https://doi.org/10.31891/2219-9365-2023-76-30
УДК 004.056.5:623.746.5:519.876.5

ЗЕМЛЯНКО Георгій
Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут»
https://orcid.org/0000-0003-4153-7608
g.zemlynko@csn.khai.edu
ХАРЧЕНКО Вячеслав
Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут»
https://orcid.org/0000-0001-5352-077X
v.kharchenko@csn.khai.edu

# ІМЕСА-АНАЛІЗ КІБЕРБЕЗПЕКИ СИСТЕМ БАГАТОФУНКЦІОНАЛЬНИХ ФЛОТІВ БПЛА ПРИ КОМБІНОВАНИХ АТАКАХ: БАЗОВІ МОДЕЛІ ТА ВИБІР КОНТРЗАХОДІВ

*У статті аналізуються особливості ризик-орієнтованого оцінювання кібербезпеки систем багатофункціональних флотів безпілотних літальних апаратів (СБФ БПЛА) в умовах комбінованих кібератак. Запропоновано базові моделі послідовних, паралельних та послідовно-паралельних комбінованих атак. Для оцінювання використано модифікований метод IMECA, який дозволяє визначати критичність кіберзагроз та атак на вразливості для систем СБФ БПЛА. Описано різні варіанти оцінки складових критичності – ймовірності та тяжкості при комбінованих атаках залежно від їх значень для окремих атак.*

*Представлено результати оцінювання кібербезпеки з використанням різних методів визначення критичності для системи СБФ БПЛА у випадку атак на навігаційні дані, систему управління та інші ключові компоненти. Проаналізовано підходи та приклади вибору та застосування контрзаходів для підвищення рівня захисту системи від потенційних загроз. Наголошено на збалансованому виборі контрзаходів за показниками якості (рівня впливу на ризики) та вартості їхнього впровадження для забезпечення безпеки СБФ БПЛА. Подальші дослідження спрямовано на деталізацію моделей і методик оцінювання безпеки при різних комбінаціях кібератак і атак засобами РЕБ.*

*Ключові слова: систем багатофункціональних флотів БПЛА, кібербезпека, комбіновані атаки, моделі послідовних та паралельних атак, IMECA аналіз, критичність, вибір контрзаходів.*

ZEMLIANKO Heorhii, KHARCHENKO Vyacheslav
National Aerospace University “Kharkiv Aviation Institute”, Kharkiv, Ukraine

# IMECA ANALYSIS OF CYBERSECURITY FOR MULTI-FUNCTIONAL UAV FLEETS UNDER COMBINED ATTACKS: BASIC MODELS AND COUNTERMEASURE CHOICE

*The article explores the specifics of risk-oriented cybersecurity assessment for multi-functional fleets of unmanned aerial vehicles (UAVs) under conditions of combined cyberattacks. Basic models of sequential, parallel, and sequential-parallel combined attacks are proposed. The modified IMECA method is utilized for assessment, enabling the determination of cyberthreat and attack criticality on vulnerabilities for UAV fleet systems. Various approaches and examples of selecting and implementing countermeasures to enhance system protection against potential threats are described. Emphasis is placed on a balanced choice of countermeasures based on quality indicators (impact on risks) and the cost of implementation to ensure the security of UAV fleet systems. Further research is directed towards refining models and methodologies for security assessment under various combinations of cyberattacks and attacks by electronic warfare means.*

*Keywords: multi-functional UAV fleets, cybersecurity, combined attacks, sequential and parallel attack models, IMECA analysis, criticality, countermeasure choice.*

## Постановка проблеми у загальному вигляді та її зв’язок із важливими науковими чи практичними завданнями

У контексті використання безпілотних літальних апаратів (БПЛА) для моніторингу критичної інфраструктури, таких як критична інформаційна інфраструктура (КІ) [1], наблюдається тенденція до розвитку складних кіберфізичних систем, зокрема систем багатофункційних флотів (СБФ) БПЛА [2]. Збільшення інтенсивності атак на фізичні та кіберактиви окремих БПЛА і СБФ БПЛА (з використанням засобів радіоелектронної боротьби) [3] актуалізує завдання аналізу та оцінювання показників кібербезпеки цих систем. Його складність зумовлена багатокомпонентністю, розподіленістю та динамічним характером таких систем. В свою чергу, це ускладнює процес забезпечення їхньої безпеки.

Додаткові труднощі розв’язання задач оцінювання кібербезпеки таких кіберфізичних систем як СБФ БПЛА обумовлені розширенням номенклатури атак та можливої взаємодії потенційних порушників. Це вимагає глибокого аналізу існуючого інструментарію для оцінки загроз та ризиків, пов'язаних з успішними кібератаками, особливо при їх комбінуванні у часі, просторі, за природою (інформаційною або радіоелектронною) та засобами, що використовуються, а також типами активів, що є об’єктами атак (кібератак і фізичних впливів).

**Аналіз досліджень та публікацій**

Під СБФ БПЛА [4] будемо розуміти системи багатофункціональних флотів безпілотних літальних апаратів. Кіберактиви для атак включають різноманітні загрози, такі як нешифровані протоколи навігації, слабкі паролі, атаки на систему керування, маніпуляції з програмним забезпеченням та фізична безпека та інше.

Аналіз статей у сфері кібербезпеки СБФ БПЛА виявив проблеми, пов'язані із забезпеченням резильєнтності управління в умовах кібератак [5]. В [6] розглянуто аспекти забезпечення кібербезпеки під час використання БПЛА у сучасних містах в мирний і воєнний час. Важливим є необхідність розробки стійких методів навчання для інтелектуальних систем БПЛА з урахуванням атак на їх окремі компоненти [7]. Аналіз ризиків у кіберпросторі для систем багатофункціональних флотів БПЛА надано у [4], де запропоновано концептуальну модель та метод аналізу на основі відомої техніки Intrusion Modes and Effects Criticality Analysis (IMECA) [3] для аналізу кібербезпеки і управління ризиками.

На основі аналізу публікацій робимо висновок про те, що аналіз кібербезпеки виконується з огляду одиничних атак і впливів, тому актуальним є вдосконалення науково-методичного апарату оцінки та забезпечення кібербезпеки СБФ БПЛА в умовах комбінованих кібератак.

**Формулювання цілей статті**

Метою статті є розроблення моделей комбінованих кібератак (ККА) та ризик-орієнтованого методу оцінювання та вибору контрзаходів для забезпечення кібербезпеки СБФ БПЛА в умовах ККА з використанням процедур IMECA-аналізу. Завданнями дослідження є:

- розроблення базових моделей послідовних, паралельних та послідовно-паралельних ККА для подальшого аналізу критичності їх наслідків для СБФ БПЛА;
- аналіз варіантів і порівняння результатів оцінювання ризиків кібербезпеки при здійсненні ККА на СБФ БПЛА;
- визначення особливостей вибору контрзаходів для забезпечення прийнятних ризиків кібербезпеки СБФ БПЛА при здійсненні ККА.

**Модель оцінювання ризиків комбінованих атак**

Визначимо множину типів комбінованих кібератак. 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.

Для математичного представлення комбінованих атак введемо наступні позначення: $A_i$, $A_j$ - атаку виду i та j, $C_x$ - компонента x системи, t – час (використовуємо дискретний час).

Математичне представлення комбінованих атак:

1. Послідовні атаки:

$$A_{comb1}(C_x)=\{A_i(t, C_x), A_j(t+1, C_x)\}, \quad (1)$$

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, намагаючись уникнути виявлення та реагування. Рисунок 1 надає графічне представлення цієї моделі, де $Crit_{comb1}(A_i \rightarrow C_x, A_j \rightarrow C_x)$ – підсумкова критичність комбінованої атаки.

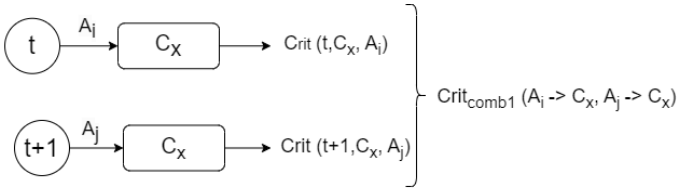


**Рис. 1. Послідовні комбіновані атаки на СБФ БПЛА**

2. Паралельні атаки:

$$A_{comb2}(C_x, C_y)=\{A_i(t, C_x), A_j(t, C_y)\}, \quad (2)$$

де $A_i$ представляє атаку, що відбувається в момент часу t на компонент $C_x$, тоді як $A_j$ виконується в той же момент часу, впливаючи на компонент $C_y$. Модель описує можливість одночасної реалізації атак на різні частини системи, що створює додаткові виклики для виявлення та ефективного реагування (рисунок 2 надає графічне представлення цієї моделі, де $Crit_{comb2}(A_i \rightarrow C_x, A_j \rightarrow C_y)$ – підсумкова критичність комбінованої атаки).

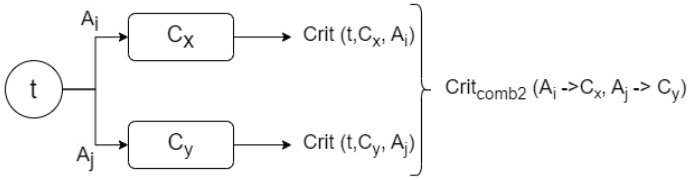


**Рис. 2. Послідовні комбіновані атаки на СБФ БПЛА**

3. Послідовно-паралельні атаки:

$$v_{comb3}(t) = \begin{cases} A_i(t) \to C_x; \\ A_j(t) \to C_y; \end{cases} \quad (3)$$

$$v_{comb3}(t+1) \begin{cases} A_r(t+1) \to Cw\ ; \\ A_s(t+1) \to Cz; \end{cases} \quad (4)$$

$$V_{comb3} = v_{comb3}(t) \times v_{comb3}(t+1), \quad (5)$$

Модель послідовно-паралельних атак визначається формулами (3), (4) та (5). Елемент $v_{comb3}(t)$ представляє можливість виконання атак $A_i$ та $A_j$ в момент часу t на компоненти $C_x$ та $C_y$ відповідно. Аналогічно, $v_{comb3}(t+1)$ описує можливість атак $A_r$ та $A_s$ в момент часу t+1 на компоненти $C_w$, $C_z$. Вираз (5) визначає загальну множину варіантів послідовно-паралельних атак, яке є добутком множин атак в моменти часу t та t+1, відповідно рисунку 3.


**Рис. 3. Послідовні комбіновані атаки на СБФ БПЛА**

Визначення ймовірності атак може включати експертні оцінки на підставі аналізу статистичних даних та моделювання сценаріїв атак.

### Послідовність і приклад IMECA аналізу при комбінованих атаках

Послідовність IMECA-аналізу при комбінованих атаках є наступною:

- виконується IMECA-аналіз кібербезпеки при одиничних кібератаках та оцінюються їх критичність [4];
- 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 різни 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 вини доповнюються додатковими контрзаходами;
- вибирається підмножина «покриваючих» контрзаходів з мінімальною вартістю при комбінованих кібератаках.

Розглянемо приклади реалізації елементів даної методики, базуючись на результатах роботи [4], 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 1, яка сформована на базі результатів аналізу [4], ілюструє варіанти комбінацій порушників та послідовні комбінації атак на систему.

Таблиця 1.

**Комбінації порушників та їх послідовні комбіновані атаки 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 2.

У роботі [4] 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, значенню ймовірності 1 відповідає 10 за шкалою оцінки для обчислення ризику. Тоді для такого еквіваленту $P^*_{A_n}$ ймовірності при оцінюванні ризику маємо:

$$P^*_{A_n} = \left(1 - \left((1-P_{A_1})\times(1-P_{A_2})\times(1-P_{A_3})\times\ldots(1-P_{A_n})\right)\right)\times 10 \quad (6)$$

$P^*_{A_n}$ використовує шкалу від 1 до 10 для визначення цілісного значення успішності послідовної комбінованої атаки. У формулі $P^*_{A_n}$ враховує ймовірність успіху всієї послідовної комбінованої атаки;

$$S^*_{A_n} = \max(S_1,\ldots,S_n) \quad ; \quad (7)$$

$$R^*_{A_n} = P^*_{A_n} \times S^*_{A_n}. \quad (8)$$

Згідно з результатами в таблиці 2, 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 2).

Таблиця № 2

**Критичність СБФ БПЛА після послідовної комбінації атак**

| № | 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. Він враховує середнє значення ризику та виокремлює найбільш критичні аспекти та ризики для подальшого підвищення безпеки системи (результати у таблиці 3).

Таблиця № 3

**Критичність СБФ БПЛА після послідовної комбінації атак**

| № | 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 |

У таблиці 4 представлено комбінації порушників та їх паралельні атаки на систему багатофункційних флотів БПЛА згідно з даними з [7], а таблиця 5 містить результати оцінки показників критичності для комбінованих паралельних атак на СБФ БПЛА, отримані за третім методом, де бралось максимальне значення ризику.

Результати паралельних комбінованих атак на систему СБФ БПЛА, представлені в таблиці 5, дозволяють зробити висновок про можливість адекватно враховувати ймовірності та тяжкості кожної атаки, а також їх взаємодію в контексті паралельних комбінацій. Матриці критичності, представлені в таблицях 6 та 7, відображають результати застосування третього методу.

Таблиця № 4

**Комбінації порушників та їх паралельні комбіновані атаки 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 № 5

**Критичність СБФ БПЛА при паралельних КА**

| № | Послідовність атак | Критичність | | | | |
|---|---|---|---|---|---|---|
| | | *3 метод* | | | *2 метод* | *1 метод* |
| | | R1 | R2 | Ризик, $R^*_{A_n}$ | 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 № 6

**Матриця критичності СБФ БПЛА при послідовних КА**

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

Таблиця № 7

**Матриця критичності СБФ БПЛА при паралельних КА**

| | Тяжкість | | |
|---|---|---|---|
| Ймовірність появи | Низька | Середня | Висока |
| Низька | | 2,4 | |
| Середня | 5 | 1,6 | |
| Висока | | 3 | |

Важливо відзначити, що оцінка критичності системи є складним завданням, що залежить від багатьох факторів, сценаріїв атак, навичок порушника, технічних характеристик. Критичність може змінюватися в залежності від ситуацій та характеристик обладнання.

**Вибір контрзаходів для підвищення захисту кібербезпеки СБФ БПЛА**

Для ілюстрації можливих підходів до вибору контрзаходів на підставі аналізу роботи [4] визначимо контрзаходи, які планується використовувати з метою підвищення рівня захищеності СБФ БПЛА. Вибір контрзаходів враховує специфіку загроз, що ставлять під загрозу кібербезпеку систем [8]. Виявлені загрози, пов'язані зі зміною навігаційних даних та шкідливим програмним забезпеченням, представляють значний ризик для стійкості та надійності системи, враховуючи слабкі механізми аутентифікації та авторизації, відсутність шифрування каналів комунікацій та недостатні заходи захисту від розподілених атак. З урахуванням виявлених загроз та вразливостей, визначено 10 контрзаходів для підвищення захищеності. Зокрема:

- автоматичне повернення або автоматична робота;
- шифрування даних;
- мережева безпека;
- стійке програмне забезпечення;
- фізична безпека;
- ефективні методи автентифікації та авторизації;
- постійний моніторинг та реагування;
- тренування персоналу;
- регулярний аудит безпеки;
- резервна підсистема відновлення.

Ці заходи спрямовані на зниження критичності атак і забезпечення кібербезпеки СБФ БПЛА (таблиця 8, де P - ймовірність, S - тяжкість, R - ризик).

Таблиця № 8

**Застосування контрзаходів для атак на СБФ БПЛА**

| № | № за [4] | Загроза | Вразливості | Атака | Контрзаходи | | | | | | | | | | Критичність після контрзаходів | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | P | S | R |
| 1 | 1 | Зміна навігаційних даних БПЛА | Використання нешифровані протоколи навігації | Маніпулювання навігаційними даними через атаку "Man-in-the-Middle". ARP-отруєння | | + | + | | | | + | | | | 6 | 5 | 30 |
| 2 | 2 | | Використання слабких паролів | Брутфорс атака на паролі | | | | | | + | | + | | | 5 | 4 | 20 |
| 3 | 3 | Віддалене вимкнення БПЛА | Відсутність або слабка сегментація мережі | Отримання несанкціонованого доступу внутрішнім користувачем | | | | | + | + | | | | | 4 | 6 | 24 |
| 4 | 4 | Віддалене вимкнення БПЛА | Несанкціонований доступ до системи через слабку аутентифікацію | Використання слабких паролів або аутентифікаційних вразливостей | | | | | | + | | | | | 5 | 5 | 25 |
| 5 | 13 | Зміна програмного забезпечення процесу зарядки | Відсутність аутентифікації та авторизації змін у програмному забезпеченні | Спуфінг ідентифікаторів або атака методом брутфорсу | + | | | + | | | + | | | + | 6 | 5 | 30 |

| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 6 | 14 | | Відсутність моніторингу програмного забезпечення | Невиявлене функціонування шпигунського ПЗ через відсутність моніторингу | + | + | + | | | | + | | + | + | 5 | 6 | 30 |
| 7 | 15 | Захоплення сеансу адміністратора | Відсутність механізму шифрування даних | Атака на перехоплення даних в процесі передавання | | + | + | | | | + | | + | + | 4 | 8 | 32 |
| 8 | 18 | Втручання в роботу системи зв'язку | Відсутність ефективних заходів захисту від розподілених атак | Розподілена атака на доступність сервісів хмарних сховищ | | | + | | | | + | | + | + | 6 | 7 | 42 |
| 9 | 19 | Злам системи управління БПЛА | Відсутність шифрування каналів комунікацій | Перехоплення та зміна команд, аналіз трафіку | | | | + | | + | + | | + | + | 4 | 8 | 32 |
| 10 | 23 | Впровадження шкідливих датчиків | Відсутня перевірка автентичності датчиків | Підміна справжніх датчиків на шкідливі | | | | | + | | + | | + | + | 5 | 6 | 30 |
| 11 | 24 | | Відсутня системи періодичної перевірки та виявлення шкідливих датчиків | Обхід системи виявлення та блокування шкідливих датчиків | | | | | + | | + | | + | + | 5 | 6 | 30 |
| 12 | 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 | + | + | | + | + | | + | | + | + | 6 | 5 | 30 |
| 13 | 26 | | Відсутня валідація вхідних даних | Впровадження шкідливого коду через вхідні дані | | + | + | + | | | + | + | + | + | 7 | 6 | 42 |
| 14 | 32 | Впровадження шкідливих датчиків | Вразливість у мережевому протоколі датчиків | Впровадження шкідливого програмного забезпечення через мережевий протокол датчиків | | | + | + | | + | + | | + | + | 7 | 8 | 56 |
| 15 | 33 | Віддалене вимкнення БПЛА | Слабка аутентифікація при віддаленому доступі до систем керування | Підміна авторизованих ідентифікаторів для отримання доступу до системи | | | | | | + | + | + | + | + | 4 | 8 | 32 |
| 16 | 36 | Злам серверів і сховищ даних | Використання старі протоколи для захисту даних в сховищах | SQL-ін'єкція або атака на сервери та сховища даних | | + | + | + | | | | | + | + | 7 | 6 | 42 |
| 17 | 37 | Захоплення чи модифікація медіа-матеріалів в процесі передачі з БПЛА | Відсутність відповідної аутентифікації | SQL ін'єкція | | + | + | + | | + | + | | + | + | 6 | 6 | 36 |

Позначки "+" у таблиці вказують на вибір максимального набору контрзаходів для конкретних загроз і вразливостей, що забезпечує зниження ймовірності та тяжкості атаки, а також загального ризику. Отже ризик для кожної з загроз – рядків таблиці може змінюватися в діапазоні від початкового - максимального (без використання будь-яких контрзаходів) до мінімального – при використанні всієї сукупності контрзаходів, позначених в таблиці.

Таким чином, важливо враховувати, що зміна обраного набору контрзаходів може вплинути на рівень кіберзахисту, збільшити ймовірність атаки та тяжкість її наслідків. Такий підхід до вибору контрзаходів враховує динаміку загроз та потребу постійного оновлення стратегії кіберзахисту для забезпечення високого рівня безпеки системи. Матриці критичності до і після впровадження контрзаходів, представлена в таблицях 9 і 10.

Таблиця № 9

**Матриця критичності СБФ БПЛА за відсутності контрзаходів**

| | Тяжкість | | |
|---|---|---|---|
| Ймовірність появи | Низька | Середня | Висока |
| Низька | | | 9 |
| Середня | | 3, 10,11,15,16 | 7,14 |
| Висока | | 2,4, 5,6 8,12,13 | 1,17 |

Таблиця № 10

**Матриця критичності СБФ БПЛА після контрзаходів**

| | Тяжкість | | |
|---|---|---|---|
| Ймовірність появи | Низька | Середня | Висока |
| Низька | | | 7,9,15 |
| Середня | | 1,2,3,4,5,6,10,11,12,17 | 8 |
| Висока | | 13,16 | 14 |

Для формулювання рейтингу ефективності (рівня зменшення критичності) та вартості застосування контрзаходів, введемо якості (Qual) та вартості (Cost) за шкалою від 1 до 10 (де 1 вказує на найнижчу якість/вартість, а 10 – на найвищу якість/вартість.

Результати експертних оцінок якості та витрат узагальнені та представлені на рисунку 4. Графічне подання даних демонструє взаємозв'язок між успішністю контрзаходів та їх вартістю, що є основою для прийняття обґрунтованих рішень у галузі кібербезпеки.

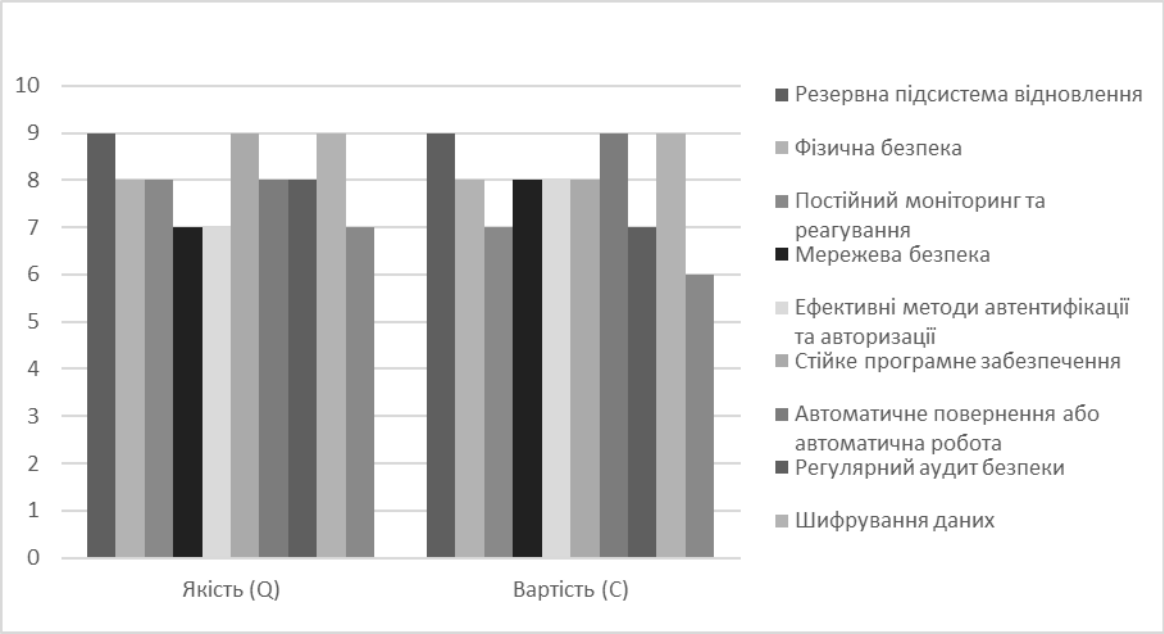


**Рис. 4. Графік оцінок якості і вартості контрзаходів для СБФ БПЛА**

Рисунок 4 ілюструє, наприклад, те, що резервна підсистема відновлення, шифрування даних та автоматичне повернення або автоматична робота визначаються як контрзаходи з високою якістю та вартістю. З іншого боку, тренування персоналу виявитися менш ефективним.

Вибір оптимальної сукупності контрзаходів на їх визначеній множині за критерієм «критичність-вартість» може бути здійснений у два кроки: спочатку відбираються множини контрзаходів, які забезпечують прийнятну критичність (ризики успішних атак), а потім серед цих множин визначається сукупність контразаходів, яка має мінімальну вартість. Уразі, якщо серед всіх можливих комбінацій контрзаходів немає такої, що забезпечує прийнятний ризик, їх множина має бути переглянута і визначено можливі шліх підсилення контрзаходів.

Варто зазначити, що вибір контрзаходів, з огляду на можливість комбінованих атак, здійснюється у такий самий спосіб після оцінки ризиків для кожної комбінації, що має бути розглянута. Не зважаючи на високу якість та вартість впровадження окремих контрзаходів, важливо враховувати, що це не гарантує їх успішність спектрі для різних сценаріїв атак або комбінованих загроз. Контекст і умови можуть впливати на ефективність контрзаходів. Доцільно проводити подальший аналізи і оцінки, враховуючи конкретні

характеристики та потенційні сценарії загроз для вибору стратегій кіберзахисту системи багатофункціональних флотів БПЛА.

**Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі**

В рамках дослідження розроблено моделі комбінованих кібератак та елементи ризик-орієнтованого методу оцінювання кібербезпеки СБФ БПЛА з використанням процедури IMECA-аналізу. Новизна результатів полягає у описі класу ККА з урахуванням різних тилів комбінування і визначення критичності. Крім того, запропоновано підхід до вибору контрзаходів для забезпечення кібербезпеки з огляду на вимоги та рівень їх якості та вартості.

Практичне значення цих результатів визначається тим, що створюється підгрунтя для розроблення інструментальних засобів для підтримки прийняття рішень в процесі аналізу та підвищення рівня кібербезпеки таких складних систем як СБФ БПЛА при одиничних і комбінованих кібератаках.

Важливим є вдосконалення методичного апарату оцінювання та забезпечення кібербезпеки СБФ БПЛА під час ККА. Подальші дослідження можуть зосереджуватися на деталізації моделей і методик оцінювання безпеки при різних комбінаціях кібератак і фізичних атак, ініційованих засобами РЕБ, аналіз впливу нових технологій на кібербезпеку, розроблення методів навчання для інтелектуальних засобів систем БПЛА з урахуванням розширених множин ККА.

**Література**

1. On the national security of Ukraine, the Law of Ukraine № 2469-VIII (2023) (Ukraine). https://zakon.rada.gov.ua/laws/show/2469-19#Text.

2. Niyonsaba, S., Konate, K., & Soidridine, M. M. (2023). A Survey on Cybersecurity in Unmanned Aerial Vehicles: Cyberattacks, Defense Techniques and Future Research Directions. *International Journal of Computer Networks and Applications*, *10*(5), 688. https://doi.org/10.22247/ijcna/2023/223417.

3. Torianyk, V., Kharchenko, V., Zemlianko, H. (2021, March). IMECA Based Assessment of Internet of Drones Systems Cyber Security Considering Radio Frequency Vulnerabilities. In IntelITSIS, pp. 460-470.

4. Zemlianko, H., & Kharchenko, V. (2023). Cybersecurity risk analysis of multifunctional UAV fleet systems: a conceptual model and IMECA-based technique. *Radioelectronic and Computer Systems*, (4), 152–170. https://doi.org/10.32620/reks.2023.4.11

5. Vazquez Trejo, J. A., Guenard, A., Adam-Medina, M., Ciarletta, L., Ponsart, J.-C., & Theilliol, D. (2023). Resilient Leader-Following Formation Control For a Fleet of Unmanned Aerial Vehicles Under Cyber-Attacks. У *2023 International Conference on Unmanned Aircraft Systems (ICUAS)*. IEEE. https://doi.org/10.1109/icuas57906.2023.10156075

6. Kharchenko, V., Kliushnikov, I., Rucinski, A., Fesenko, H., & Illiashenko, O. (2022). UAV Fleet as a Dependable Service for Smart Cities: Model-Based Assessment and Application. *Smart Cities*, *5*(3), 1151–1178. https://doi.org/10.3390/smartcities5030058

7. Medhi, J. K., Liu, R., Wang, Q., & Chen, X. (2023). Robust Multiagent Reinforcement Learning for UAV Systems: Countering Byzantine Attacks. *Information*, *14*(11), 623. https://doi.org/10.3390/info14110623

8. ТЗІ - інформаційна безпека та захист інформації [*TECHNICAL PROTECTION OF INFORMATION - information security and information protection*]. https://tzi.com.ua/downloads/2.5-004-99.pdf

**References**

1. On the national security of Ukraine, the Law of Ukraine № 2469-VIII (2023) (Ukraine). https://zakon.rada.gov.ua/laws/show/2469-19#Text.

2. Niyonsaba, S., Konate, K., & Soidridine, M. M. (2023). A Survey on Cybersecurity in Unmanned Aerial Vehicles: Cyberattacks, Defense Techniques and Future Research Directions. *International Journal of Computer Networks and Applications*, *10*(5), 688. https://doi.org/10.22247/ijcna/2023/223417.

3. Torianyk, V., Kharchenko, V., Zemlianko, H. (2021, March). IMECA Based Assessment of Internet of Drones Systems Cyber Security Considering Radio Frequency Vulnerabilities. In IntelITSIS, pp. 460-470.

4. Zemlianko, H., & Kharchenko, V. (2023). Cybersecurity risk analysis of multifunctional UAV fleet systems: a conceptual model and IMECA-based technique. *Radioelectronic and Computer Systems*, (4), 152–170. https://doi.org/10.32620/reks.2023.4.11

5. Vazquez Trejo, J. A., Guenard, A., Adam-Medina, M., Ciarletta, L., Ponsart, J.-C., & Theilliol, D. (2023). Resilient Leader-Following Formation Control For a Fleet of Unmanned Aerial Vehicles Under Cyber-Attacks. У *2023 International Conference on Unmanned Aircraft Systems (ICUAS)*. IEEE. https://doi.org/10.1109/icuas57906.2023.10156075

6. Kharchenko, V., Kliushnikov, I., Rucinski, A., Fesenko, H., & Illiashenko, O. (2022). UAV Fleet as a Dependable Service for Smart Cities: Model-Based Assessment and Application. *Smart Cities*, *5*(3), 1151–1178. https://doi.org/10.3390/smartcities5030058

7. Medhi, J. K., Liu, R., Wang, Q., & Chen, X. (2023). Robust Multiagent Reinforcement Learning for UAV Systems: Countering Byzantine Attacks. *Information*, *14*(11), 623. https://doi.org/10.3390/info14110623

8. ТЗІ - інформаційна безпека та захист інформації [*TECHNICAL PROTECTION OF INFORMATION - information security and information protection*]. https://tzi.com.ua/downloads/2.5-004-99.pdf