Міністерство освіти і науки України

Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Наукова робота
представлена на здобуття премії Президента України для молодих учених

МЕТОДИ ТА ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КОМП’ЮТЕРНИХ СИСТЕМ І МЕРЕЖ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Колектив авторів:

1. **ЗЕМЛЯНКО Георгій Андрійович** – доктор філософії (PhD), старший викладач кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут».

2. **МОРОЗОВА Ольга Ігорівна** – доктор технічних наук, професор, професор кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут».

3. **НІЧЕПОРУК Андрій Олександрович** – кандидат технічних наук, доцент, доцент кафедри комп’ютерної інженерії та інформаційних систем Хмельницького національного університету.

4. **ТЕЦЬКИЙ Артем Григорович** – кандидат технічних наук, доцент кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут».

Харків – 2025

ОСНОВНІ ПОЛОЖЕННЯ ДОСЛІДЖЕННЯ

Мета роботи

Забезпечення кібербезпеки комп’ютерних систем і мереж об'єктів критичної інфраструктури шляхом розроблення та впровадження відповідної методології (концепції, принципів, комплексу моделей, методів) і технологій в критичних системах, а також при підготовці фахівців з кібербезпеки під час здобуття професійних знань.

Науково-прикладна задача

Розроблення моделей, методів і технологій забезпечення кібербезпеки мобільних операційних систем, вебсистем критичної інфраструктури, флотів безпілотних апаратів, комп’ютерних мереж, що забезпечують їх взаємодію, та методології підготовки фахівців з кібербезпеки комп’ютерних систем і мереж об'єктів критичної інфраструктури.

Завдання дослідження

1. Запропоновано концепцію та принципи забезпечення кібербезпеки комп’ютерних систем і мереж об'єктів критичної інфраструктури.

2. Розроблено модель згорткової нейронної мережі на основі використання змішаних даних, а також метод виявлення шкідливого програмного забезпечення в Android-сумісних мобільних операційних системах для об'єктів критичної інфраструктури.

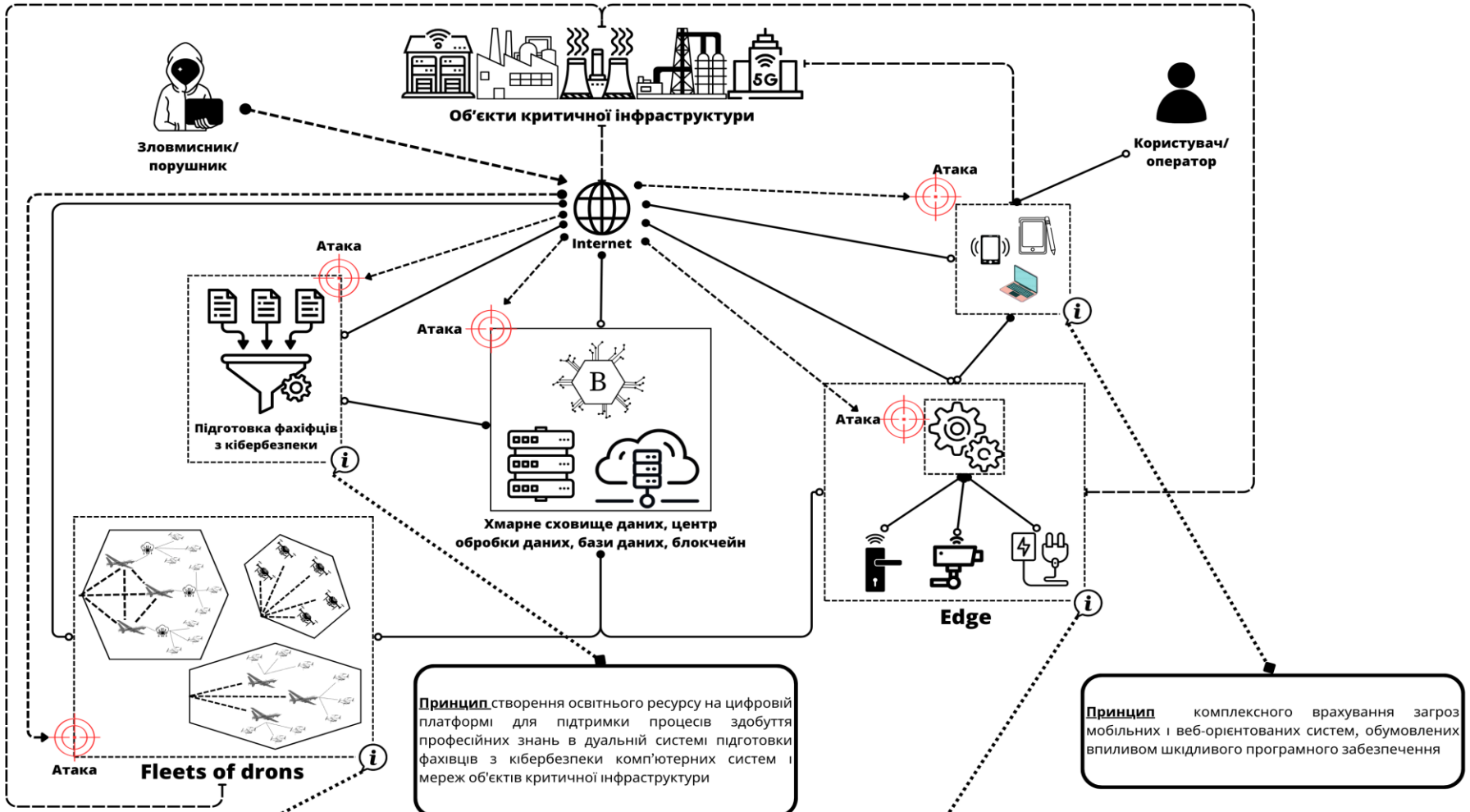
3. Розроблено методи оцінювання та забезпечення кібербезпеки вебсистем критичної інфраструктури на основі систем керування вмістом шляхом використання дерев атак.

4. Розроблено модель та методи забезпечення кібербезпеки флотів безпілотних апаратів, які враховують особливості їхньої багатофункціональної структури, динаміку взаємодії між окремими компонентами системи та зовнішніми середовищами, а також забезпечують захист від різноманітних одиничних і комбінованих атак.

5. Розроблено методологічні основи створення інформаційної технології й модель цифрової платформи знань для використання в дуальній системі підготовки фахівців з кібербезпеки комп`ютерних систем і мереж об'єктів критичної інфраструктури.

6. Впроваджено методи технологій забезпечення кібербезпеки комп’ютерних систем і мереж об'єктів критичної інфраструктури.

ПРЕДМЕТНА ОБЛАСТЬ ДОСЛІДЖЕННЯ



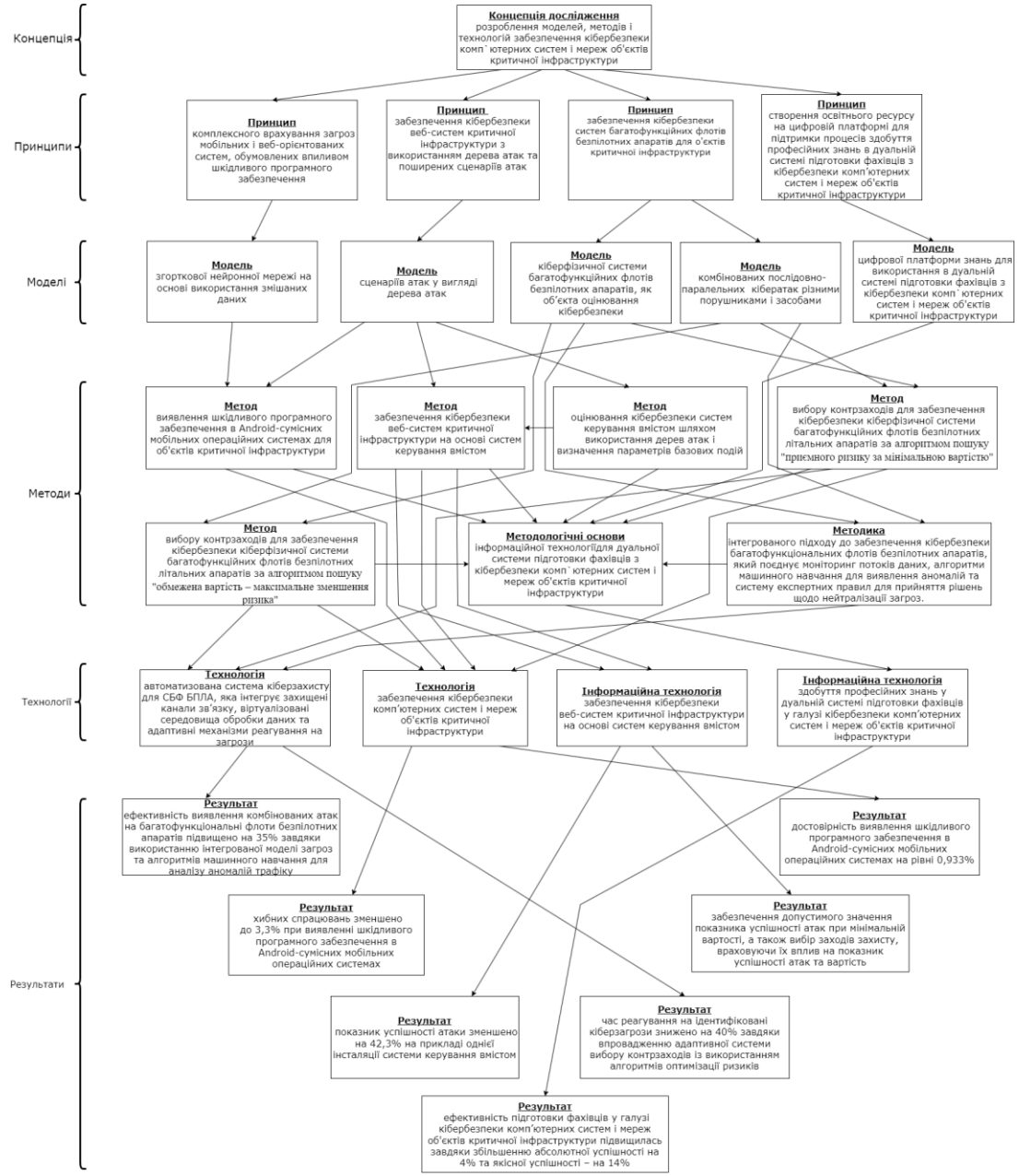
Принцип створення освітнього ресурсу на цифровій платформі для підтримки процесів здобуття професійних знань в дуальній системі підготовки фахівців з кібербезпеки комп'ютерних систем і мереж об'єктів критичної інфраструктури

Принцип забезпечення кібербезпеки систем багатофункційних флотів безпілотних апаратів для о'єктів критичної інфраструктури

Принцип забезпечення кібербезпеки веб-систем критичної інфраструктури з використанням дерева атак та поширених сценаріїв атак

Принцип комплексного врахування загроз мобільних і веб-орієнтованих систем, обумовлених впливом шкідливого програмного забезпечення

СТРУКТУРА ТА ВЗАЄМОЗВ'ЯЗОК ЕЛЕМЕНТІВ МЕТОДОЛОГІЇ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ



МЕТОД ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В ANDROID-СУМІСНИХ МОБІЛЬНИХ ОПЕРАЦІЙНИХ СИСТЕМАХ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

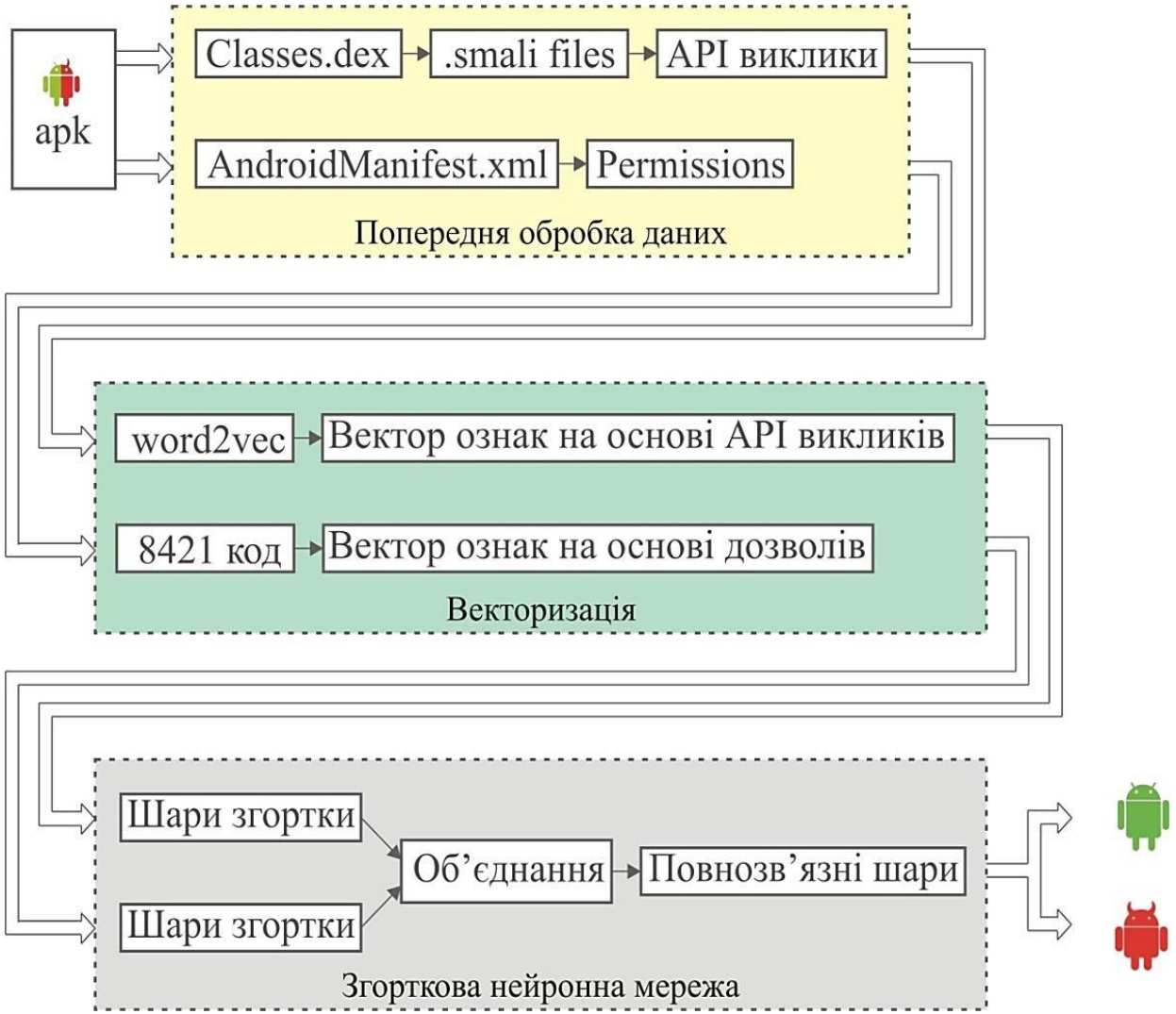


Рисунок 5.1 – Узагальнена структура методу виявлення шкідливого програмного забезпечення в Android-сумісних мобільних операційних системах для об'єктів критичної інфраструктури

Input: AndroidManifest.xml *Manifest*
SetOfSmaliFiles S_i
Output: API_list *API*
begin
  PointsToBeProcessed=emptyList();
  API = emptyList();
  foreach M_i **in** *Manifest* **do**
    if $M_i \in$ AndroidManifest.Activities || $M_i \in$ AndroidManifest.Services
      PointsToBeProcessed $\leftarrow M_i$
  foreach S_i **in** *PointsToBeProcessed* **do**
    foreach *Instruction* **in** S_i **do**
      if *Instruction* $\in$ (invoke-* = android, java, javax)
        API $\leftarrow$ *Instruction*
      if *Instruction* $\in$ ReferencesToCustomMethodCall
        PointsToBeProcessed $\leftarrow$ *Instruction*
  return *API*
end

Рисунок 5.2 – Алгоритм отримання API викликів зі smali файлів

МЕТОД ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В ANDROID-СУМІСНИХ МОБІЛЬНИХ ОПЕРАЦІЙНИХ СИСТЕМАХ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

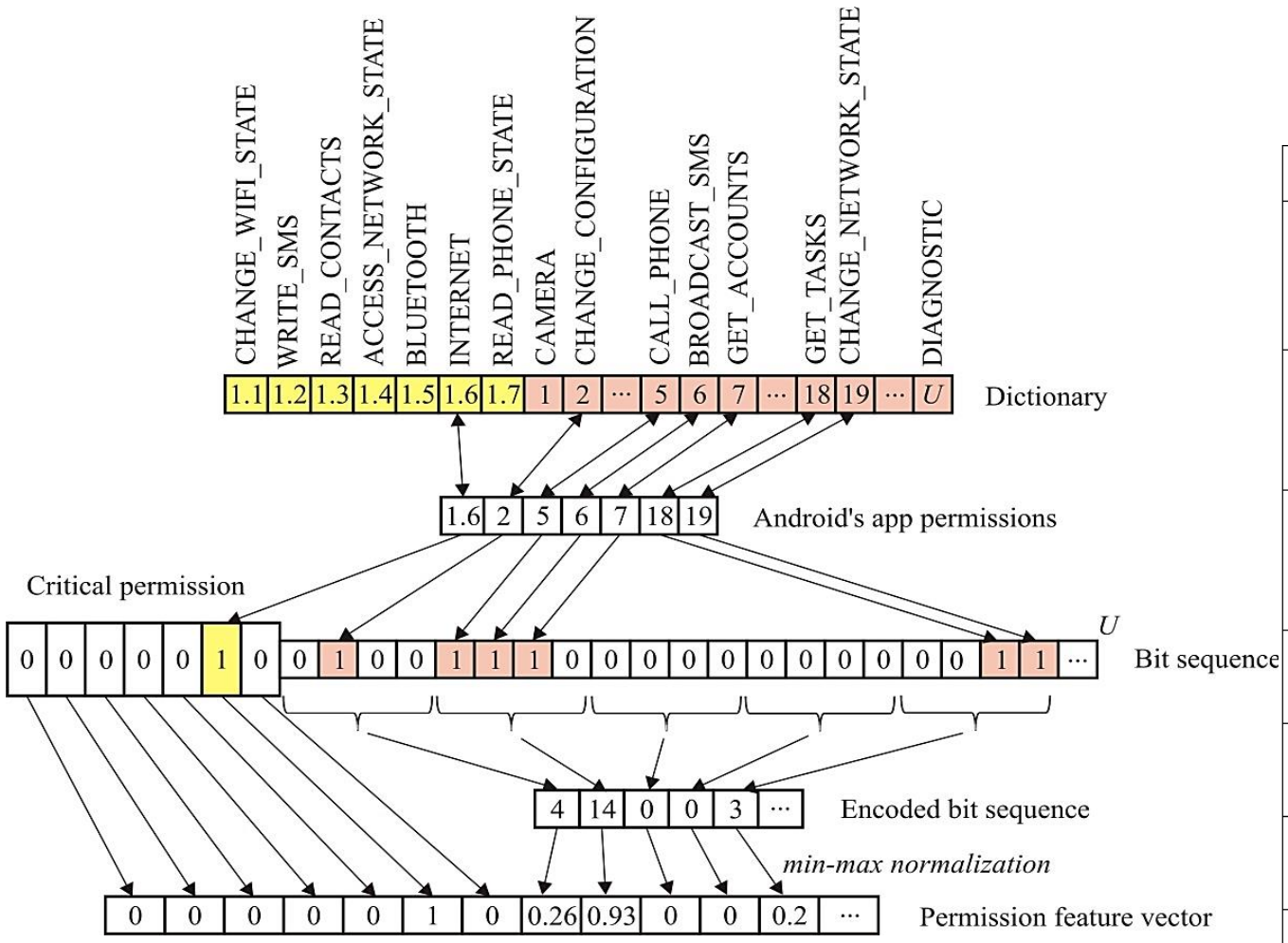


Рисунок 6 – Процес представлення множини дозволів Android-сумісного мобільного додатку у вигляді вектора ознак

Таблиця 6 – Значення параметрів для пропонованої моделі згорткової нейронної мережі на основі використання змішаних даних

Параметри згорткової підмережі для опрацювання API викликів		Параметри згорткової підмережі для опрацювання дозволів		Параметри повнозв'язних шарів	
Розмірність вхідного вектора D_a	64	Розмірність вхідного вектора D_p	49	Кількість нейронів у вхідному шарі F_1+F_2, активація	128, ReLu
Довжина вхідної послідовності L_a	200	Довжина вхідної послідовності L_p	50	Кількість нейронів у прихованому шарі H, активація	32, ReLu
Розмірність ядра K_{11}, значення padding, stride	3, 1, 1	Розмірність ядра K_{21}, значення padding, stride	2, 1, 1	Кількість нейронів у прихованому шарі O, активація	2, Softmax
Розмірність ядра K_{12}, значення padding, stride	3, 1, 2	Розмірність ядра K_{22}, значення padding, stride	3, 1, 2	–	–
Кількість нейронів в шарі C_{11}, активація	64, ReLu	Кількість нейронів в шарі C_{21}, активація	64, ReLu	–	–
Кількість нейронів в шарі C_{12}, активація	128, ReLu	Кількість нейронів в шарі C_{22}, активація	128, ReLu	–	–
Кількість нейронів у flatten шарі F_1, активація	64, ReLu	Кількість нейронів у flatten шарі F_2, активація	64, ReLu	–	–

МОДЕЛЬ ЗГОРТКОВОЇ НЕЙРОННОЇ МЕРЕЖІ НА ОСНОВІ ВИКОРИСТАННЯ ЗМІШАНИХ ДАНИХ

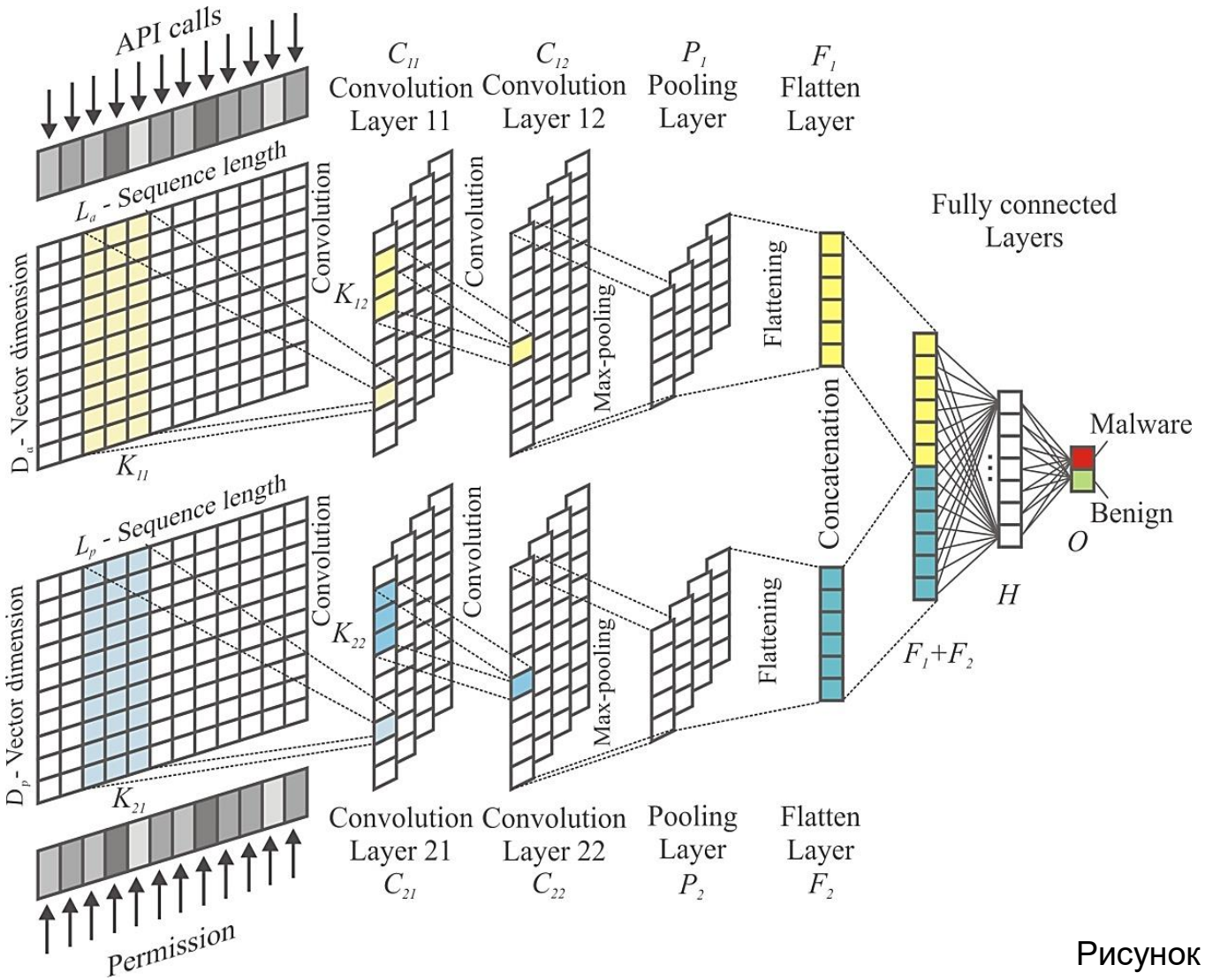


Рисунок 7.1 – Модель згорткової нейронної мережі на основі використання змішаних даних

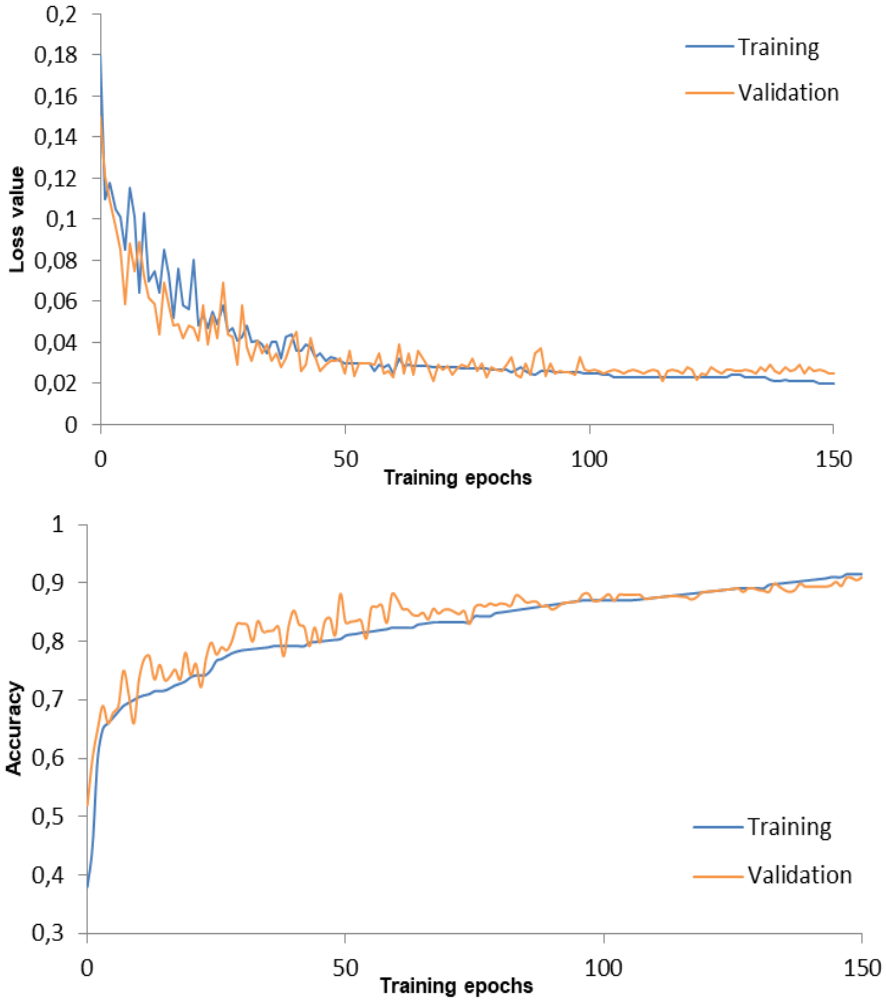


Рисунок 7.2 – Параметри навчання та валідації нейронної мережі: а) функція втрат; б) значення достовірності

МЕТОД ОЦІНЮВАННЯ КІБЕРБЕЗПЕКИ СИСТЕМ КЕРУВАННЯ ВМІСТОМ

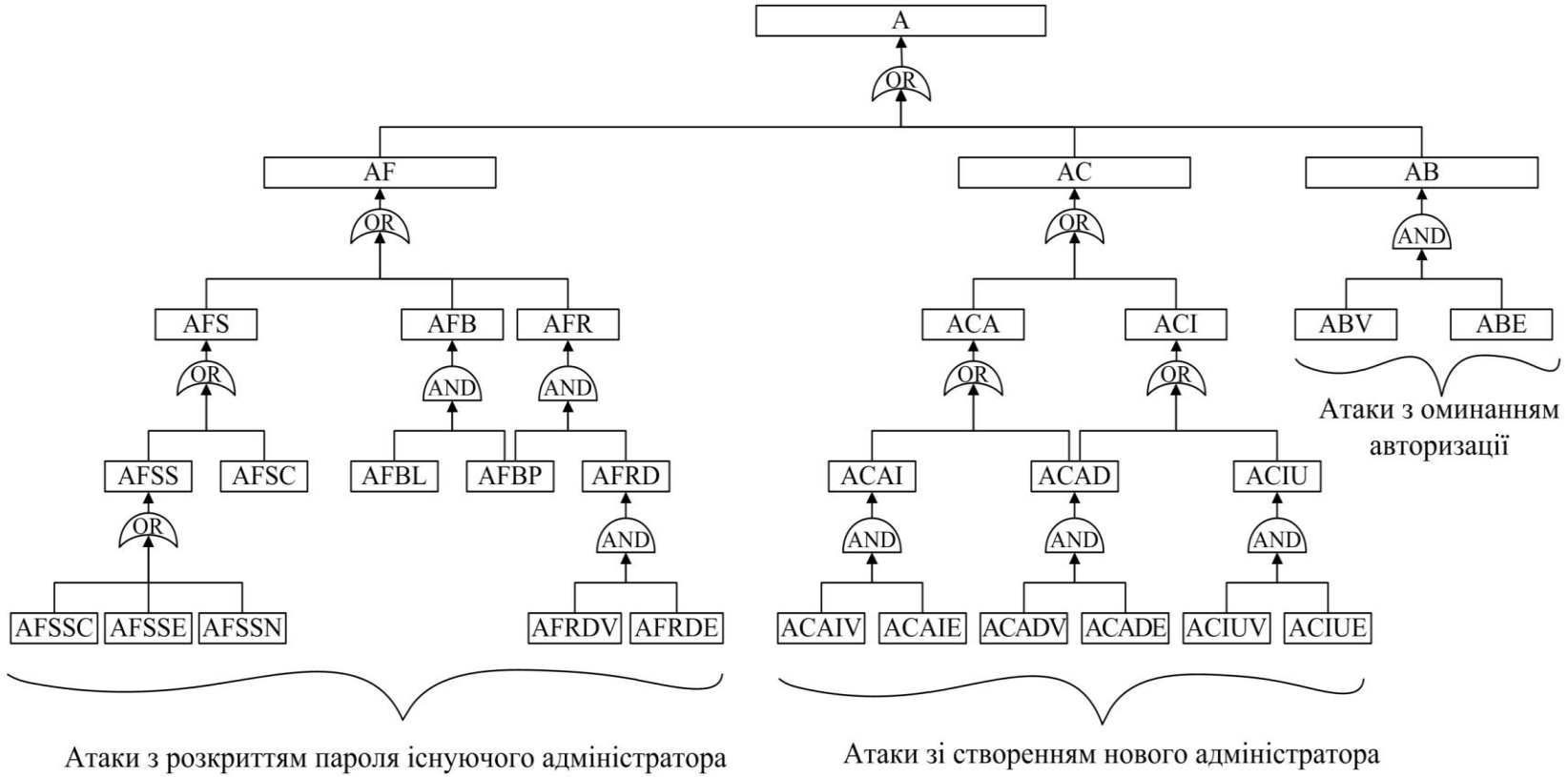


Рисунок 8 – Дерево атак на систему керування вмістом, на якому базується метод

Основна подія – успішна атака Web-застосунку. Під успішної атакою мається на увазі отримання несанкціонованого доступу до функцій, доступним тільки адміністратору з панелі управління.

Таблиця 8 – Повні назви подій

Скорочення	Повна назва події
A	Отримати доступ до функцій панелі управління
AF	Дізнатися логін і пароль існуючого адміністратора
AC	Створити новий обліковий запис адміністратора
AB	Оминути авторизацію
AFS	Вкрасти логін і пароль
AFB	Дізнатися логін і пароль методом перебору
AFR	Підібрати пароль за допомогою відомого хеша
ACA	Додати новий обліковий запис з привілеями безпосередньо в базу даних
ACI	Збільшити стандартні користувацькі привілеї
ABV	Знайдено вразливості для оминання авторизації
ABE	Експлуатуються вразливості для оминання авторизації
AFSS	Облікові дані вкрадені зі сховища
AFSC	Облікові дані вкрадені під час передачі по незашифрованому каналу
AFBL	У зловмисника є словник, який містить шуканий логін
AFBP	У зловмисника є словник, який містить шуканий пароль
AFRD	Отримати ім’я користувача та пароль з бази даних
ACAI	Використання відповідних вразливостей (наприклад, SQL-ін’єкція при вставленні)
ACAD	Відомі облікові дані для підключення до бази даних
ACIU	Використання відповідних вразливостей (наприклад, SQL-ін’єкція при оновленні)
AFSSC	Облікові дані вкрадені з ПК
AFSSE	Облікові дані вкрадені з електронної пошти або будь-якого хмарного сховища
AFSSN	Облікові дані вкрадені з нецифрового сховища
AFRDV	Виявлено відповідні вразливості, що дозволяють отримати ім’я користувача і пароль з бази даних
AFRDE	Експлуатація вразливостей, що дозволяють отримати ім’я користувача і пароль з бази даних
ACAIV	Виявлено відповідні вразливості (наприклад, SQL-ін’єкція при вставленні)
ACAIE	Експлуатація вразливостей (наприклад, SQL-ін’єкція при вставленні)
ACADV	Виявлено відповідні вразливості для підключення до бази даних
ACADE	Експлуатація вразливостей для підключення до бази даних
ACIUV	Виявлено відповідні вразливості (наприклад, SQL-ін’єкція при оновленні)
ACIUE	Експлуатація вразливостей (наприклад, SQL-ін’єкція при оновленні)

МЕТОД ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СИСТЕМ КЕРУВАННЯ ВМІСТОМ

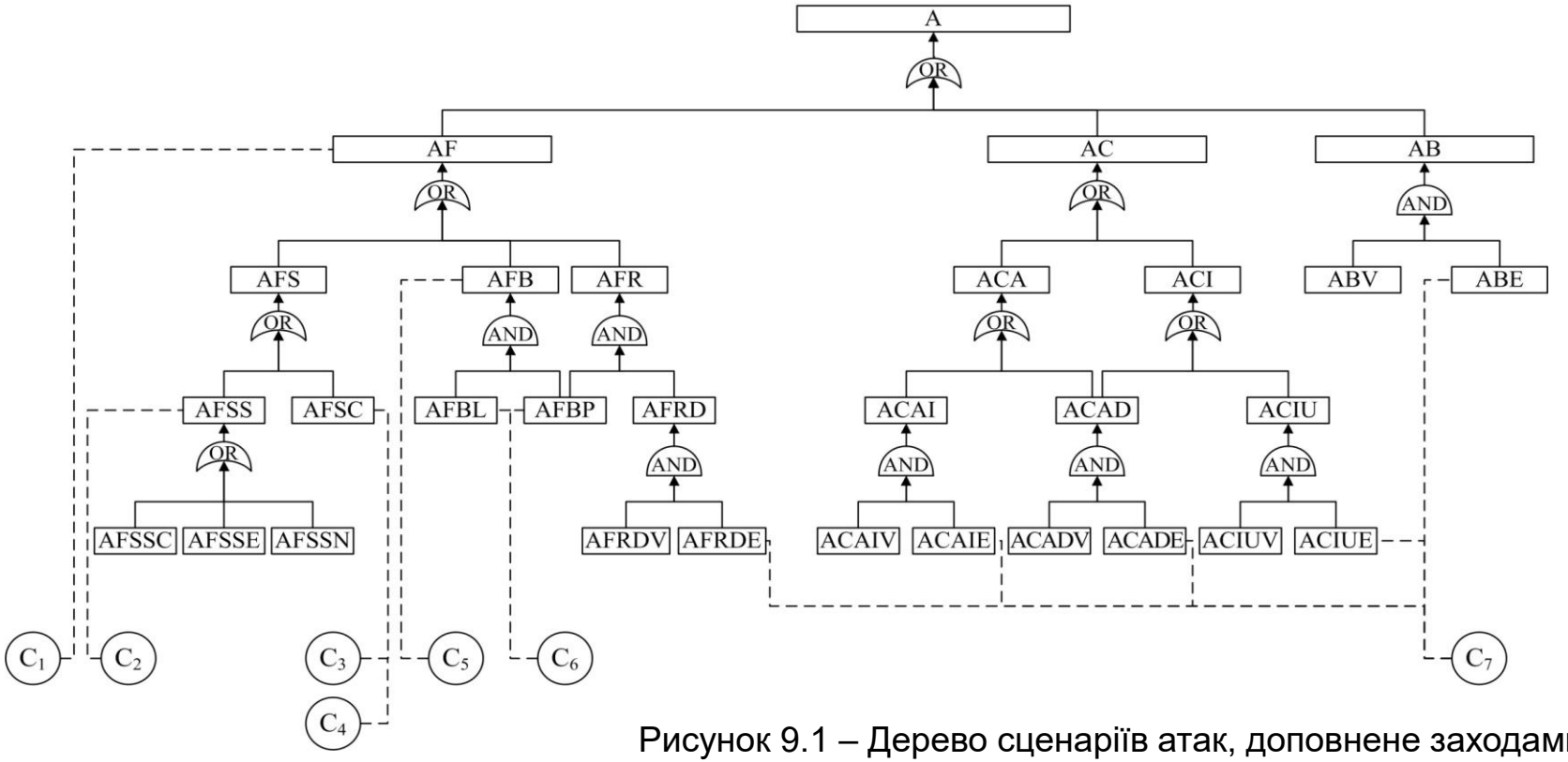


Рисунок 9.1 – Дерево сценаріїв атак, доповнене заходами захисту

Таблиця 9 – Перелік контрзаходів і їх параметрів

Контрзахід	Події, на які впливає контрзахід	Коефіцієнт впливу	Вартість (ум. од.)
C_1 – Використання двофакторної автентифікації	AF	0,8	120
C_2 – Тренінги для персоналу	AFSS	0,5	300
C_3 – Використання HTTPS	AFSC	0,7	50
C_4 – Використання VPN	AFSC	0,8	80
C_5 – Захист від перебору логінів і паролів	AFB	0,9	60
C_6 – Встановлення складних паролів і нестандартних логінів	AFBL, AFBP	0,6	20
C_7 – Встановлення та налаштування файрволу	AFRDE, ACAIE, ACADE, ACIUE, ABE	0,75	220

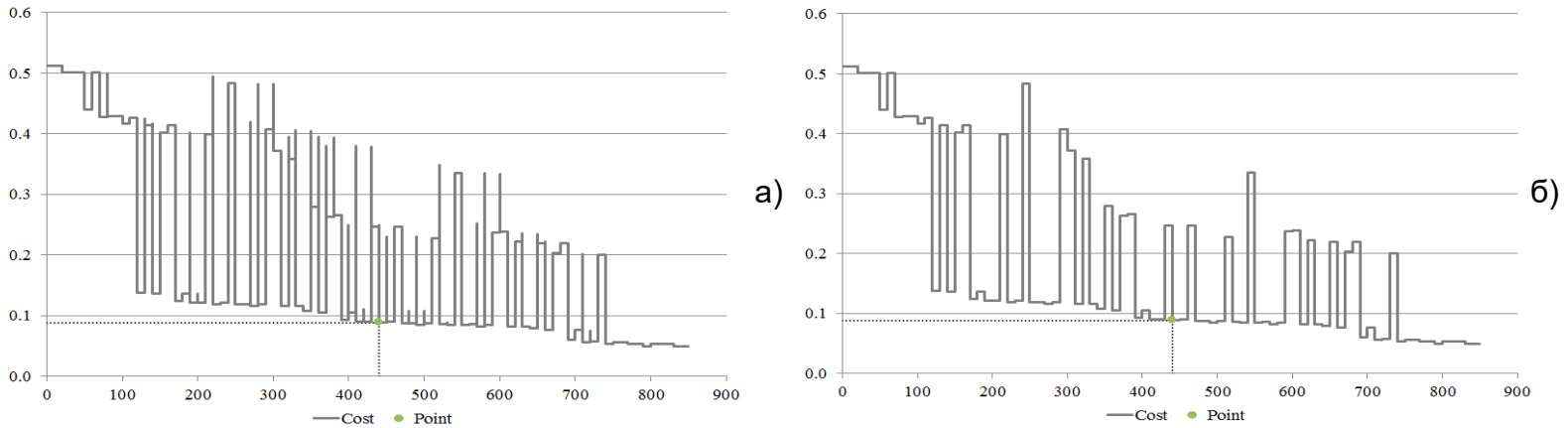


Рисунок 9.2 – Графік залежності показника успішності атаки від бюджету:
а) усі комбінації контрзаходів
б) найефективніші комбінації

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СИСТЕМ КЕРУВАННЯ ВМІСТОМ

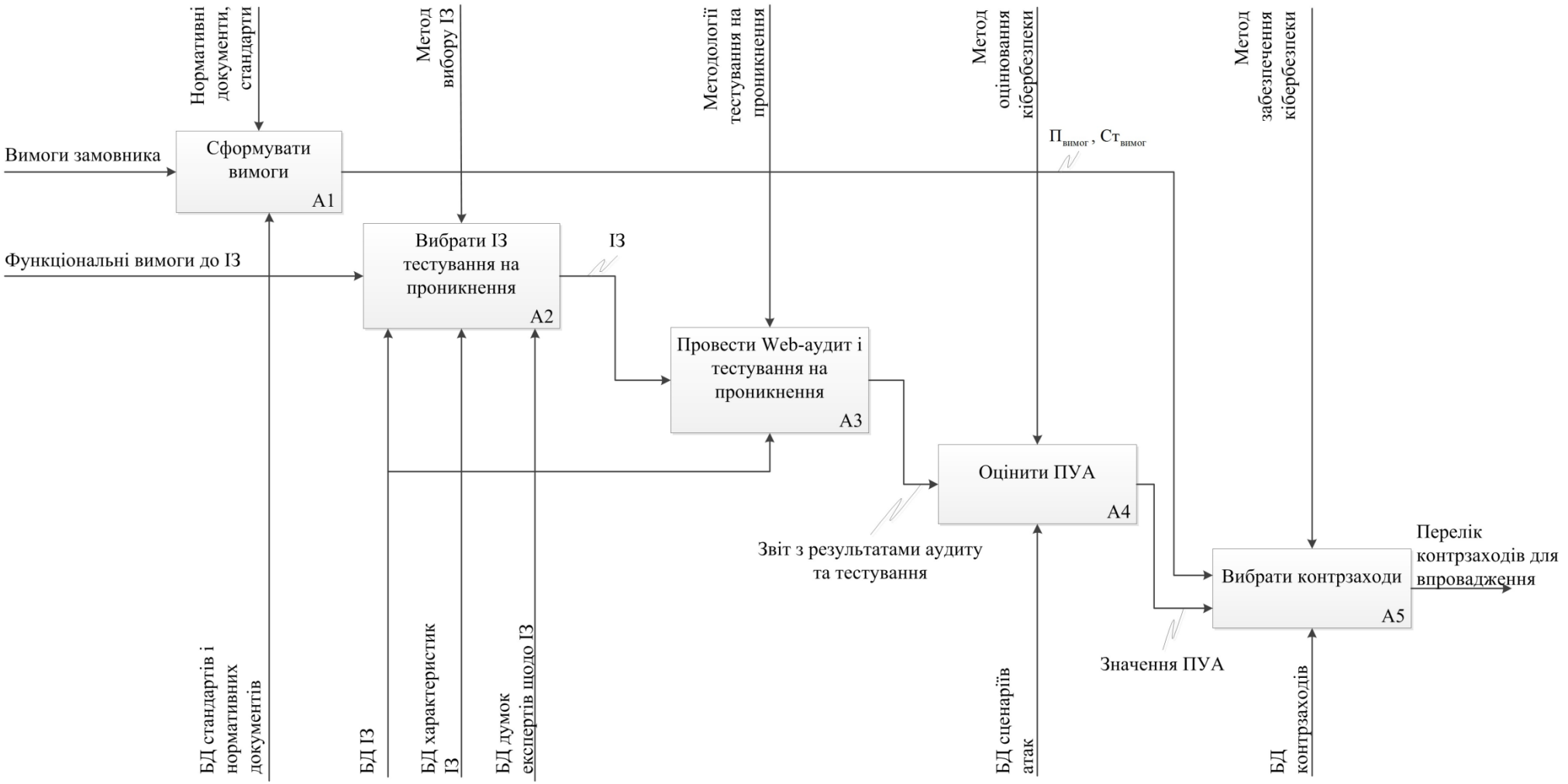


Рисунок 10 – Вузол А0 – Вибрати заходи захисту, враховуючи їх вплив на показник успішності атаки

МОДЕЛЬ КІБЕРФІЗИЧНОЇ СИСТЕМИ БАГАТОФУНКЦІЙНИХ ФЛОТІВ БЕЗПІЛОТНИХ АПАРАТІВ (1)

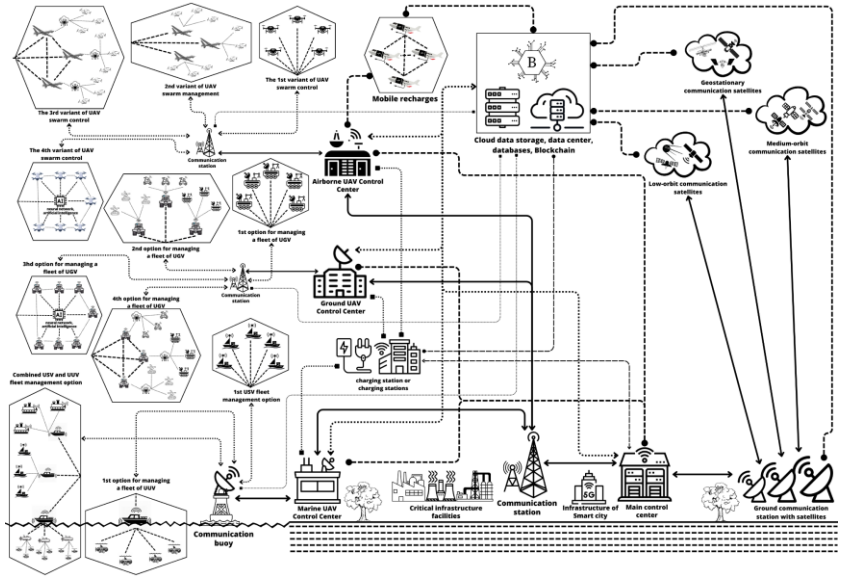


Рисунок 11.1 – Узагальнена схема кіберфізичної системи СБФ БА

Система складається з трьох груп:

- Критичні об'єкти та інфраструктура
- Мобільні системи (всі безпілотники та рухомі станції для зарядження та обслуговування)
- Центри керування та зв'язку, комунікаційне обладнання, програмне забезпечення, тощо.

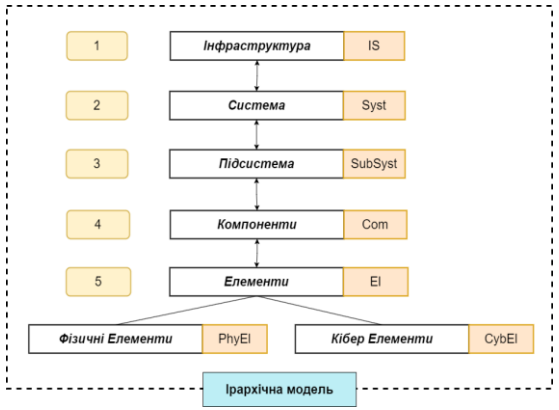


Рисунок 11.3 – Концептуальна схема системи багатофункційних флотів БПЛА

Позначення:

IS – інфраструктура;

Syst – системи;

SubSyst – підсистеми;

Com – компоненти;

El – елементи;

L – зв'язки між системами, підсистемами, компонентами та елементами

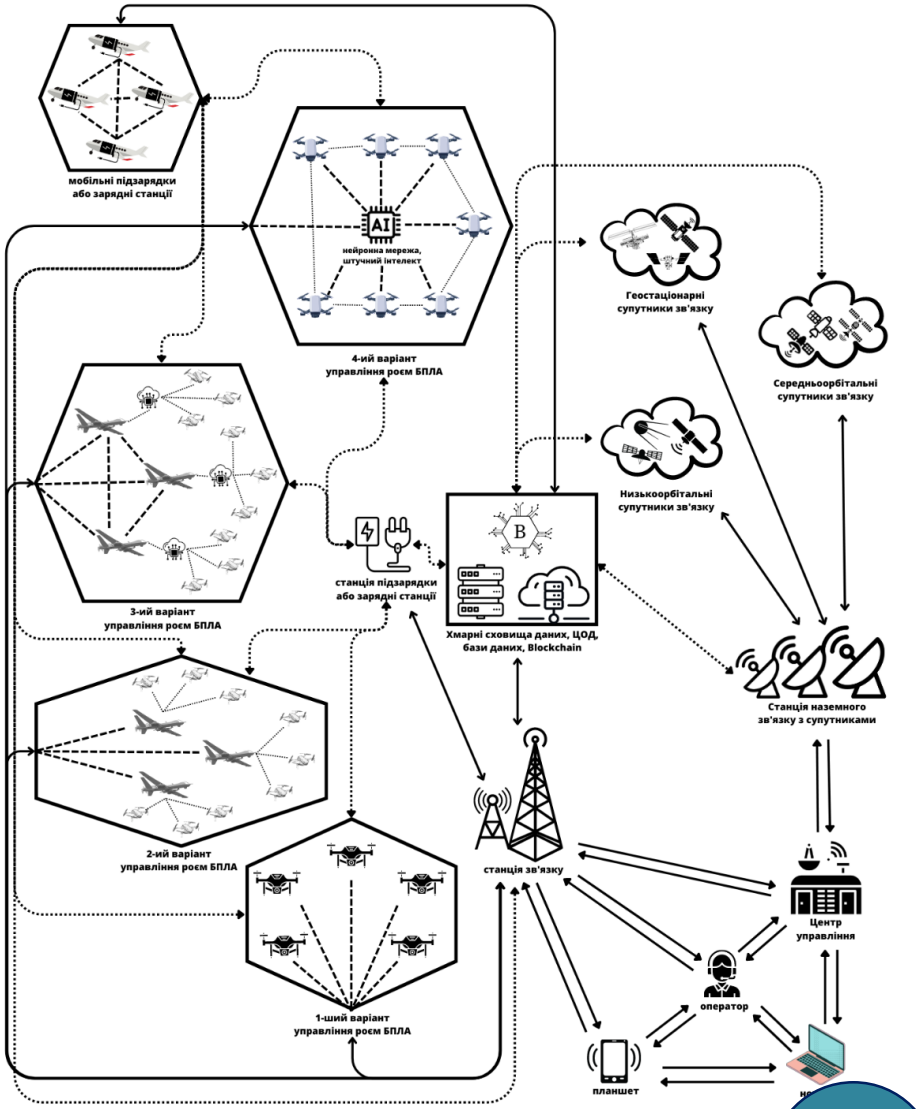


Рисунок 11.2 – Концептуальна схема системи багатофункційних флотів БПЛА

МОДЕЛЬ КІБЕРФІЗИЧНОЇ СИСТЕМИ БАГАТОФУНКЦІЙНИХ ФЛОТІВ БЕЗПІЛОТНИХ АПАРАТІВ (2)

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

$$L_{Syst_i} = \begin{array}{c} \\ SubSyst_{i1} \\ \vdots \\ SubSyst_{ij} \\ \vdots \\ SubSyst_{in_i} \end{array} \begin{array}{c} \begin{array}{ccccc} SubSyst_{i1} & \cdots & SubSyst_{ij} & \cdots & SubSyst_{in_i} \end{array} \\ \begin{bmatrix} - & \cdots & L_{i1,ij}^{cyber}, L_{i1,ij}^{phys} & \cdots & L_{i1,in_i}^{cyber}, L_{i1,in_i}^{phys} \\ L_{ij,i1}^{cyber}, L_{ij,i1}^{phys} & \cdots & - & \cdots & L_{ij,in_i}^{cyber}, L_{ij,in_i}^{phys} \\ L_{in_i,i1}^{cyber}, L_{in_i,i1}^{phys} & \cdots & L_{in_i,ij}^{cyber}, L_{in_i,ij}^{phys} & \cdots & - \end{bmatrix} \end{array} \quad (2)$$

$$L_{Com_{ijk}} = \begin{array}{c} \\ El_{ijk1} \\ \vdots \\ El_{ijkp} \\ \vdots \\ El_{ijkn_{ijk}} \end{array} \begin{array}{c} \begin{array}{ccccc} El_{ijk1} & \cdots & El_{ijkp} & \cdots & El_{ijkn_{ijk}} \end{array} \\ \begin{bmatrix} - & \cdots & L_{ijk1,ijkp}^{cyber}, L_{ijk1,ijkp}^{phys} & \cdots & L_{ijk1,ijkn_{ijk}}^{cyber}, L_{ijk1,ijkn_{ijk}}^{phys} \\ L_{ijkp,ijk1}^{cyber}, L_{ijkp,ijk1}^{phys} & \cdots & - & \cdots & L_{ijkp,ijkn_{ijk}}^{cyber}, L_{ijkp,ijkn_{ijk}}^{phys} \\ L_{ijkn_{ijk},ijk1}^{cyber}, L_{ijkn_{ijk},ijk1}^{phys} & \cdots & L_{ijkn_{ijk},ijkp}^{cyber}, L_{ijkn_{ijk},ijkp}^{phys} & \cdots & - \end{bmatrix} \end{array} \quad (3)$$

$$L_{SubSyst_{ij}} = \begin{array}{c} \\ Com_{ij1} \\ \vdots \\ Com_{ijk} \\ \vdots \\ Com_{ijn_{ij}} \end{array} \begin{array}{c} \begin{array}{ccccc} Com_{ij1} & \cdots & Com_{ijk} & \cdots & Com_{ijn_{ij}} \end{array} \\ \begin{bmatrix} - & \cdots & L_{ij1,ijk}^{cyber}, L_{ij1,ijk}^{phys} & \cdots & L_{ij1,ijn_{ij}}^{cyber}, L_{1,ijn_{ij}}^{phys} \\ L_{ijk,ij1}^{cyber}, L_{ijk,ij1}^{phys} & \cdots & - & \cdots & L_{ijk,ijn_{ij}}^{cyber}, L_{ijk,ijn_{ij}}^{phys} \\ L_{ijn_{ij},ij1}^{cyber}, L_{ijn_{ij},ij1}^{phys} & \cdots & L_{ijn_{ij},ijk}^{cyber}, L_{ijn_{ij},ijk}^{phys} & \cdots & - \end{bmatrix} \end{array} \quad (4)$$

$$El_q = \{CybEl_q, PhyEl_q, L_{ijkp}\} \quad (5)$$

Для математичного опису використовуються позначення: IS (інфраструктура), Syst (системи), SubSyst (підсистеми), Com (компоненти), El (елементи). Зв'язки між ними моделюються за допомогою множин, наприклад, IS - множина об'єктів інфраструктури, L_IS - матриця зв'язків між ними.
Аналогічно описуються Syst, SubSyst, Com та El. Цей підхід дозволяє систематично аналізувати інфраструктуру багатофункційних флотів БПЛА з точки зору кібербезпеки та вразливостей до комбінованих атак.

Порушники системи багатофункційних флотів БПЛА, згідно з українськими стандартами, є особами чи організаціями, що діють протиправно. Їхні мотивації враховують вплив на конфіденційність, цілісність, доступність та спостережуваність інформації. У таблиці наведено види порушників, їх мотивації та потенціал загроз, включаючи змову для підвищення ефективності. Класифікація адаптована до особливостей досліджуваної системи.

Тип. поруш.	№ виду	Види порушника	Можливі цілі (мотивація) реалізації загроз
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
	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.

МОДЕЛЬ КОМБІНОВАНИХ ПОСЛІДОВНО-ПАРАЛЕЛЬНИХ КІБЕРАТАК РІЗНИМИ ПОРУШНИКАМИ І ЗАСОБАМИ

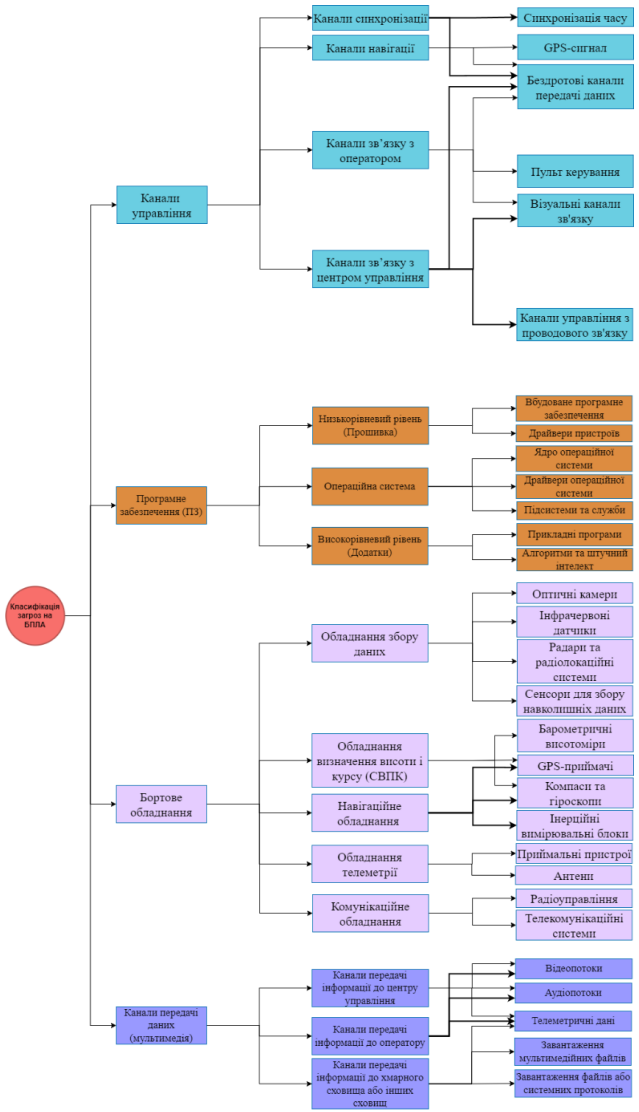
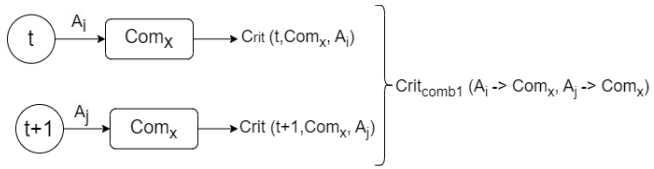


Рисунок 13.1 – Класифікація загроз на БПЛА

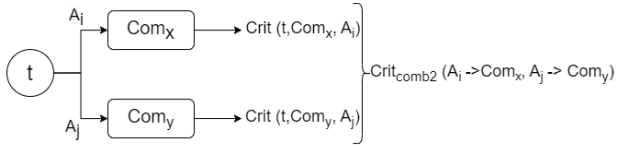
Послідовні комбіновані атаки на СБФ БПЛА



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

Рисунок 13.2 – Послідовні комбіновані атаки

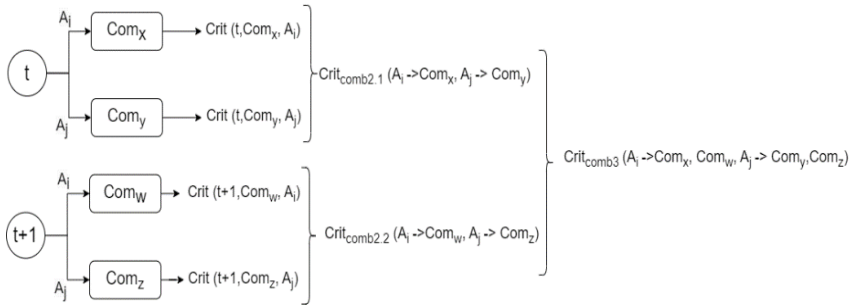
Паралельні комбіновані атаки на СБФ БПЛА



$$A_{comb2}(Com_x, Com_y)=\{A_i(t, Com_x), A_j(t, Com_y)\},$$

Рисунок 13.2 – Паралельні комбіновані атаки

Послідовно-паралельні комбіновані атаки на СБФ БПЛА



$$v_{comb3}(t) = \begin{cases} A_i(t) \rightarrow Com_x; \\ A_j(t) \rightarrow Com_y; \end{cases}$$

$$v_{comb3}(t+1) = \begin{cases} A_r(t+1) \rightarrow Com_w; \\ A_s(t+1) \rightarrow Com_z; \end{cases}$$

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

Рисунок 13.2 – Послідовно-паралельні комбіновані атаки

МЕТОДИ ВИБОРУ КОНТРЗАХОДІВ ЗА ВИЗНАЧЕНИМИ КРИТЕРІЯМИ

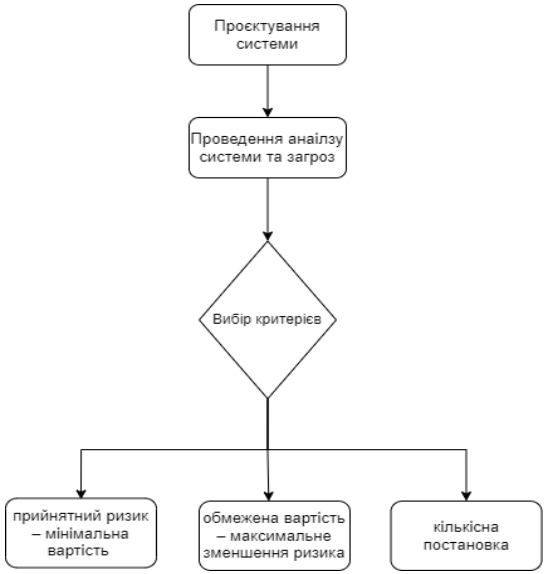


Рисунок 14.1 – Загальна схема методу вибору контрзаходів для забезпечення кібербезпеки СБФ БПЛА за визначеними критеріями

Показник відносного зменшення ризиків системи

RDR = ((IVR – EVR)/IVR)*100%

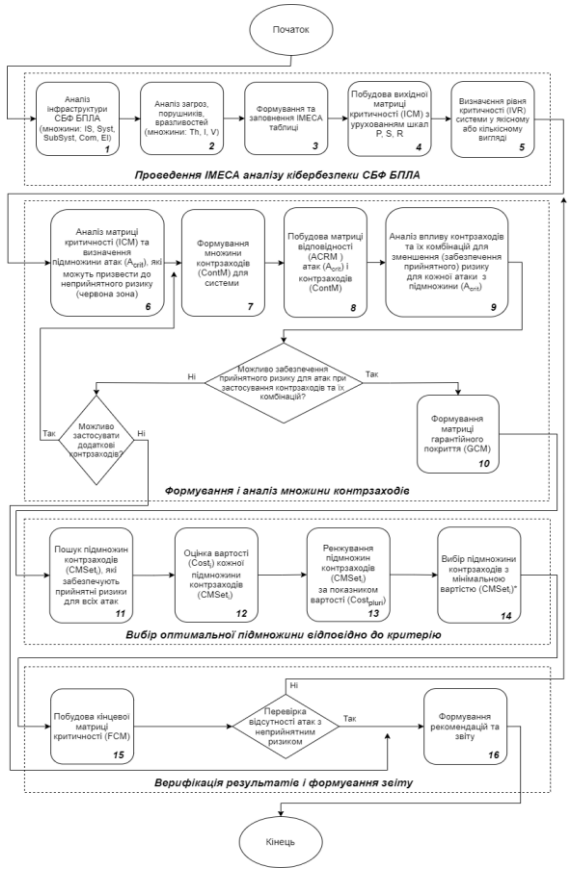
де:

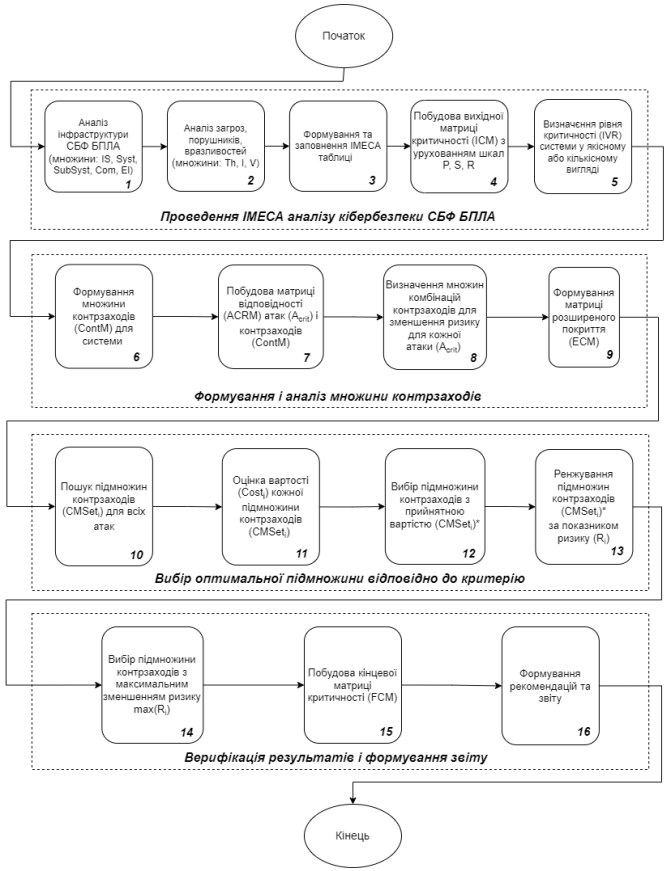
- **IVR** – інтегральний показник рівня ризиків без впровадження контрзаходів,
- **EVR** - інтегральний показник рівня ризиків після впровадження визначеної множини контрзаходів.

$$IVR = \sum IRVA_i$$

$$EVR = \sum ERVA_i$$

(i – кількість рядків IMECA таблиці)





Розраховуються значення показників **IVR**, **EVR**, як сума значень відповідних RVA_i (початкового значення - $IRVA_i$ та кінцевого значення після застосування контрзаходів - $ERVA_i$)

МЕТОДОЛОГІЧНІ ОСНОВИ СТВОРЕННЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ У ГАЛУЗІ ПІДГОТОВКИ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ (1)

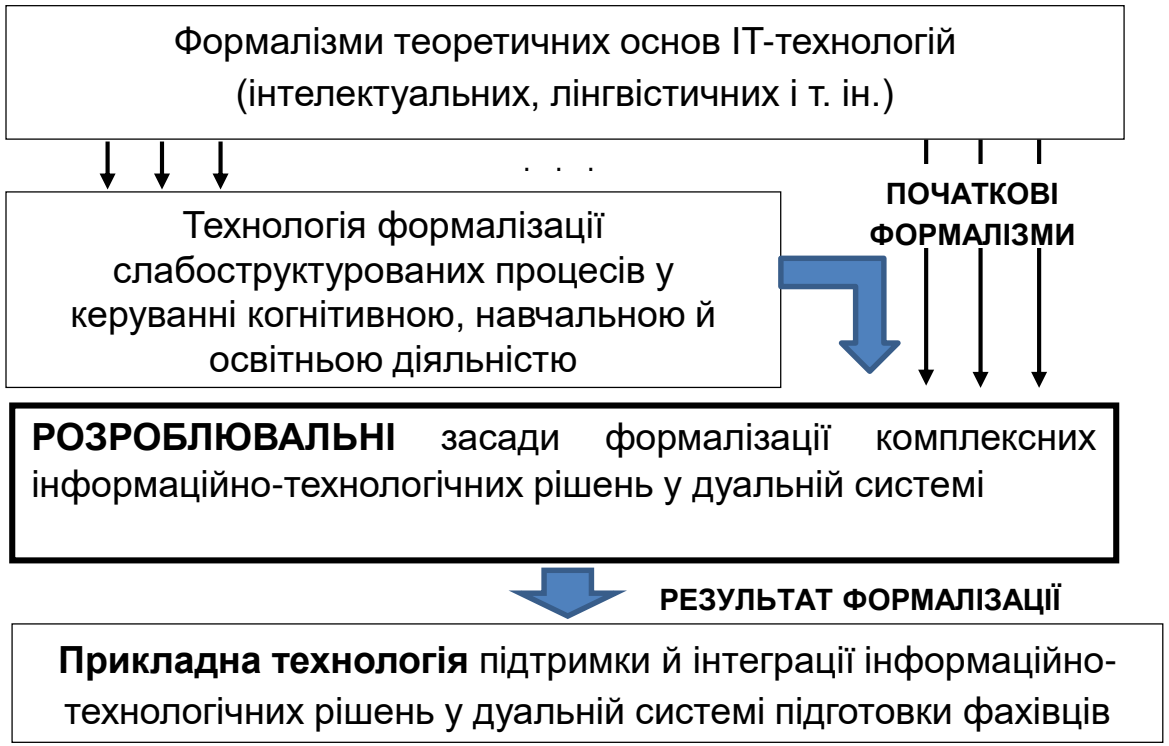


Рисунок 15.1 – Узагальнена модель основ формалізації

Відмінною особливістю формалізації процесів, що протікають в досліджуваних системах, а також відносин між ними є використання топологічних різноманіть (формальне подання у теорії множин є окремим випадком топологічного різноманіття), що виводять дослідження на новий більш високий рівень абстрагування цих процесів.

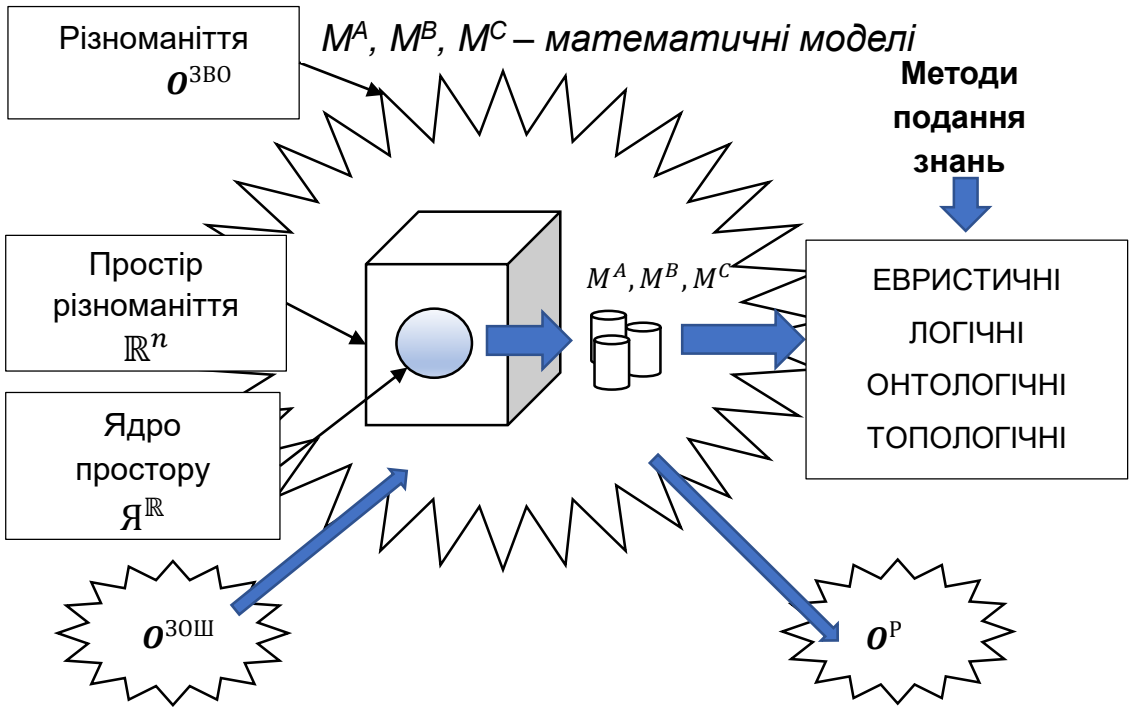
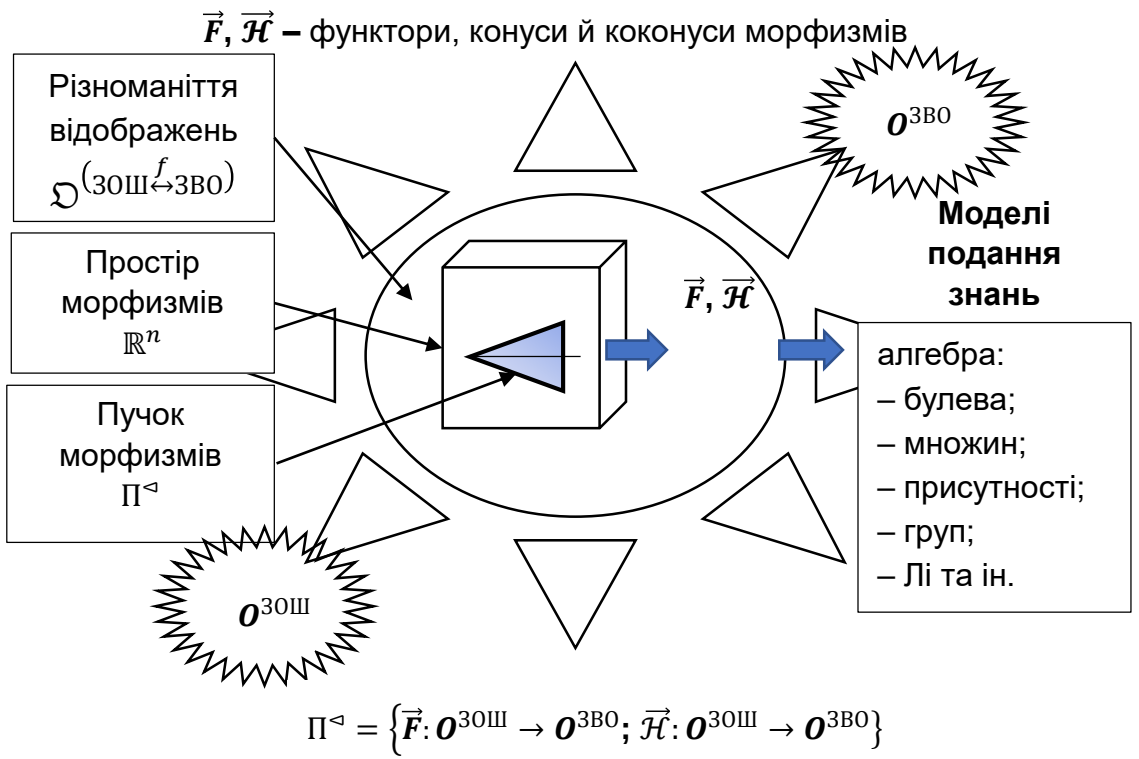


Рисунок 15.2 – Ілюстрація ієрархії формалізмів різноманіття закладів вищої освіти

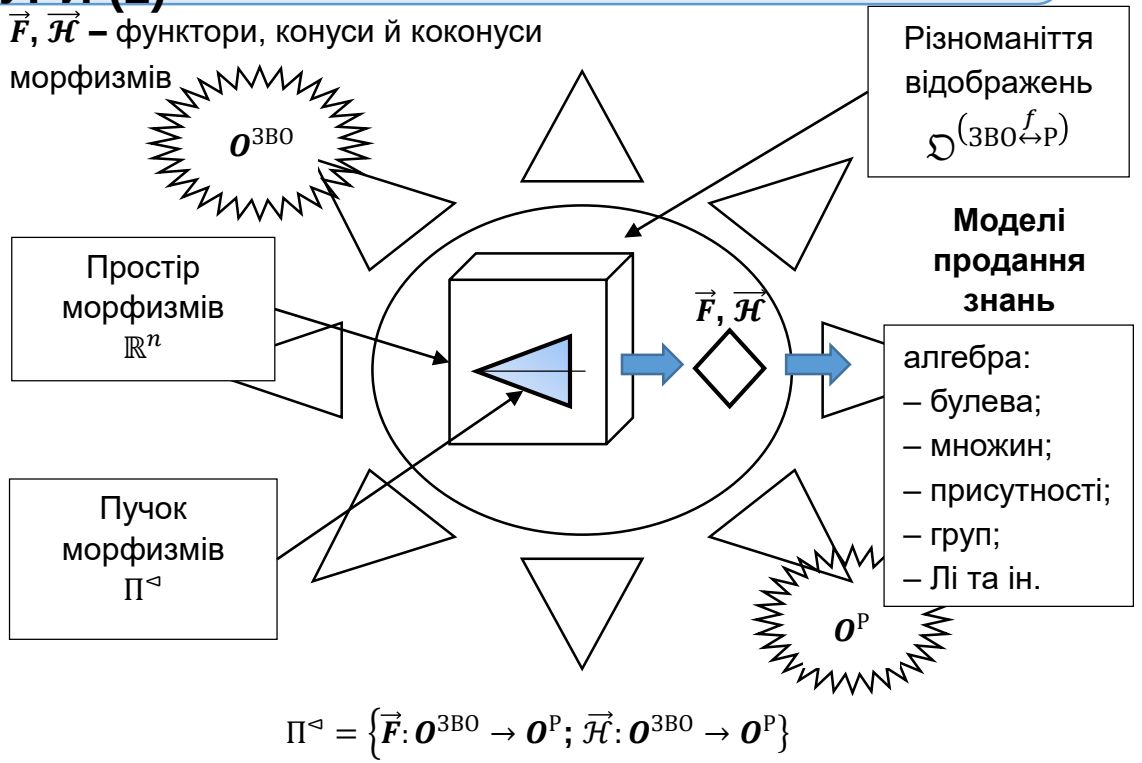
По суті розроблена схема дозволяє задати темпоральні відношення в процесі формалізації, наприклад, опис різноманіття закладів вищої освіти, задати простір $\mathbb{R}^n$, вибрати значущі елементи топологічного простору, тобто сформувати ядро простору $Я^{\mathbb{R}}$, розробити моделі значущих елементів ядра простору $\{M^A, M^B, M^C\}$.

МЕТОДОЛОГІЧНІ ОСНОВИ СТВОРЕННЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ У ГАЛУЗІ ПІДГОТОВКИ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ (2)



$$\Pi^{\triangleleft} = \left\{\vec{F}: O^{\text{ЗОШ}} \to O^{\text{ЗВО}}; \vec{\mathcal{H}}: O^{\text{ЗОШ}} \to O^{\text{ЗВО}}\right\}$$

Рисунок 16.1 – Графічна та аналітична інтерпретація різноманіття відображень процесів, які відбуваються між загальноосвітніми школами та закладами вищої освіти



$$\Pi^{\triangleleft} = \left\{\vec{F}: O^{\text{ЗВО}} \to O^{\text{Р}}; \vec{\mathcal{H}}: O^{\text{ЗВО}} \to O^{\text{Р}}\right\}$$

Рисунок 16.2 – Графічна та аналітична інтерпретація різноманіття відображень процесів, які відбуваються між закладами вищої освіти та роботодавцями

Де символами $O^{\text{ЗОЗ}}, O^{\text{ЗВО}}, O^{\text{Р}}$ позначено різноманіття процесів, що протікають в освітніх системах ($O^{\text{ЗОШ}}$ – загальноосвітні школи (ЗОШ); $O^{\text{ЗВО}}$ – заклади вищої освіти (ЗВО)) та виробничих системах $O^{\text{Р}}$ (роботодавці (Р)), відповідно;

$\mathfrak{O}^{\left(\text{ЗОШ}\overset{f}{\leftrightarrow}\text{ЗВО}\right)}$ – відображення процесів, які відбуваються між загальноосвітніми школами й закладами вищої освіти;

$\mathfrak{O}^{\left(\text{ЗВО}\overset{f}{\leftrightarrow}\text{Р}\right)}$ – відображення процесів, які відбуваються між закладами вищої освіти й роботодавцями

ЦИФРОВА ПЛАТФОРМА ЗДОБУТТЯ ПРОФЕСІЙНИХ ЗНАНЬ ПРИ ПІДГОТОВЦІ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Під терміном «цифрова платформа здобуття професійних знань» (ЦПЗПЗ) будемо розуміти спеціальним чином організовані й взаємозв'язані між собою моделі професійних знань з основної і суміжних спеціальностей, які ізоморфно відображають зміст навчальних програм навчального плану. Відмінною рисою пропонованої ЦПЗПЗ є те, що навчальна інформація у вигляді моделей класифікується і систематизується відповідно до навчальних планів конкретних спеціальностей.

Рисунок 17.1 – Узагальнена схема побудови моделі професійних знань

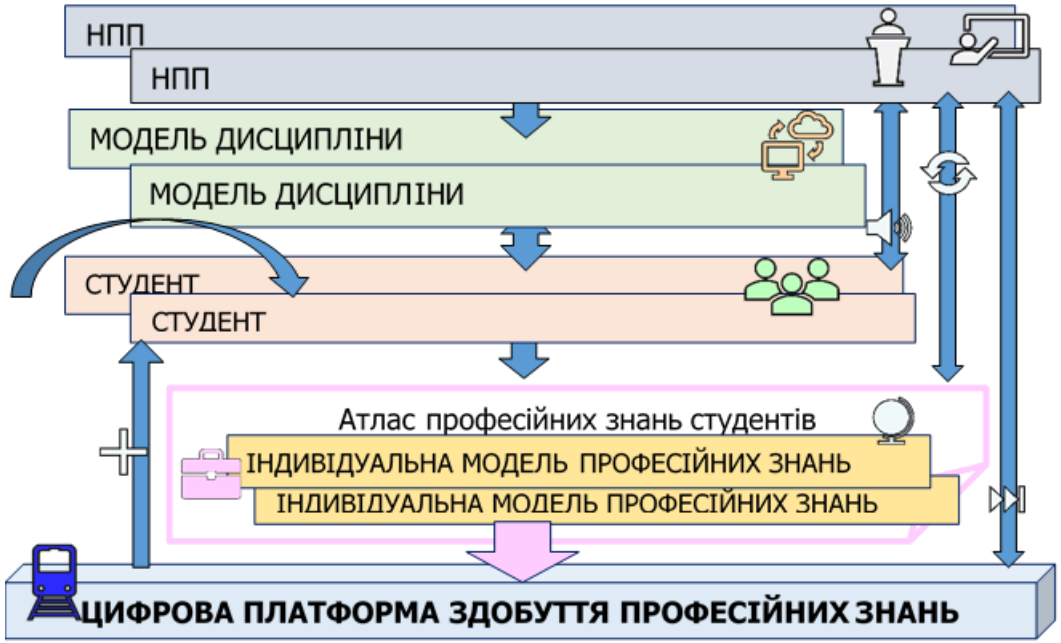


Рисунок 17.2 – Узагальнена схема побудови моделі професійних знань

Модель професійних знань будується за наступною формулою:

$$M_{ПЗ}^{ПІБ} = \langle D, P, S, O, \Omega, T \rangle,$$

де $M_{ПЗ}^{ПІБ}$ – індивідуальна (прізвище, ім'я, по батькові) модель професійних знань студента; P – множина вивчених дисциплін; S – множина практичних занять, включаючи практики; O – множина технічних засобів навчання; D – множина оцінок і самооцінок; Ω – множина відносин між елементами $d \in D, p \in P, s \in S$; T – множина темпоральних відносин, які утворюються між множинами моделі.

РЕЗУЛЬТАТИ НАУКОВОЇ РОБОТИ

Комплекс науково-прикладних задач розроблення моделей, методів і технологій забезпечення кібербезпеки мобільних операційних систем, вебсистем критичної інфраструктури, флотів безпілотних апаратів, що забезпечують їх взаємодію, та методології підготовки фахівців з кібербезпеки комп’ютерних систем і мереж об'єктів критичної інфраструктури.

ВИРІШЕНО

1. Запропоновано концепцію та принципи забезпечення кібербезпеки комп’ютерних систем і мереж об'єктів критичної інфраструктури.

2. Розроблено модель згорткової нейронної мережі на основі використання змішаних даних, а також метод виявлення шкідливого програмного забезпечення в Android-сумісних мобільних операційних системах для об'єктів критичної інфраструктури.

3. Розроблено методи оцінювання та забезпечення кібербезпеки вебсистем критичної інфраструктури на основі систем керування вмістом шляхом використання дерев атак.

4. Розроблено модель та методи забезпечення кібербезпеки флотів безпілотних апаратів, які враховують особливості їхньої багатофункціональної структури, динаміку взаємодії між окремими компонентами системи та зовнішніми середовищами, а також забезпечують захист від різноманітних одиничних і комбінованих атак.

5. Розроблено методологічні основи створення інформаційної технології й модель цифрової платформи знань для використання в дуальній системі підготовки фахівців з кібербезпеки комп`ютерних систем і мереж об'єктів критичної інфраструктури.

6. Впроваджено методи технологій забезпечення кібербезпеки комп`ютерних систем і мереж об'єктів критичної інфраструктури.

ДОЗВОЛИЛО

Розробити та впровадити відповідні моделі, методи та технології забезпечення кібербезпеки комп’ютерних систем і мереж об'єктів критичної інфраструктури у сфері інформаційних та телекомунікаційних технологій, машинобудуванні, оборонної та авіаційної промисловості, а також у закладах вищої освіти під час розробки навчальних курсів і модулів для підготовки фахівців з кібербезпеки комп’ютерних систем і мереж об'єктів критичної інфраструктури.

ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ ДОСЛІДЖЕНЬ І РОЗРОБОК

Галузі, підприємства (організації), системи			Основні результати досліджень і розробок								
			Модель згорткової нейронної мережі на основі використання змішаних даних	Метод виявлення шкідливого програмного забезпечення в Android-сумісних мобільних операційних системах для об'єктів критичної інфраструктури	Метод забезпечення кібербезпеки вебсистем критичної інфраструктури на основі систем керування вмістом	Метод оцінювання кібербезпеки систем керування вмістом шляхом використання дерев атак	Модель кіберфізичної системи багатофункційних флотів безпілотних апаратів, як об'єкта оцінювання кібербезпеки	Модель комбінованих послідовно-паралельних кібератак різними порушниками і засобами	Метод вибору контрзаходів для забезпечення кібербезпеки кіберфізичної системи багатофункційних флотів безпілотних апаратів	Методологічні основи інформаційної технології для дуальної системи підготовки фахівців з кібербезпеки комп'ютерних систем і мереж об'єктів критичної інфраструктури	Модель цифрової платформи підтримки процесів здобуття професійних знань
1	2	3	4	5	6	7	8	9	10	11	12
Інформаційні технології	ПП «Авіві»	Цифрова освітня платформа			+				+		+
	ТОВ «ІТТ»	Система виявлення вторгнень	+	+							
	ТОВ «GMhost»	Автоматизована система вибору заходів кіберзахисту			+	+					
Машинобудування	АТ «ФЕД»	Повний цикл створення сучасного авіаційного агрегату								+	+
Оборонна галузь	Харківський національний університет Повітряних Сил імені Івана Кожедуба	Система виявлення вразливостей					+	+	+		
Вища освіта	Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ», Хмельницький національний університет	Навчальний процес	+	+	+	+	+	+	+	+	+
Міжнародні проекти	Освітні проекти TEMPUS	SEREIN, CABRIOLET			+	+				+	+
	Освітній проект ERASMUS+	ALIOT			+	+	+	+	+	+	+
	Науковий проект Horizon 2020	ECHO			+	+				+	+

РЕЗУЛЬТАТИ ВПРОВАДЖЕННЯ

Досягнуто значення достовірності виявлення шкідливого програмного забезпечення в мобільній операційній системі Android на рівні 0,933% та зменшити показник хибних спрацювань до 3,3%, у порівнянні із відомими методами виявлення шкідливого програмного забезпечення в мобільній операційній системі Android.

Забезпечено допустиме значення показника успішності атак при мінімальній вартості й вибрати заходи захисту, враховуючи їх вплив на показник успішності атак та вартість, а саме використання методів на прикладі однієї інсталяції системи керування вмістом дозволило зменшити значення показника успішності атаки на 42,3%.

Забезпечено підвищення кібербезпеки багатофункціональних флотів безпілотних апаратів, збільшивши ефективність виявлення атак на 35% і знизивши час реагування на кіберзагрози на 40% завдяки впровадженню інтегрованої моделі загроз і алгоритмам адаптивного вибору контрзаходів.

Підвищено ефективність підготовки фахівців з кібербезпеки комп`ютерних систем і мереж об'єктів критичної інфраструктури, зокрема експериментальна перевірка свідчить, що абсолютна успішність унаслідок впровадження запропонованої інформаційної технології в навчальний процес, збільшилися на 4%, а якісна успішність – на 14% відповідно.

ПУБЛІКАЦІЇ ПРЕТЕНДЕНТІВ

Загальна кількість публікацій – 111. Серед них: 1 одноосібна монографія, 7 колективних монографій, у т.ч. 5 у зарубіжних виданнях, 4 посібників, 51 стаття в журналах, включених до категорії "А" Переліку наукових фахових видань України та у закордонних виданнях, проіндексованих у базах даних Web of Science Core Collection та/або Scopus (у т.ч. 38 у зарубіжних виданнях) та 37 статей у журналах, включених до категорії "Б" Переліку наукових фахових видань України, 7 тез доповідей.

Загальна кількість посилань на публікації авторів/h-індекс за роботою згідно з базами даних складає відповідно: Web of Science 51/4, Scopus 341/11, Google Scholar 550/12.

Отримано 4 патенти на корисну модель.

ЦИТУВАННЯ ПУБЛІКАЦІЙ ПРЕТЕНДЕНТІВ

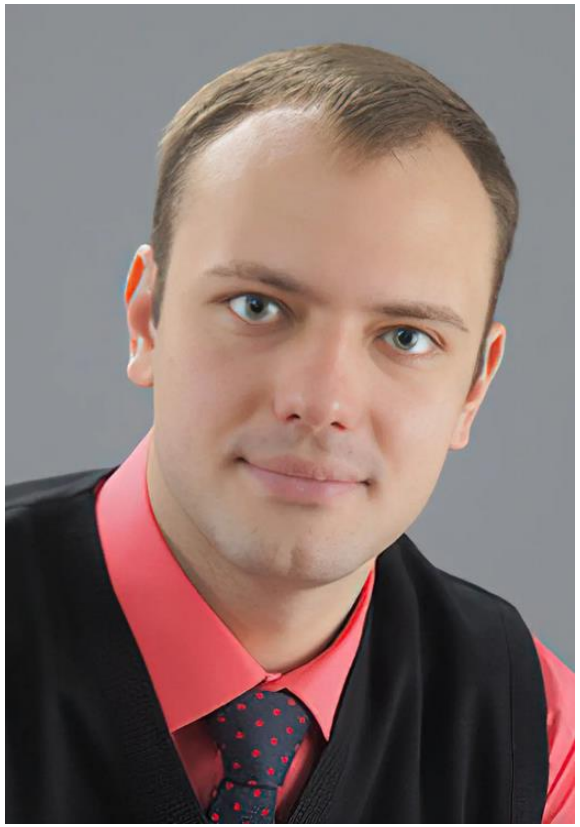
	Кількість посилань згідно бази даних		
	Web of Science	Scopus	Google Scholar
Загальна кількість цитувань	51	347	550
h-індекс робіт	4	11	12
кількість посилань / h-індекс авторів			
Землянко Г. А.	-/-	16/3	52/5
Морозова О. І.	62/4	141/7	271/8
Нічепорук А. О.	1/1	197/8	273/8
Тецький А. Г.	-/-	46/4	97/5

АВТОРСЬКИЙ КОЛЕКТИВ

Землянко Георгій Андрійович
д-р філос. (PhD), ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут».
E-mail: g.zemlynko@csn.khai.edu

Морозова Ольга Ігорівна,
д.т.н., професор, професор кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут».
E-mail: o.morozova@csn.khai.edu

Нічепорук Андрій Олександрович
к.т.н., доцент, доцент кафедри комп’ютерної інженерії та інформаційних системХмельницького національного університету.
E-mail:
andrey.nicheporuk@khnu.km.ua



Тецький Артем Григорович
к.т.н., доцент кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут».
E-mail: a.tetskiy@csn.khai.edu