якість підготовки фахівців за напрямами комп'ютерних інженерії, кібербезпеки та захисту інформації.

Голова комісії Олексій ОДОКІЄНКО

Члени комісії Клайд ФУРМАНОВ

Володимир ПЄВНЄВ

Ігорь КЛЮШНІКОВ

Затверджую
Проректор з наукової роботи
Національного аерокосмічного університету
ім. М.Є. Жуковського
«Харківський авіаційний інститут»
д.т.н., професор
_____ Володимир ПАВЛІКОВ
«11» _____ 2024 року

АКТ ВПРОВАДЖЕННЯ

наукових результатів дисертаційної роботи Землянко Георгія Андрійовича, виконаної на здобуття наукового ступеня доктора філософії, у науково-дослідних проєктах Національного аерокосмічного університету ім. М. Є. Жуковського «ХАІ»

Комісія у складі: голови – декана факультету радіоелектроніки, комп'ютерних систем та інфокомунікацій к.т.н. Олексія Одокієнка і членів – професора кафедри комп'ютерних систем, мереж і кібербезпеки д.т.н., професора Герман Фесенка, д.т.н., професора кафедри компютерних систем, мереж і кібербезпеки професора Ольги Морозової, доцента кафедри компютерних систем, мереж і кібербезпеки к.т.н., с.н.с. Ігоря Клюшнікова, встановила, що наукові результати, а саме:

– модель кіберфізичної системи багатофункційних флотів безпілотних апаратів, як об'єкта оцінювання кібербезпеки;

– метод (IMECA) аналізу кіберзагроз, наслідків та критичності атак на активи кіберфізичної системи багатофункційних флотів безпілотних літальних апаратів;

– модель комбінованих послідовно-паралельних кібератак різними порушниками і засобами;

– метод вибору контрзаходів для забезпечення кібербезпеки кіберфізичної системи багатофункційних флотів безпілотних літальних апаратів;

реалізовані у вигляді наукових положень і розробок, використаних при виконанні науково-дослідних проєктів за замовленням Міністерства освіти та науки України:

– Наукові засади і методи забезпечення гарантоздатності флотів БПЛА інтелектуальних систем моніторингу потенційно небезпечних і військових об'єктів (Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», ДР № 0121U112172, 2021-2023);

– Методи, моделі та інформаційні технології підвищення надійності та безпечності складних ІТ-систем на етапах розроблення та впровадження (Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», ДР № 0121U113842, 2021-2023);

– Методи, програмно-апаратні засоби та інформаційні технології розроблення і модернізації гарантоздатних комп'ютерних систем, мереж та ІТ-інфраструктур (Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», ДР № 0117U05349, 2018-2020);

– Методологія сталого розвитку та інформаційні технології зеленого комп'ютингу та комунікацій (Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», ДР № 0118U003822, 2018-2020),

а також у міжнародному проєкті:

– Internet of Things: Emerging Curriculum for Industry and Human Applications (ALIOT, №573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP) впродовж 2016-2019 рр., за програмою ЄС ERASMUS +.

Це дозволило підвищити показники кібербезпеки та точності оцінювання кіберризиків для безпілотних мобільних і стаціонарних систем та критичних інфраструктур, які досліджувалися в рамках виконання НДР впродовж 2018-2023 рр.

Голова комісії Олексій ОДОКІЄНКО

Члени комісії Герман ФЕСЕНКО

Ольга МОРОЗОВА

Ігорь КЛЮШНІКОВ

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «СІДІ ЛІНК»

61166, м. Харків
вул. Серпова, 4
р/р UA143515330000026000052147747
в ХГРУ АТ КБ "ПРИВАТБАНК»
МФО 339500
Код ЄДРПОУ 37575641
ІПН 375756420301
cdlink1977@gmail.com
тел. +38(050)-915-24-32

ЗАТВЕРДЖУЮ
Директор ТОВ «СІДІ ЛІНК»
Дмитро КОЧКАР
«29» березня 2024 р.

АКТ ВПРОВАДЖЕННЯ

наукових результатів дисертаційної роботи
Землянка Георгія Андрійовича,
виконаної на здобуття наукового ступеня доктора філософії,
у ТОВ «СІДІ ЛІНК»

Комісія у складі Голови комісії – Генерального директора Дмитра КОЧКАРЯ та членів комісії – фінансового директора Юлії КОЧКАР, бухгалтера Галини ГОЛОВИНОЇ склала цей акт про те, що наукові результати, а саме:

- метод IMECA-аналізу кіберзагроз, наслідків та критичності атак на системи багатофункційних флотів безпілотних літальних апаратів;
- метод вибору контрзаходів для забезпечення кібербезпеки кіберфізичної системи багатофункційних флотів безпілотних літальних апаратів,

впроваджені в ТОВ «СІДІ ЛІНК».

Зазначені результати було використано під час розроблення проєктів комп'ютерних мереж і мобільних систем різного призначення, зокрема, для аналізу вимог до кібербезпеки та її оцінювання для варіантів можливих рішень.

Голова комісії: Дмитро КОЧКАР

Члени комісії: Юлія КОЧКАР

Галина ГОЛОВИНА