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 індустріальних і веб-орієнтованих систем і мереж

Автори:

1. **МОРОЗОВА Ольга Ігорівна** – доктор технічних наук, доцент, професор Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут».

2. **НІЧЕПОРУК Андрій Олександрович** – кандидат технічних наук, доцент, доцент Хмельницького національного університету.

3. **ТЕЦЬКИЙ Артем Григорович** – кандидат технічних наук, старший викладач Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут».

4. **ТКАЧОВ Віталій Миколайович** – кандидат технічних наук, доцент Харківського національного університету радіоелектроніки.

Харків – 2021

ОСНОВНІ ПОЛОЖЕННЯ ДОСЛІДЖЕННЯ

Мета роботи

Забезпечення кібербезпеки індустріальних і веб-орієнтованих систем і мереж шляхом розроблення та впровадження відповідної методології (концепції, принципів, комплексу моделей, методів) і технологій в індустрії, а також при підготовці фахівців з кібербезпеки під час здобуття професійних знань.

Науково-прикладна задача

Розроблення моделей, методів і технологій забезпечення кібербезпеки мобільних систем, веб-орієнтованих систем на основі систем керування вмістом, віртуальних мереж, що забезпечують їх взаємодію, та методології підготовки фахівців з кібербезпеки.

Завдання дослідження

1. Запропонувати концепцію та принципи забезпечення кібербезпеки індустріальних і веб-орієнтованих систем і мереж.

2. Розробити модель згорткової нейронної мережі на основі використання змішаних даних та метод виявлення шкідливого програмного забезпечення в операційній системі Android на основі опрацювання викликів прикладного програмного інтерфейсу (API) та набору дозволів.

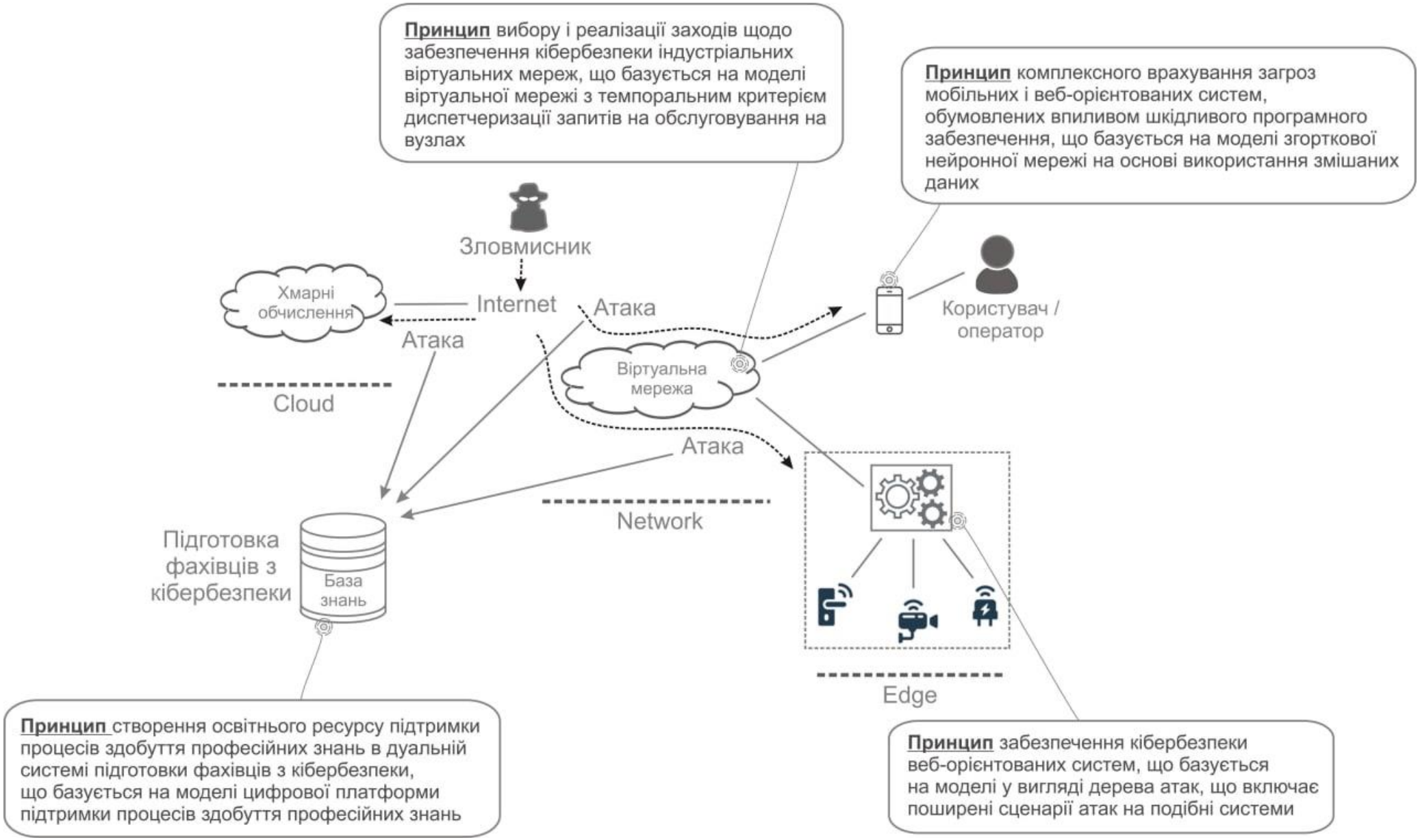
3. Розробити методи інформаційної технології забезпечення кібербезпеки веб-орієнтованих систем на основі систем керування вмістом, засновані на оцінюванні схильності до поширених сценаріїв атак та виборі найбільш ефективних засобів захисту.

4. Розробити моделі та методи забезпечення кібербезпеки віртуальних мереж, засновані на використанні концепції віртуального тунелювання в мережі Інтернет

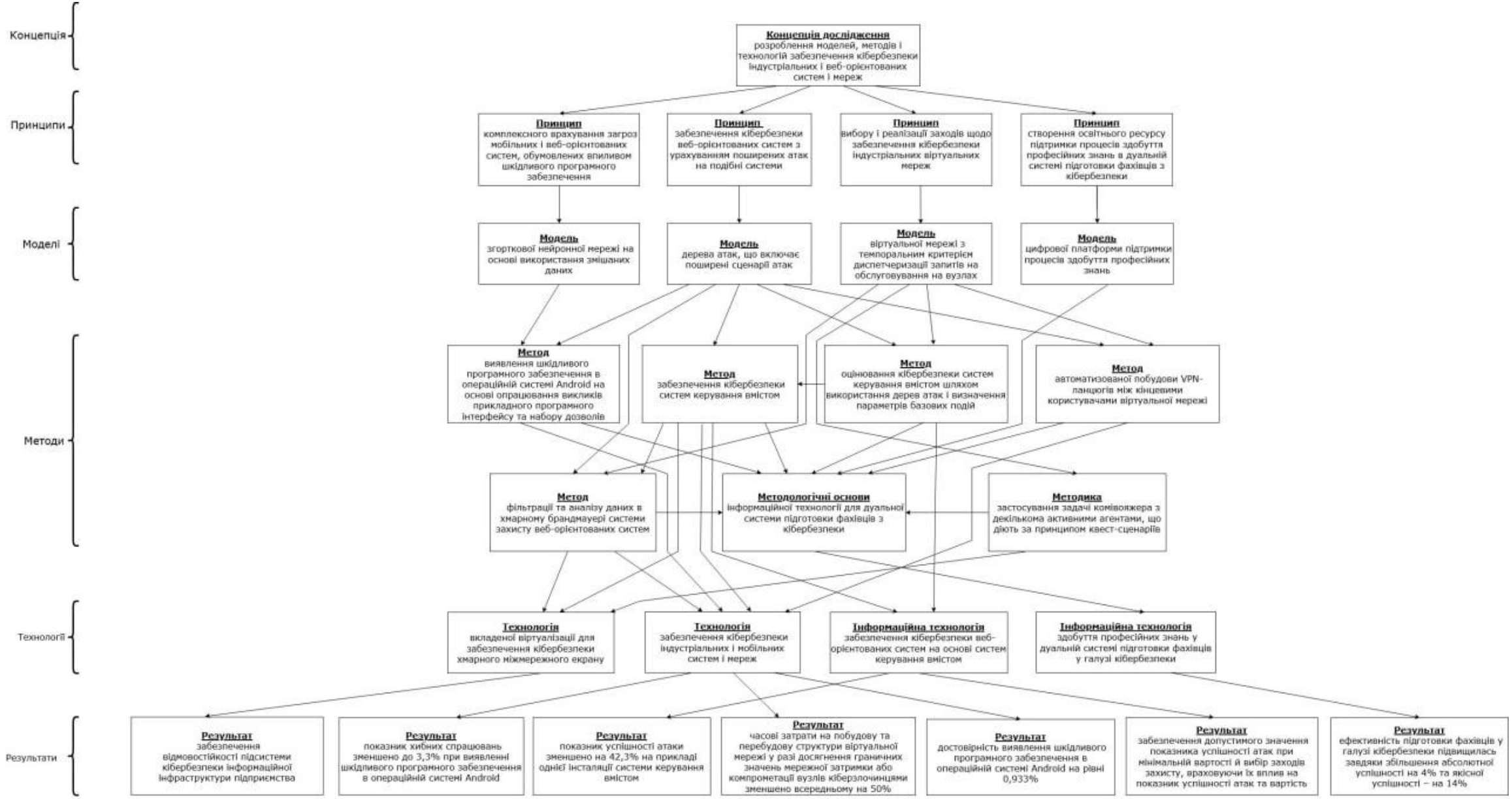
5. Розробити методологічні основи створення інформаційної технології та модель цифрової платформи знань для використання в дуальній системі підготовки фахівців під час здобуття професійних знань.

6. Впровадити методи технологій забезпечення кібербезпеки індустріальних і веб-орієнтованих систем і мереж.

ПРЕДМЕТНА ОБЛАСТЬ ДОСЛІДЖЕННЯ



СТРУКТУРА ТА ВЗАЄМОЗВ'ЯЗОК ЕЛЕМЕНТІВ МЕТОДОЛОГІЇ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ІНДУСТРІАЛЬНИХ І ВЕБ-ОРІЄНТОВАНИХ СИСТЕМ І МЕРЕЖ



МЕТОД ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В ОПЕРАЦІЙНІЙ СИСТЕМІ ANDROID НА ОСНОВІ ОПРАЦЮВАННЯ ВИКЛИКІВ ПРИКЛАДНОГО ПРОГРАМНОГО ІНТЕРФЕЙСУ ТА НАБОРУ ДОЗВОЛІВ

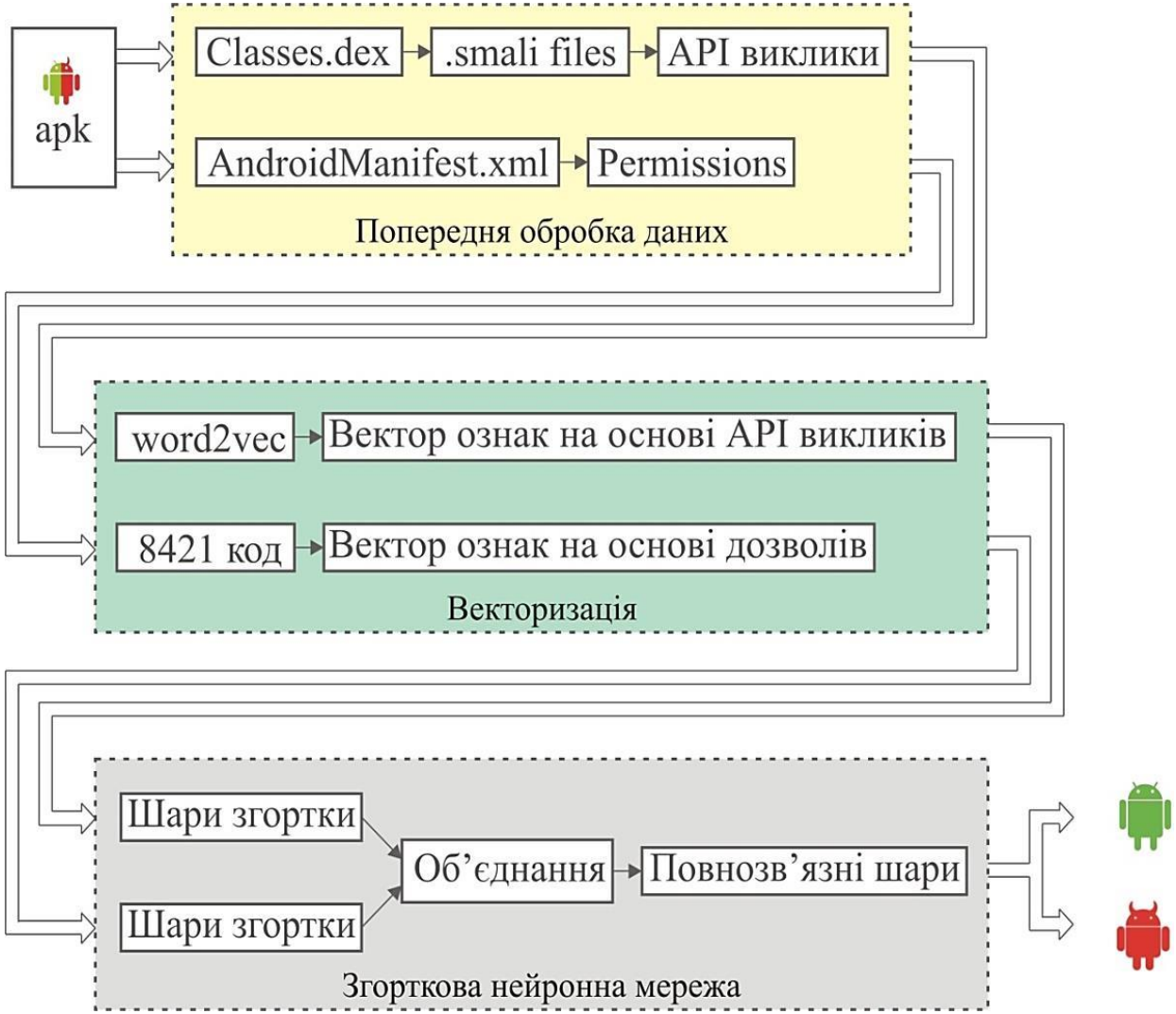


Рисунок 5.1 – Узагальнена структура методу виявлення шкідливого програмного забезпечення в операційній системі Android на основі опрацювання викликів прикладного програмного інтерфейсу (API) та набору дозволів

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 ← M_i
  foreach S_i **in** *PointsToBeProcessed* **do**
    foreach *Instruction* **in** S_i **do**
      if *Instruction* ∈ (invoke-* = android, java, javax)
        API ← *Instruction*
      if *Instruction* ∈ ReferencesToCustomMethodCall
        PointsToBeProcessed ← *Instruction*
  return *API*
end

Рисунок 5.2 – Алгоритм отримання API викликів зі smali файлів

МЕТОД ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В ОПЕРАЦІЙНІЙ СИСТЕМІ ANDROID НА ОСНОВІ ОПРАЦЮВАННЯ ВИКЛИКІВ ПРИКЛАДНОГО ПРОГРАМНОГО ІНТЕРФЕЙСУ ТА НАБОРУ ДОЗВОЛІВ

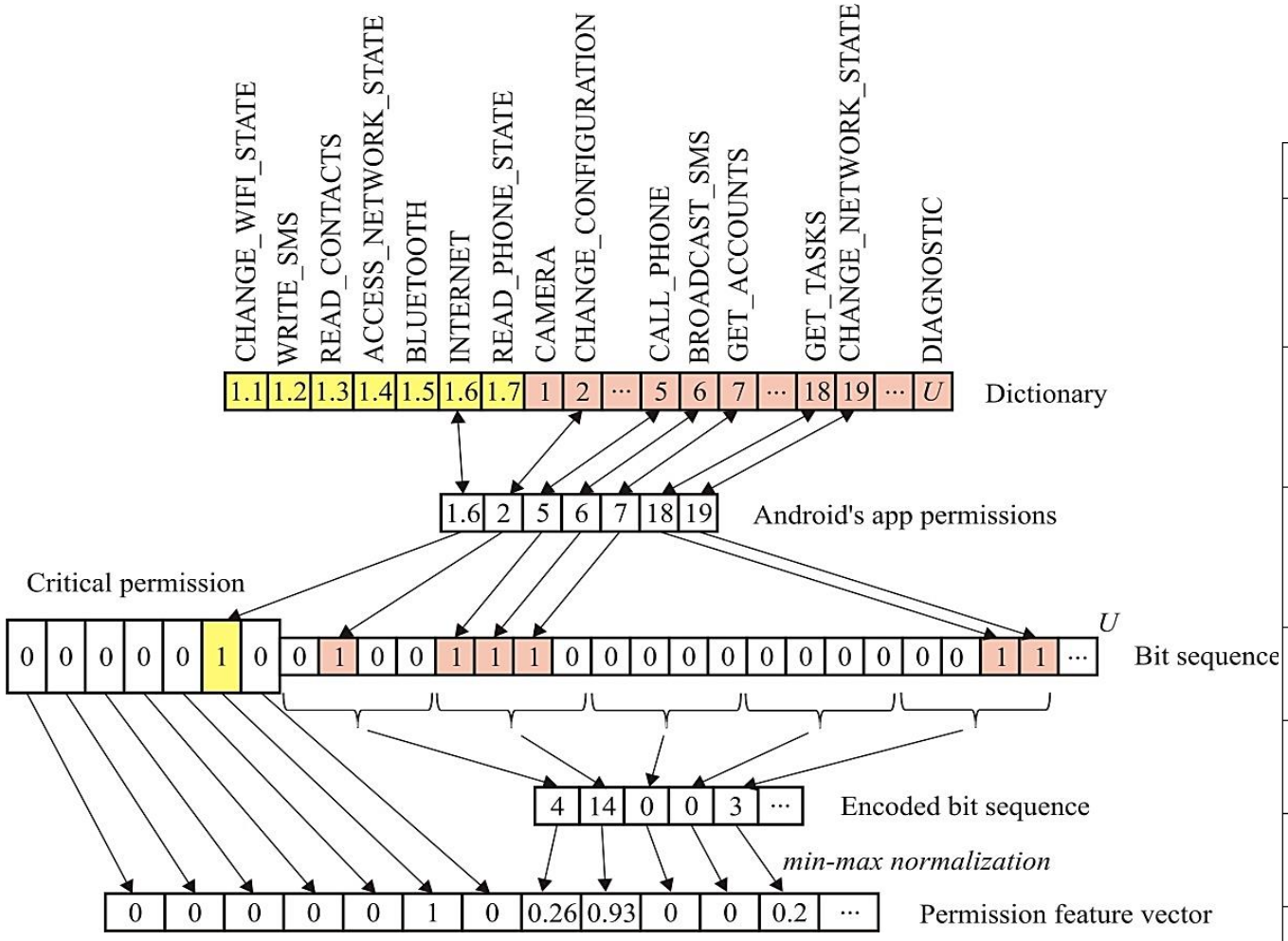


Рисунок 6 – Процес представлення множини дозволів додатку Android у вигляді вектора ознак

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

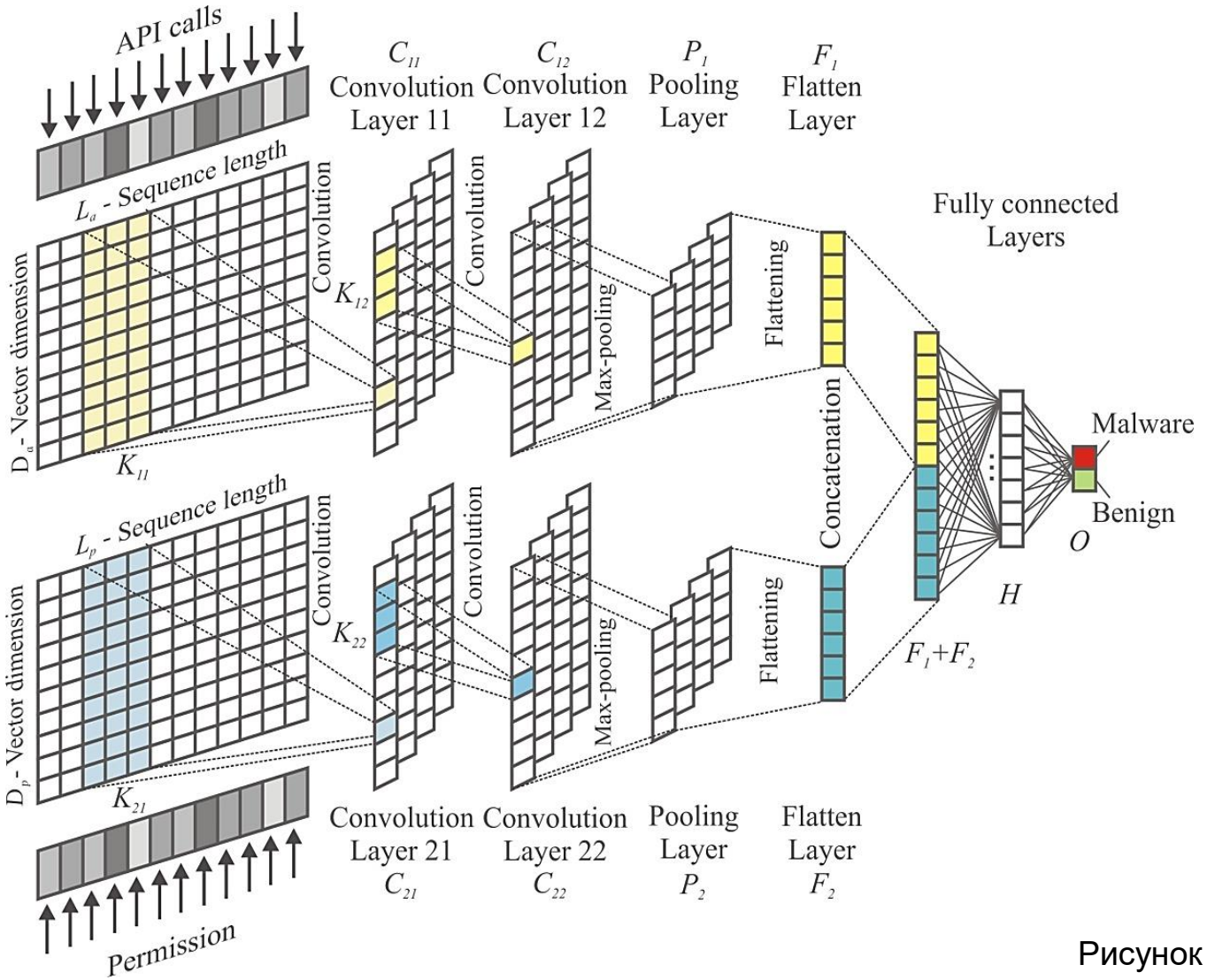


Рисунок 7.1 – Модель згорткової нейронної мережі на основі використання змішаних даних

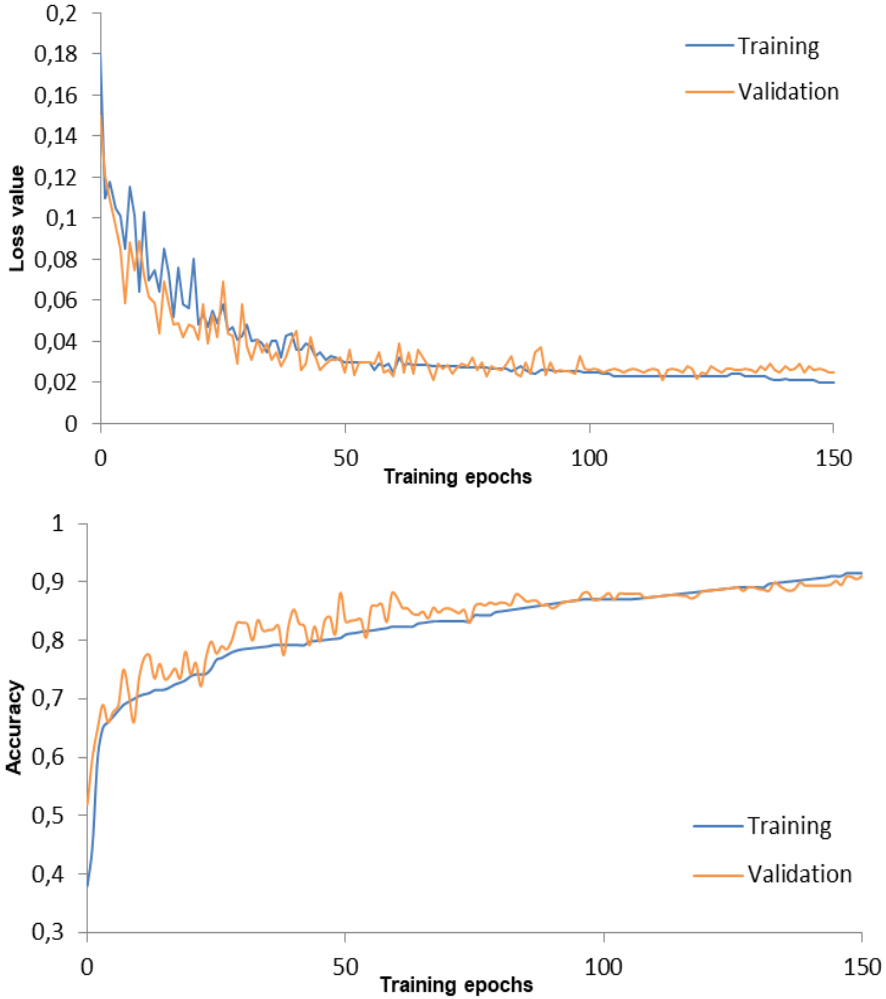


Рисунок 7.2 – Параметри навчання та валідації нейронної мережі: а) функція втрат; б) значення достовірності

МЕТОД ОЦІНЮВАННЯ КІБЕРБЕЗПЕКИ ВЕБ-СИСТЕМ НА ОСНОВІ СИСТЕМ КЕРУВАННЯ ВМІСТОМ

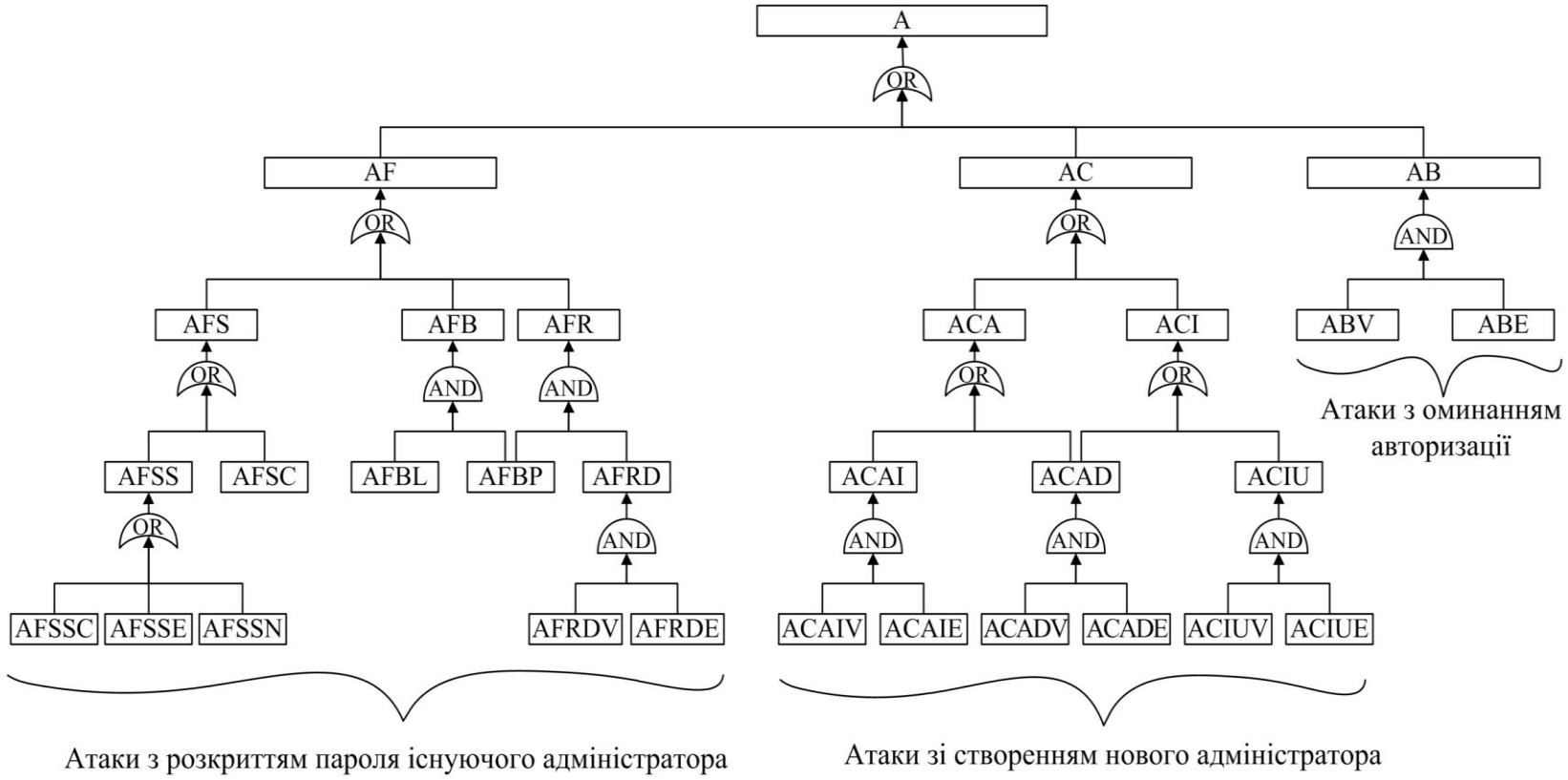


Рисунок 8 – Дерево атак на систему керування вмістом, на якому базується метод

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 ВЕБ-СИСТЕМ ШЛЯХОМ ВИБОРУ ЗАХОДІВ ЗАХИСТУ

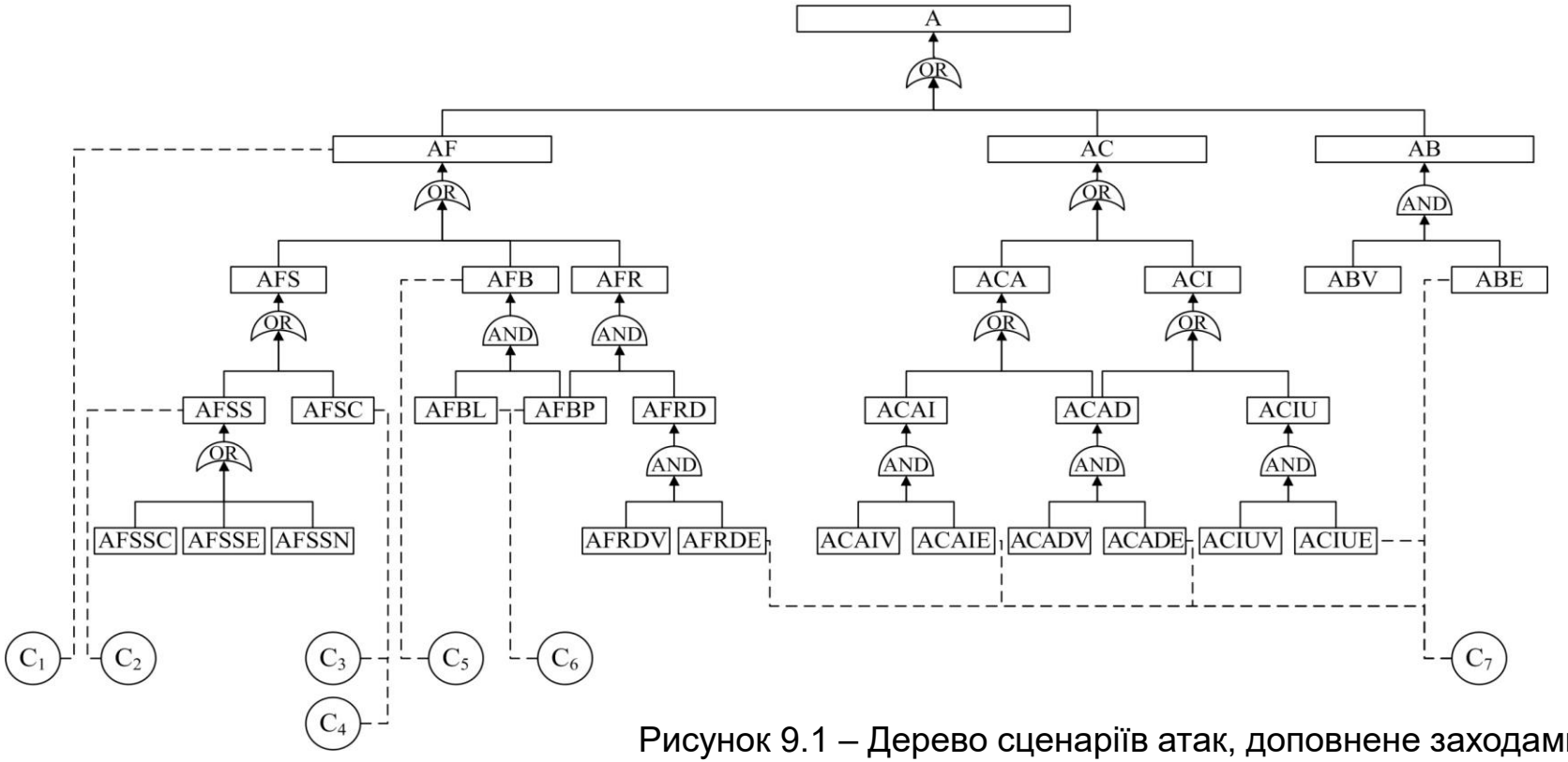


Рисунок 9.1 – Дерево сценаріїв атак, доповнене заходами захисту

Таблиця 6.1. 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

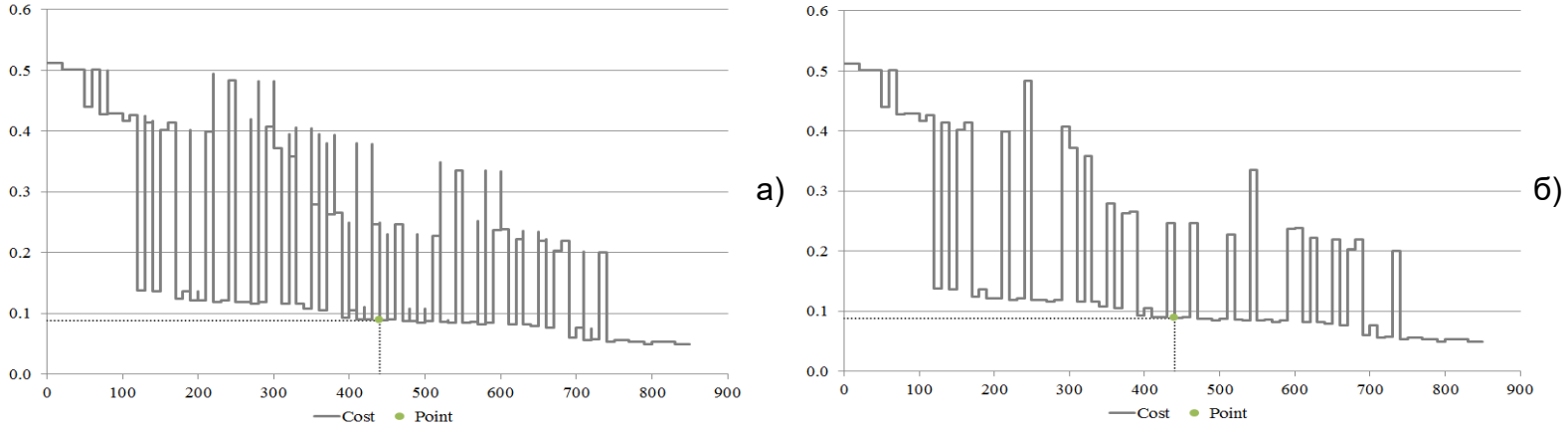


Рисунок 9.2 – Графік залежності показника успішності атаки від бюджету:
а) усі комбінації контрзаходів
б) найефективніші комбінації

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ВЕБ-ОРІЄНТОВАНИХ СИСТЕМ

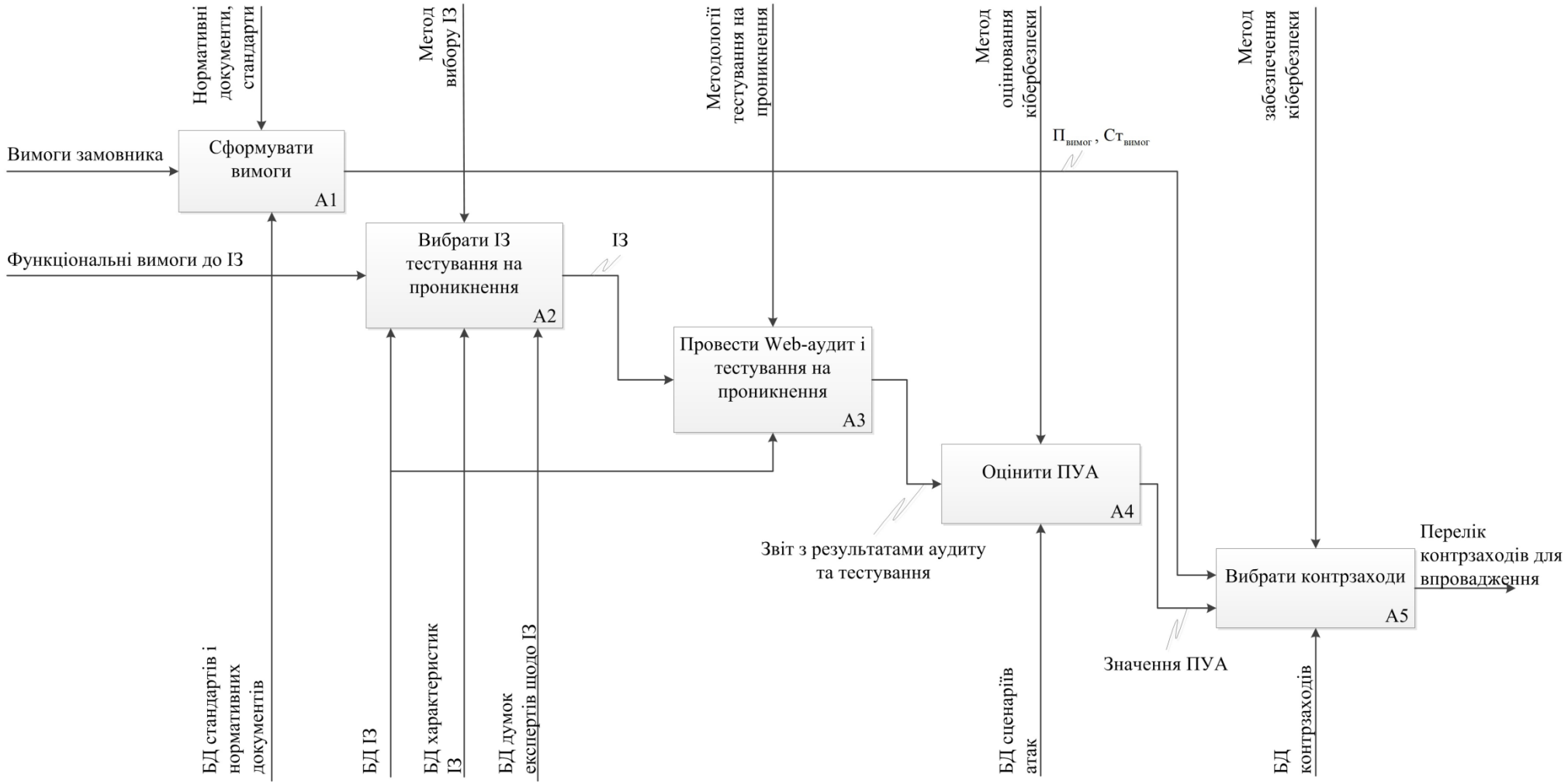


Рисунок 10 – Вузол А0 – Вибрати заходи захисту, враховуючи їх вплив на показник успішності атаки

МОДЕЛІ ВІРТУАЛЬНОЇ МЕРЕЖІ

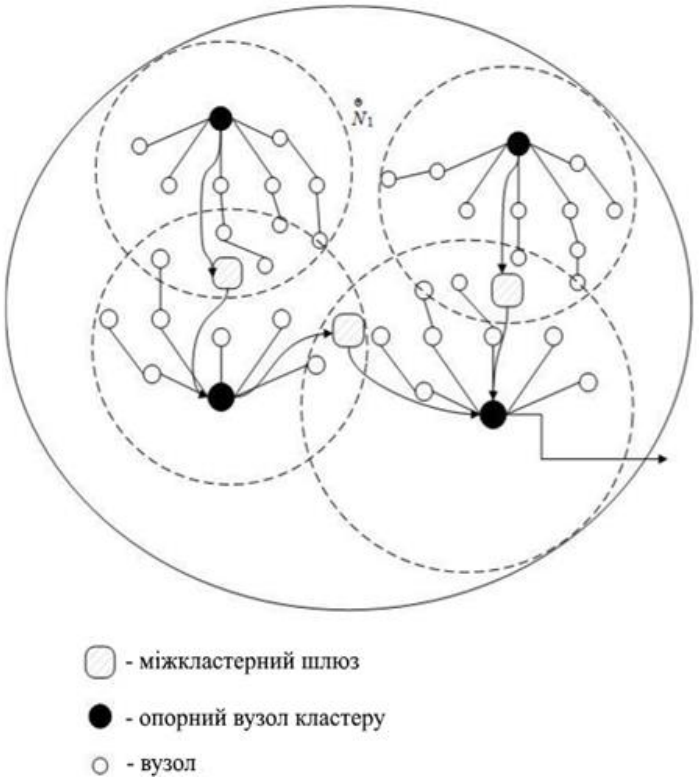


Рисунок 11 – Графова модель віртуальної мережі

Організація передачі даних усередині СВМ з багатоінтервальною кластеризацією через міжкластерні шлюзи на представленій графовій моделі віртуальної мережі

Модель віртуальної мережі з темпоральним критерієм диспетчеризації запитів на обслуговування

Модель обробки запитів на обслуговування в вузлах віртуальної мережі з застосуванням змін темпорального критерію:

$$L(t) = \langle W_1(t), W_2(t),\ K_{ТБ}, T_1, T_2 \rangle$$

Запропонована модель функціонування віртуальної мережі передбачає отримання субоптимальних рішень задачі обслуговування запитів в вузлах мережі, які відповідають темпоральним критеріям:

$$K_{ТБ} = \sum_{j=1}^{J} \beta_j(t) \Delta I_{xjU} - \sum_{v=1}^{V} \gamma_v(t) \Delta z_v \to \max$$

Рішення, які повинні задовольняти інформаційним критеріям і обмеженням отримаємо із застосуванням відповідних функцій для визначення невизначених множників Лагранжа:

$$\beta_j = \beta_j(t, W(G), S, C),\ \ \gamma_v = \gamma_v(t, W(G), S, C) \ \text{ для } \ j = \overline{1, J}\ ,\ \ v = \overline{1, V}$$

Для вирішення задачі про вибір параметрів розглянутої моделі функціонування, можуть бути використані, наприклад, реальні навчальні вибірки обмеженого обсягу або експертні оцінки.

МЕТОДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ВІРТУАЛЬНОЇ МЕРЕЖІ (1)

Квест-метод аналізу віртуальних мереж

Математичний опис роботи вузла віртуальної мережі:

$$a_0 \frac{d^n y}{dt^n} + a_1 \frac{d^{n-1} y}{dt^{n-1}} + \ldots + a_n y = b_0 \frac{d^m x}{dt^m} + b_1 \frac{d^{m-1} x}{dt^{m-1}} + \ldots + b_m x$$

Представлення завдання аналізу в термінах лінійного цілочисельного програмування при обмеженнях виду:

$$\begin{cases} T \geq \sum_{u=1}^{n} k_{f,u} t_u, \ u = 1,2,\ldots,M; \\ \sum_{u=1}^{M} k_{f,u} = 1, \ f = 1,2,\ldots,n; \\ \sum_{u=1}^{m} k_{f,u} \geq \sum_{j=1}^{m} k_{l,u}, m = 1,2,\ldots,M, \ f \prec l; \\ k_{f,u} \geq 0; \\ T \geq 0; \\ E(k_{f,u}) = k_{f,u}. \end{cases}$$

Умова вибору вузла при квест-переході ПА в віртуальній мережі:

$$H_{u_n} = t_{u_n \to u_{n+m}} - (f_r \times g) - \zeta$$

Розрахунок часу для кожного вузла на кожному кроці (крім визначення u_{finish}).

$$\begin{cases} t_{u_n \to u_{n+m}} \geq f_r(g+1), \ при \ g = 0,1,2,\ldots \Rightarrow \\ \Rightarrow H_{u_n} = t_{u_n \to u_{n+m}} + f_r; \\ t_{u_n \to u_{n+m}} < f_r(g+1), \ при \ g = 0 \Rightarrow \\ \Rightarrow H_{u_n} = t_{u_n \to u_{n+m}} + f_r; \\ t_{u_n \to u_{n+m}} < f_r(g+1), \ при \ g = 1,2,\ldots \Rightarrow \\ \Rightarrow H_{u_n} = f_r(g+1). \end{cases}$$

Метод фільтрації запитів у віртуальних мережах хмарним брандмауером

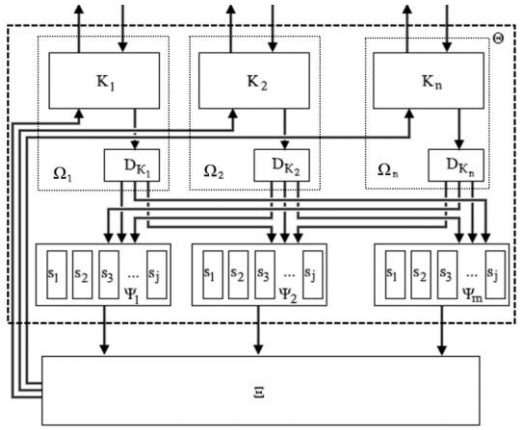


Рисунок 12 – Структурна схема хмарного брандмауера

Математичне представлення хмарного брандмауера у вигляді кортежу:

$$\Theta = \langle K_n, D_{K_n}, \Psi_m \rangle$$

Ефективність роботи гіпервізора хмарного серверу при виконанні завдань брандмауернінга:

$$\Psi(u_1, u_2, \ldots, u_S) = \sum_{s=1}^{S} B_s * v_s$$

при

$$B_s = \frac{\varphi_s \left(\sum u_s + 1 \right)}{\mu_0 u_s \left(\frac{\mu_0 u_s}{\sum u_s + 1} - \varphi_s \right)}$$

МЕТОДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ВІРТУАЛЬНОЇ МЕРЕЖІ (2)

Метод автоматизованої побудови VPN-ланцюгів між вузлами віртуальної мережі термінальної системи

Математичний опис постановки задачі:

$$T_{(x\to y)} \to \min, при \begin{cases} T_{(x\to y)} \le T_{protocol} \\ T_{route} \le T_{task} \\ b = 1, 2, n \end{cases}$$

Часова затримка при передачі даних між x-терміналом і y-хостом

$$T_{(x\to y)} = t_{(x\to b_1)} + t_{(x\to b_2)} + \ldots + t_{(x\to b_n)} + t_{(b_n\to y)} + \sum t_{b_n}$$

Часова затримка на побудову маршруту передачі даних між x-терміналом і y-хостом визначається за формулою:

$$T_{route} = t_{route} + \sum t_{communication}$$

Час, що витрачається на побудову квазіоптимального маршруту передачі даних між усіма учасниками віртуальної мережі

$$t_{route} = \begin{cases} t_{(\Theta)} + t_{(\Theta_x+\Theta_y)} + t_{search\min},\ if\ \ b=1; \\ t_{(\Theta_x)} + t_{sort\min\Theta_x} + t_{search\,group\,I},\ if\ \ b=2; \\ t_{(\Theta)} + t_{sort\min\Theta} + t_{search\,group\,II},\ if\ \ b=3; \\ t_{(\Theta)} + t_{sort\min\Theta} + (n-1)\times t'_{sort\min\Theta_{b_n}} + \sum t_{(\Theta_{b_n})} + t_{search\,group\,I},\ якщо\ \ b=4,6,\ldots n,\ n=2k,\ k\in\ \ ; \\ t_{(\Theta)} + t_{sort\min\Theta} + n\times t'_{sort\min\Theta_{b_n}} + \sum t_{(\Theta_{b_n})} + t_{search\,group\,II},\ якщо\ \ b=5,7,\ldots n,\ n=2k+1,\ k\in\ \ ; \end{cases}$$

$$t_{(\Theta)} = \begin{cases} t_{(\Theta_x)},\ if\ t_{(\Theta_x)} \ge t_{(\Theta_y)}; \\ t_{(\Theta_y)},\ if\ t_{(\Theta_y)} \ge t_{(\Theta_x)}; \end{cases}$$

$t_{search\,group\,I}$ – час, що витрачається на пошук першого-ліпшого VPN-сервера, який задовольняє умові:

$$T_{protocol} - t_{(x\to b_1)} - \sum t_{b_n} \ge t_{(b_{n-1}\to b_n)} + t_{(b_n\to y)}$$

$t_{search\,group\,II}$ – час, що витрачається на пошук першого-ліпшого VPN-сервера, який задовольняє умові:

$$T_{protocol} - t_{(x\to b_1)} - \sum t_{b_n} - t_{(b_n\to y)} \ge t_{(b_{n-2}\to b_{n-1})} + t_{(b_{n-1}\to b_n)}$$

МЕТОДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ВІРТУАЛЬНОЇ МЕРЕЖІ (3)

Метод багатошарового VPN-тунелювання при організації віддаленого управління технологічним обладнанням

Загальна пропускна здатність тунелю окремо взятого підключення до комп'ютерної мережі підприємства через VPN-тунель обчислюється аналітично щодо з'єднання «точка-точка»:

$$\Psi = D\ell(2S + (2i-1)\sum_{i=1}^{log_2 S} 2^{i-1}$$

При передачі даних по з'єднанню «точка-бродкаст» (наприклад для широкомовної відправки моніторингової інформації) для кожного з тунелів всім клієнтам VPN-мережі, загальна пропускна здатність може бути представлена у вигляді:

$$\Psi' = D(1 + log_2 S + \sum_{i=1}^{log_2 S} 2^{i} + \ell S)$$

Значення пропускної здатності, яка не ефективно використовується під час передачі від кожного з клієнтів VPN-мережі можна визначити як:

$$\theta = D(\ell S - YW)$$

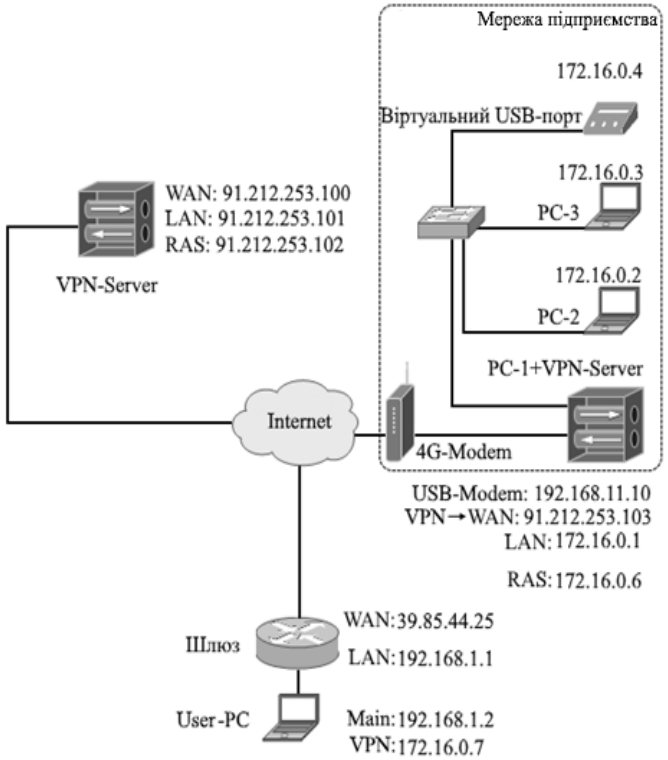


Рисунок 14.1 – Схема мережної взаємодії при наявності пулу реальних IP-адрес (сервісний провайдер)

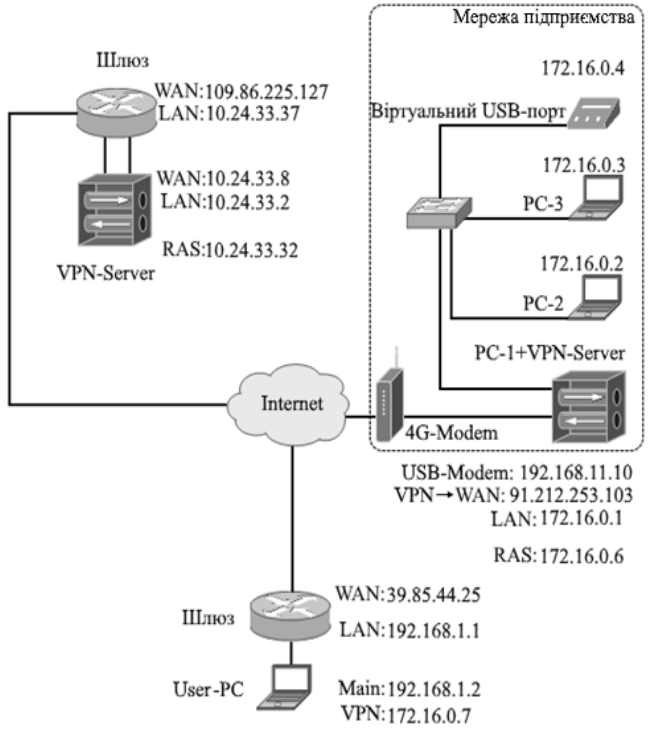


Рисунок 14.2 – Організація віртуальної мережі за наявності однієї реальної IP-адреси

МЕТОДОЛОГІЧНІ ОСНОВИ СТВОРЕННЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ У ГАЛУЗІ ПІДГОТОВКИ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ ТА БЕЗПЕКИ ІНДУСТРІАЛЬНИХ СИСТЕМ (1)

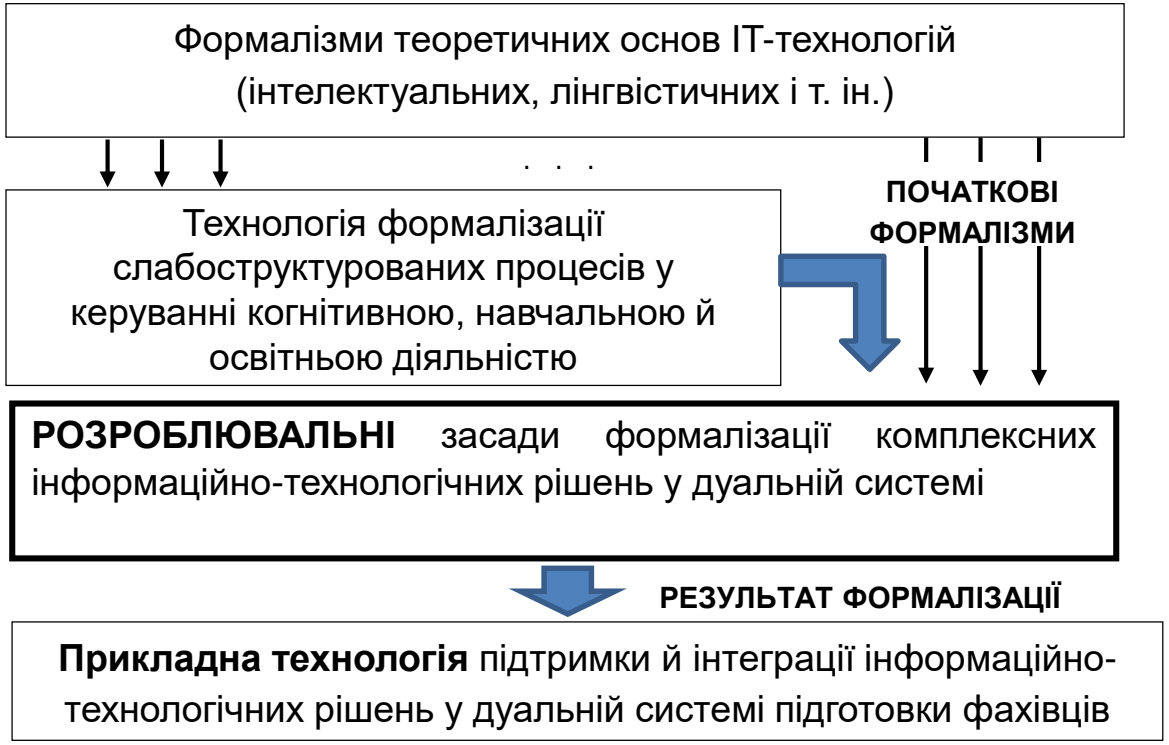


Рисунок 15.1 – Узагальнена модель основ формалізації

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.

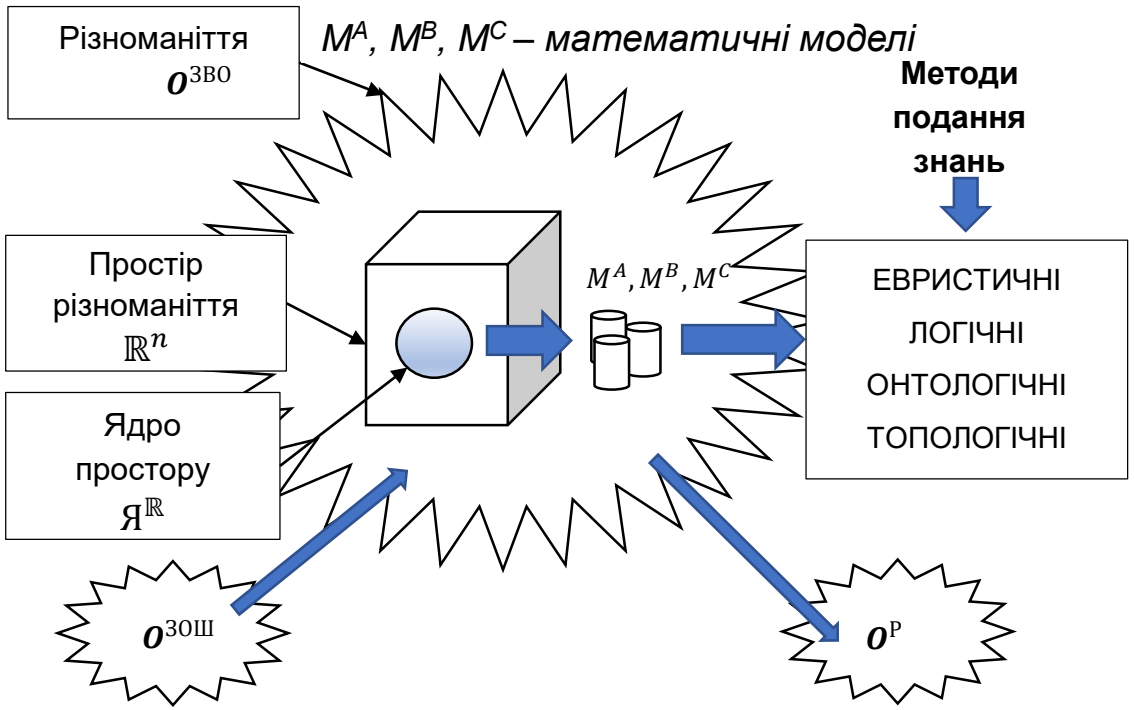
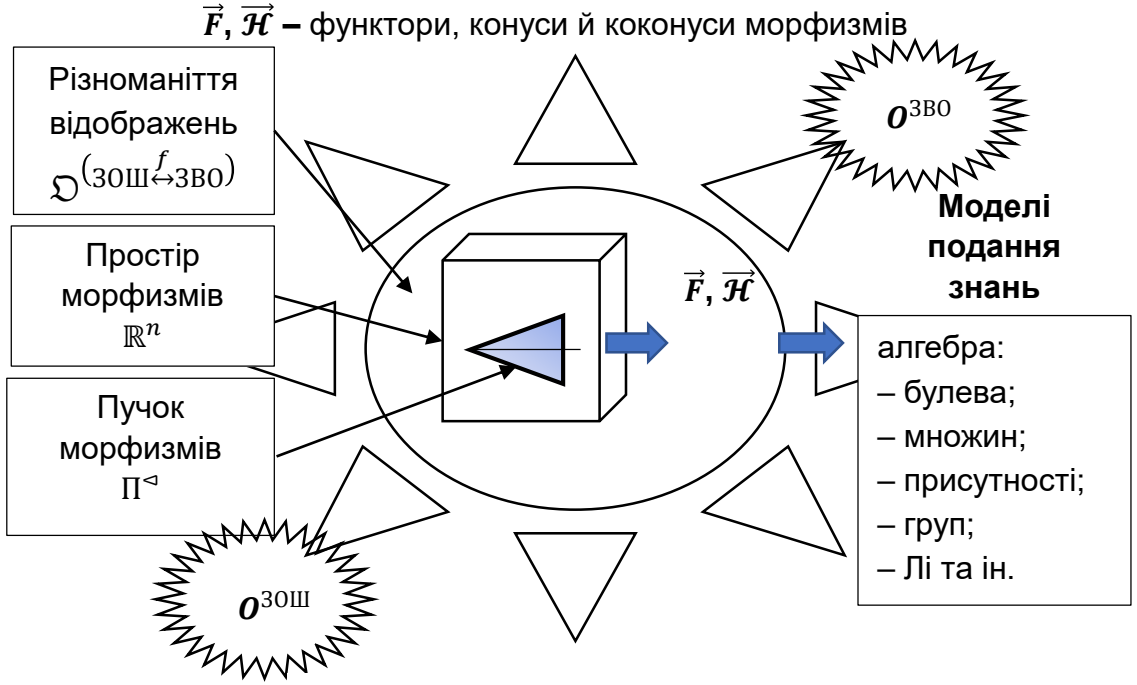


Рисунок 15.2 – Ілюстрація ієрархії формалізмів різноманіття закладів вищої освіти

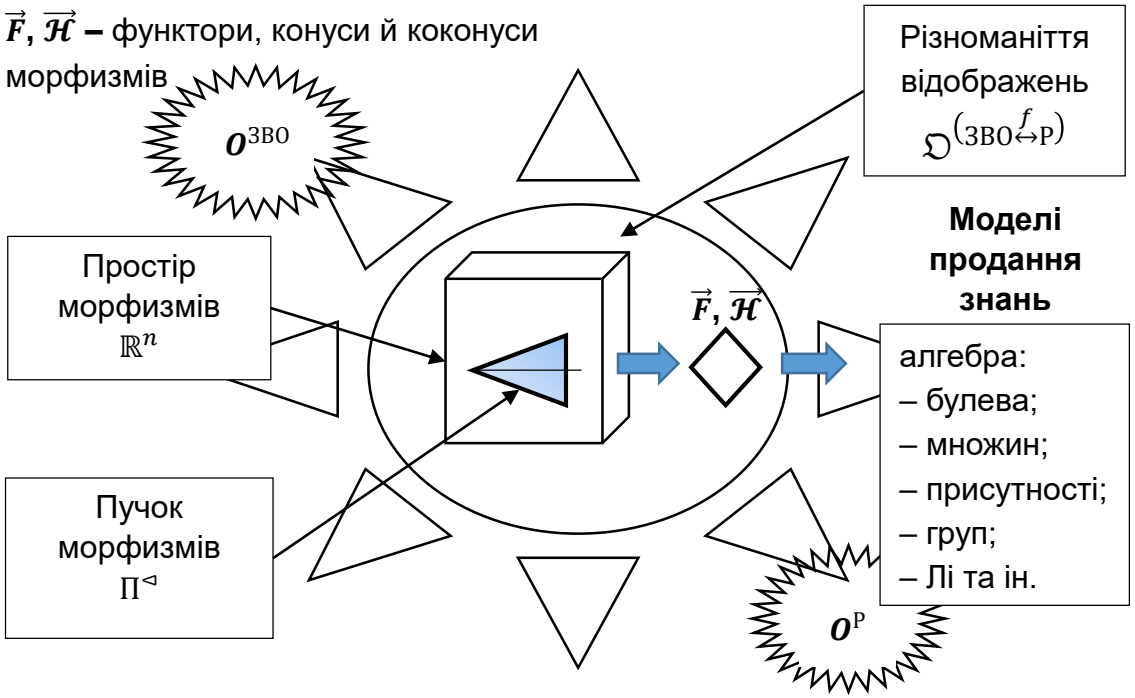
По суті розроблена схема дозволяє задати темпоральні відношення в процесі формалізації, наприклад, опис різноманіття закладів вищої освіти, задати простір $\mathbb{R}^n$, вибрати значущі елементи топологічного простору, тобто сформувати ядро простору $Я^{\mathbb{R}}$, розробити моделі значущих елементів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

МЕТОДОЛОГІЧНІ ОСНОВИ СТВОРЕННЯ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ У ГАЛУЗІ ПІДГОТОВКИ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ ТА БЕЗПЕКИ ІНДУСТРІАЛЬНИХ СИСТЕМ (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

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 7.1 – Узагальнена схема побудови моделі професійних знань

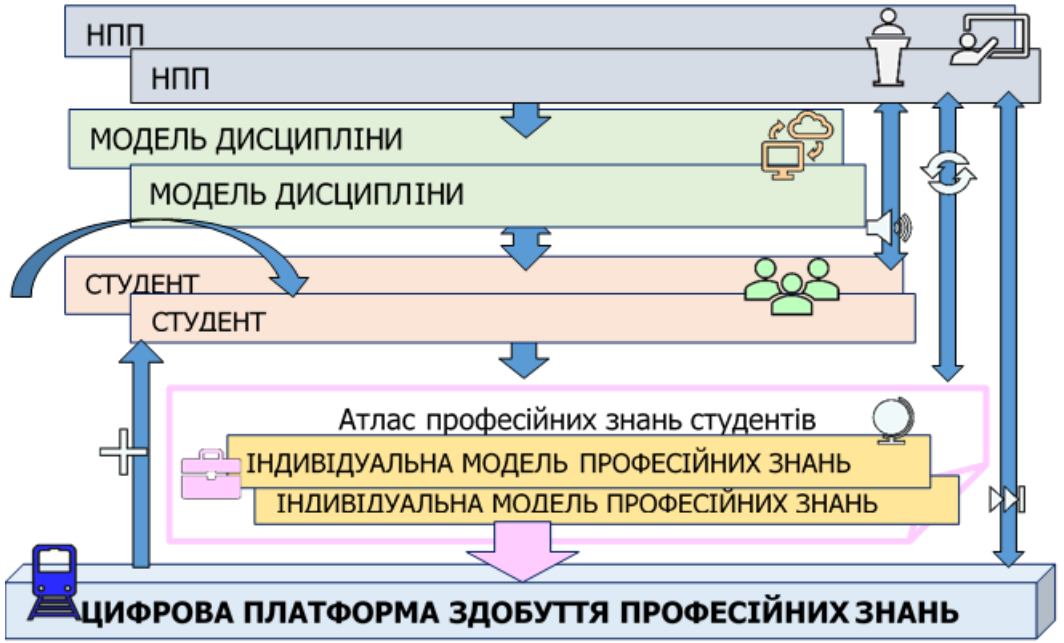


Рисунок 7.2 – Узагальнена схема побудови моделі професійних знань

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 систем, веб-орієнтованих систем на основі систем керування вмістом, віртуальних мереж, що забезпечують їх взаємодію, та методології підготовки фахівців з кібербезпеки

ВИРІШЕНО

1. Запропоновано концепцію та принципи забезпечення кібербезпеки індустріальних і веб-орієнтованих систем і мереж.

2. Розроблено модель згорткової нейронної мережі на основі використання змішаних даних та метод виявлення шкідливого програмного забезпечення в операційній системі Android на основі опрацювання викликів прикладного програмного інтерфейсу (API) та набору дозволів.

3. Розроблено методи інформаційної технології забезпечення кібербезпеки веб-орієнтованих систем на основі систем керування вмістом, засновані на оцінюванні схильності до поширених сценаріїв атак та виборі найбільш ефективних засобів захисту.

4. Розроблено моделі та методи забезпечення кібербезпеки віртуальних мереж, засновані на використанні концепції віртуального тунелювання в мережі Інтернет.

5. Розроблено методологічні основи створення інформаційної технології та модель цифрової платформи знань для використання в дуальній системі підготовки фахівців під час здобуття професійних знань.

6. Впроваджено методи технологій забезпечення кібербезпеки індустріальних і веб-орієнтованих систем і мереж.

ДОЗВОЛИЛО

Розробити та впровадити моделі, методи та технології забезпечення кібербезпеки мобільних систем, веб-орієнтованих систем на основі систем керування вмістом, віртуальних мереж, що забезпечують їх взаємодію, та методологію підготовки фахівців з кібербезпеки в сфері інформаційних технологій, машинобудуванні, авіаційній промисловості, вищій освіті тощо. Використання результатів досліджень підтверджується актами впровадження розроблених моделей і методів технологій в навчальний процес, сферу інформаційних технологій та науково-дослідну діяльність підприємств індустрії.

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 операційній системі Android	Метод забезпечення кібербезпеки систем керування вмістом	Метод оцінювання кібербезпеки систем керування вмістом шляхом використання дерев атак	Модель віртуальної мережі з темпоральним критерієм диспетчеризації запитів	Метод автоматизованої побудови VPN-ланцюгів між кінцевими користувачами віртуальної мережі	Методика застосування задачі комівояжера з декількома активними агентами, що діють за принципом квест-сценаріїв	Методологічні основи інформаційної технології для дуальної системи підготовки фахівців	Модель цифрової платформи підтримки процесів здобуття професійних знань
1	2	3	4	5	6	7	8	9	10	11	12
Інформаційні технології	Компанія «LineUp»	Інформаційні системи						+	+		
	Підприємство «GMhost»	Хостинг з віртуалізації веб-орієнтованих систем		+							
	ТОВ «Blackthorn Vision»	Мобільні системи		+							
	ТОВ «ІТТ»	Система тестування програмного забезпечення в індустріальних системах передачі даних	+	+							
	ТОВ «ХАКЕН»	Системи забезпечення кібербезпеки веб-орієнтованих систем			+	+					
	ТОВ «Компанія «Електронний Світ»	Електронна комерція			+						
Авіаційна промисловість	ДП «Південний державний проектно-конструкторський та науково-дослідний інститут авіаційної промисловості»	Комплексні проекти авіаційних підприємств					+	+			
Машинобудування	АТ «ФЕД»	Повний цикл створення сучасного авіаційного агрегату								+	+
Вища освіта	Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Хмельницький національний університет, Харківський національний університет радіоелектроніки	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 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 операційній системі Android

Забезпечено допустиме значення показника успішності атак при мінімальній вартості й обрано 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%

Зменшено часові затрати на побудову та перебудову структури віртуальної мережі у разі досягнення граничних значень мережної затримки або компроментації вузлів кіберзлочинцями всередньому на 50%

Підвищено ефективність підготовки фахівців з кібербезпеки, 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

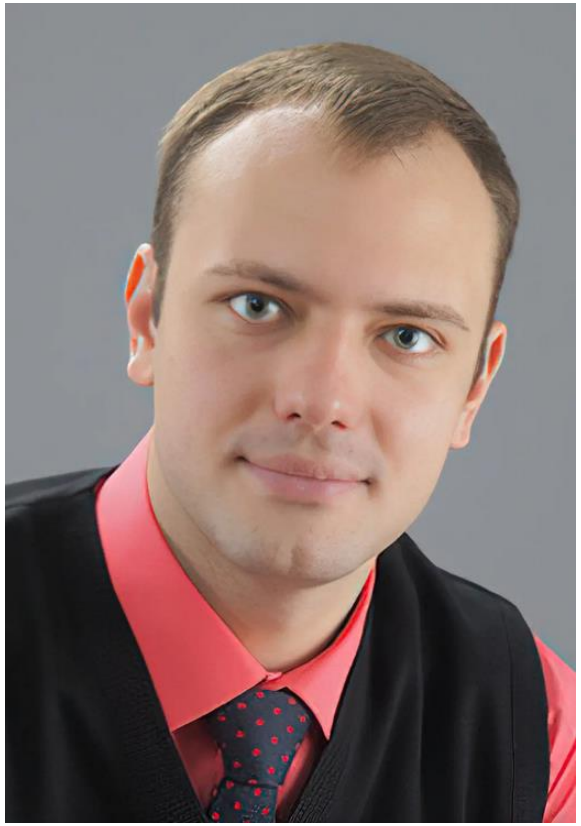
Кількість публікацій претендентів за роботою: **145**, а саме:

- **6** монографій (у тому числі **2** у видавництвах Springer, River Publishers),
- **4** навчальних посібника,
- **56** статей (**48** наукових статей у збірниках, що включені до переліку наукових фахових видань України, **4** статті в збірниках, що входять до наукометричних баз даних, **4** наукові статті в міжнародних журналах);
- **69** публікації матеріалів міжнародних конференцій та тези доповідей (**24** публікації в матеріалах конференцій, що входять до наукометричних баз даних (з них **12** публікацій у періодичних виданнях), **45** публікацій у матеріалах конференцій, тезах доповідей та виданнях, що не включені до переліку наукових фахових видань України);
- **8** патентів України на корисну модель, **2** свідоцтва на авторський твір.

ЦИТУВАННЯ ПУБЛІКАЦІЙ ПРЕТЕНДЕНТІВ

	Кількість посилань згідно бази даних		
	Web of Science	Scopus	Google Scholar
Загальна кількість цитувань	15	131	332
h-індекс робіт	2	8	12
h-індекс авторів			
Морозова О. І.	-	2	4
Нічепорук А. О.	1	4	4
Тецький А. Г.	-	1	2
Ткачов В. М.	2	5	11
Загальний h-індекс авторів	3	12	21

АВТОРСЬКИЙ КОЛЕКТИВ



Морозова Ольга Ігорівна,
д.т.н., доцент, професор
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
Хмельницького національного
університету.
E-mail:
andrey.nicheporuk@khnu.km.ua

Тецький Артем Григорович
к.т.н., старший викладач
Національного аерокосмічного
університету ім. М. Є. Жуковського
«Харківський авіаційний інститут».
E-mail: a.tetskiy@csn.khai.edu

Ткачов Віталій Миколайович
к.т.н., доцент Харківського
національного університету
радіоелектроніки.
E-mail: vitalii.tkachov@nure.ua